Networking Academy

CyberOps Associate

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
1.0 Introduction						
1.0.1 First Time in this Course						
1.0.2 Student Resources						
1.0.3 Ethical Hacking Statement						
1.0.4 Why Should I Take this Module?						
1.0.5 What Will I Learn in this Module?						
1.0.6 Class Activity - Top Hacker Shows Us How It's Done						
1.1 War Stories						
1.1.1 Hijacked People	K0003, K0004, K0005	HS-ETS1-3.	ITEA.1	IT 08-1	3A-NI-08, 3B-NI-04	
1.1.2 Ransomed Companies	K0003, K0004, K0005	HS-ETS1-3.	ITEA.1	IT 08-1	3A-NI-08, 3B-NI-04	
1.1.3 Targeted Nations	K0003, K0004, K0005	HS-ETS1-3.	ITEA.1	IT 08-1	3A-NI-08, 3B-NI-04	
1.1.4 Video - Anatomy of an Attack						
1.1.5 Lab - Installing the Virtual Machines	K0003, K0004, K0005	HS-ETS1-4.	ITEA.2	IT-NET 3	3A-NI-08, 3B-NI-04	
1.1.6 Lab - Cybersecurity Case Studies	K0003, K0004, K0005	HS-ETS1-4.	ITEA.3	IT-NET 3	3A-NI-08, 3B-NI-04	
1.2 Threat Actors						
1.2.1 Threat Actors	K0003, K0004, K0005	HS-ETS1-1.	ITEA.2.	IT 08-1	3A-NI-08, 3B-NI-04	1.3.d Threat actor
1.2.2 How Secure is the Internet of Things?	K0003, K0004, K0005	HS-ETS1-1.	ITEA.2.	IT 08-1	3A-NI-08, 3B-NI-04	1.3.d Threat actor
1.2.3 Lab - Learning the Details of Attacks	K0003, K0004, K0005	HS-ETS1-4.	ITEA.2.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-08, 3B-NI-04	1.3.d Threat actor
1.3 Threat Impact						
1.3.1 PII, PHI, and PSI	K0003, K0004, K0005; K0202; K0260	HS-ETS1-1.	ITEA.3.	IT 04	3A-NI-08, 3B-NI-04	5.9 Identify protected data in a network (a - d)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
1.3.2 Lost Competitive Advantage	K0003, K0004, K0005	HS-ETS1-1.	ITEA.3.	IT 04	3A-NI-08, 3B-NI-04	5.9 Identify protected data in a network (a - d)
1.3.3 Politics and National Security	K0003, K0004, K0005	HS-ETS1-1.	ITEA.3.	IT 04	3A-NI-08, 3B-NI-04	5.9 Identify protected data in a network (a - d)
1.3.4 Lab - Visualizing the Black Hats	K0003, K0004, K0005	HS-ETS1-4.	ITEA.3.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-08, 3B-NI-04	5.9 Identify protected data in a network (a - d)
1.4 The Danger Summary						
1.4.1 What Did I Learn in this Module?						
1.6.2 Module 1: The Danger Quiz						
2.0 Introduction						
2.0.1 Why Should I Take this Module?						
2.0.2 What Will I Learn in this Module?						
2.1 The Modern Security Operations Center						
2.1.1 Elements of a SOC	K0001; K0235;	HS-ETS1-1.	ITEA.4.	IT 04	3A-NI-06, 3A-NI-08	1.2 Compare security deployments 1.2.d SIEM/SOAR 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)
2.1.2 People in the SOC	K0001; K0235;	HS-ETS1-1.	ITEA.4.	IT 04	3A-NI-06, 3A-NI-08	1.2 Compare security deployments 1.2.d SIEM/SOAR 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)
2.1.3 Process in the SOC	K0001; K0235;	HS-ETS1-1.	ITEA.4.	IT 04	3A-NI-06, 3A-NI-08	1.2 Compare security deployments 1.2.d SIEM/SOAR 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)
2.1.4 Technologies in the SOC: SIEM	K0001; K0235;	HS-ETS1-1.	ITEA.4.	IT 04	3A-NI-06, 3A-NI-08	1.2 Compare security deployments 1.2.d SIEM/SOAR 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
2.1.5 Technologies in the SOC: SOAR	K0001; K0235;	HS-ETS1-1.	ITEA.4.	IT 04	3A-NI-06, 3A-NI-08	1.2 Compare security deployments 1.2.d SIEM/SOAR 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)
2.1.6 SOC Metrics	K0001; K0235;	HS-ETS1-1.	ITEA.4.	IT 04	3A-NI-06, 3A-NI-08	1.2 Compare security deployments 1.2.d SIEM/SOAR 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)
2.1.7 Enterprise and Managed Security	K0001; K0235;	HS-ETS1-1.	ITEA.4.	IT 04	3A-NI-06, 3A-NI-08	1.2 Compare security deployments 1.2.d SIEM/SOAR 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)
2.1.8 Security vs. Availability	K0001; K0235;	HS-ETS1-1.	ITEA.4.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-06, 3A-NI-08	1.2 Compare security deployments 1.2.d SIEM/SOAR 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)
2.1.9 Check Your Understanding – Identify the SOC Terminology	K0001; K0235;	HS-ETS1-4.	ITEA.4.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-06, 3A-NI-08	1.2 Compare security deployments 1.2.d SIEM/SOAR 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)
2.2 Becoming a Defender						
2.2.1 Certifications	K0243; K0245; K0252;	HS-ETS1-1.	ITEA.1.	IT 02	3A-NI-06, 3A-NI-08	
2.2.2 Further Education	K0243; K0245; K0252;	HS-ETS1-1.	ITEA.1.	IT 02	3A-NI-06, 3A-NI-08	
2.2.3 Sources of Career Information	K0243; K0245; K0252;	HS-ETS1-1.	ITEA.1.	IT 02	3A-NI-06, 3A-NI-08	
2.2.4 Getting Experience	K0243; K0245; K0252;	HS-ETS1-1.	ITEA.1.	IT 02	3A-NI-06, 3A-NI-08	

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
2.2.5 Lab – Becoming a Defender	K0243; K0245; K0252;	HS-ETS1-4.	ITEA.1.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-06, 3A-NI-08	
2.3 Fighters in the War Against Cybercrime Summary						
2.3.1 What Did I Learn in this Module?						
2.3.2 Module 2: Fighters in the War Against Cybercrime Quiz						
3.0 Introduction						
3.0.1 Why Should I Take this Module?						
3.0.3 Class Activity - Identify Running Processes						
3.0.2 What Will I Learn in this Module?						
3.1 Windows History						
3.1.1 Disk Operating System	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	
3.1.2 Windows Versions	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.1.3 Windows GUI	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.1.4 Operating System Vulnerabilities	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2 Windows Architecture and Operations						
3.2.1 Hardware Abstraction Layer	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
3.2.2 User Mode and Kernel Mode	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2.3 Windows File Systems	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2.4 Alternate Data Streams	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2.5 Windows Boot Process	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2.6 Windows Startup	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2.7 Windows Shutdown	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2.8 Processes, Threads, and Services	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2.9 Memory Allocation and Handles	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2.10 The Windows Registry	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
3.2.11 Lab - Exploring Processes, Threads, Handles, and Windows Registry	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.7.	CCR.ELA-Literacy.RST. 11-12.3.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.2.12 Check Your Understanding - Identify the Windows Registry Hive	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3 Windows Configuration and Monitoring						
3.3.1 Run as Administrator	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.2 Local Users and Domains	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.3 CLI and PowerShell	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.4 Windows Management Instrumentation	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.5 The net Command	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.6 Task Manager and Resource Monitor	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
3.3.7 Networking	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.8 Accessing Network Resources	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.9 Windows Server	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.10 Lab - Create User Accounts	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.9.	CCR.ELA-Literacy.RST. 11-12.3.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.11 Lab - Using Windows PowerShell	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.9.	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.3.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.12 Lab - Windows Task Manager	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.9.	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.3.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.3.13 Lab - Monitor and Manage System Resources in Windows	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.9.	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.3.	3A-CS-02, 3B-CS-01	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
3.4 Windows Security						
3.4.1 The netstat Command	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	1.2 Compare security deployments 1.2.c Legacy antivirus and antimalware
3.4.2 Event Viewer	K0060; K0224; K0452;	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	1.2 Compare security deployments 1.2.c Legacy antivirus and antimalware

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	K0537; K0608					
3.4.3 Windows Update Management	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	1.2 Compare security deployments 1.2.c Legacy antivirus and antimalware
3.4.4 Local Security Policy	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	1.2 Compare security deployments 1.2.c Legacy antivirus and antimalware
3.4.5 Windows Defender	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	1.2 Compare security deployments 1.2.c Legacy antivirus and antimalware
3.4.6 Windows Defender Firewall	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1	3A-CS-02, 3B-CS-01	1.2 Compare security deployments 1.2.c Legacy antivirus and antimalware
3.4.7 Check Your Understanding - Identify the Windows Tool	K0060; K0224; K0452; K0537; K0608	HS-ETS1., HS-PS4-2.	ITEA.12	IT-NET 4.1 CCR.ELA-Literacy.RST. 11-12.4.	3A-CS-02, 3B-CS-01	1.2 Compare security deployments 1.2.c Legacy antivirus and antimalware
3.5 The Windows Operating System Summary						
3.5.1 What Did I Learn in this Module?						
3.5.2 Module 3: The Windows Operating System Quiz						
4.0 Introduction						
4.0.1 Why Should I Take this Module?						
4.0.2 What Will I Learn in this Module?						
4.1 Linux Basics						
4.1.1 What is Linux?	K0224; K0397; K0537; K0608;	HS-ETS1.	ITEA.2., ITEA.9., ITEA.17.	IT-NET 1.4 IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.1.2 The Value of Linux	K0224; K0397;	HS-ETS1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	K0537; K0608;					
4.1.3 Linux in the SOC	K0224; K0397; K0537; K0608;	HS-ETS1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.1.4 Linux Tools	K0224; K0397; K0537; K0608;	HS-ETS1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.2 Working in the Linux Shell						
4.2.1 The Linux Shell	K0224; K0397; K0537; K0608;		ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.2.2 Basic Commands	K0224; K0397; K0537; K0608;	HS-ETS1.	ITEA.2., ITEA.9., ITEA.17.	IT-NET 1.4	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.2.3 File and Directory Commands	K0224; K0397; K0537; K0608;	HS-ETS1.	ITEA.2., ITEA.9., ITEA.17.	IT-NET 1.4	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.2.4 Working with Text Files	K0224; K0397; K0537; K0608;	HS-ETS1.	ITEA.2., ITEA.9., ITEA.17.	IT-NET 1.4	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.2.5 The Importance of Text Files in Linux	K0224; K0397; K0537; K0608;	HS-ETS1.	ITEA.2., ITEA.9., ITEA.17.	IT-NET 1.4	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.2.6 Lab – Working with Text Files in the CLI	K0224; K0397; K0537; K0608;	HS-ETS1.	ITEA.2., ITEA.9., ITEA.17.	IT-NET 1.4 CCR.ELA-Literacy.RST. 11-12.3.	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.2.7 Lab – Getting Familiar with the Linux Shell	K0224; K0397; K0537; K0608;		ITEA.9.	CCR.ELA-Literacy.RST. 11-12.3.	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.3 Linux Servers and Clients	K0224; K0397; K0537; K0608;					

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
4.3.1 An Introduction to Client-Server Communications	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.3.2 Servers, Services, and Their Ports	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.3.3 Clients	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.3.4 Lab - Linux Servers	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.4 Basic Server Administration						
4.4.1 Service Configuration Files	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.4.2 Hardening Devices	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.4.3 Monitoring Service Logs	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.4.4 Lab – Locating Log Files	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.5 The Linux File System	K0224; K0397; K0537; K0608;					
4.5.1 The File System Types in Linux	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.5.2 Linux Roles and File Permissions	K0224; K0397;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	K0537; K0608;					
4.5.3 Hard Links and Symbolic Links	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.5.4 Lab - Navigating the Linux Filesystem and Permission Settings	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.6 Working with the Linux GUI						
4.6.1 X Window System	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.6.2 The Linux GUI	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.7 Working on a Linux Host						
4.7.1 Installing and Running Applications on a Linux Host	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.7.2 Keeping the System Up to Date	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.7.3 Processes and Forks	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.7.4 Malware on a Linux Host	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.7.5 Rootkit Check	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.7.6 Piping Commands	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	IT 06	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
4.7.7 Video - Applications, Rootkits, and Piping Commands	K0224; K0397; K0537; K0608;	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7.	3A-CS-02, 3A-NI-08, 3B-AP-08	3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
4.8 Linux Basics Summary						
4.8.1 What Did I Learn in this Module?						
4.8.2 Module 4: Linux Basics Quiz						
5.0 Introduction						
5.0.1 Why Should I Take this Module?						
5.0.2 What Will I Learn in this Module?						
5.1 Network Communications Process						
5.1.1 Networks of Many Sizes	K0001; K0034; K0174; K0255; K0332;	HS-ETS1-3.	ITEA.1.L.	IT-NET 3 CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04, 3B-NI-03	
5.1.2 Client-Server Communications	K0001; K0034; K0174; K0255; K0332;	HS-ETS1-3.	ITEA.1.L.	IT-NET 3	3A-NI-04, 3B-NI-03	
5.1.3 Typical Sessions	K0001; K0034; K0174; K0255; K0332;	HS-ETS1-3.	ITEA.1.L.	IT-NET 3	3A-NI-04, 3B-NI-03	
5.1.4 Tracing the Path	K0001; K0034; K0111; K0174; K0255; K0332;	HS-ETS1-3.	ITEA.1.L.	IT-NET 3	3A-NI-04, 3B-NI-03	
5.1.5 Lab - Tracing a Route	K0001; K0034; K0111; K0174; K0255; K0332;	HS-ETS1.	ITEA.10.I	IT-NET 3 CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04, 3B-NI-03	
5.2 Communications Protocols	K0001; K0034; K0174; K0255; K0332;					

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
5.2.1 What are Protocols?	K0001; K0034; K0174; K0255; K0332;	HS-ETS1-3.	ITEA.8.H, ITEA.17.L	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS
5.2.2 Network Protocols	K0001; K0034; K0174; K0255; K0332;	HS-ETS1-3.	ITEA.8.H, ITEA.17.L	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS
5.2.3 The TCP/IP Protocol Suite	K0001; K0034; K0061; K0174; K0255; K0332; K0555; K0565;	HS-ETS1-3.	ITEA.8.H, ITEA.17.L	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS
5.2.4 Message Formatting and Encapsulation	K0001; K0034; K0174; K0255; K0332;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS
5.2.5 Message Size	K0001; K0034; K0174; K0255; K0332;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS
5.2.6 Message Timing	K0001; K0034; K0174; K0255; K0332;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS
5.2.7 Unicast, Multicast, and Broadcast	K0001; K0034; K0174; K0255; K0332;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
5.2.8 The Benefits of Using a Layered Model	K0001; K0034; K0174; K0255; K0332;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS
5.2.9 The OSI Reference Model	K0001; K0034; K0174; K0221; K0255; K0332;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS
5.2.10 The TCP/IP Protocol Model	K0001; K0034; K0061; K0174; K0255; K0332;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP 4.8.f ICMP 4.8.g DNS
5.3 Data Encapsulation	K0001; K0034; K0174; K0255; K0332;					
5.3.1 Segmenting Messages	K0001; K0034; K0174; K0255; K0332;	HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	3A-NI-04, 3B-NI-03	2.3 Describe the impact of these technologies on data visibility 2.3.g Encapsulation
5.3.2 Sequencing	K0001; K0034; K0174; K0255; K0332;	HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	3A-NI-04, 3B-NI-03	2.3 Describe the impact of these technologies on data visibility 2.3.g Encapsulation
5.3.3 Protocol Data Units	K0001; K0034; K0174; K0255; K0332;	HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	3A-NI-04, 3B-NI-03	2.3 Describe the impact of these technologies on data visibility 2.3.g Encapsulation
5.3.4 Three Addresses	K0001; K0034; K0174; K0255; K0332;	HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	3A-NI-04, 3B-NI-03	2.3 Describe the impact of these technologies on data visibility 2.3.g Encapsulation

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
5.3.5 Encapsulation Example	K0001; K0034; K0174; K0255; K0332;	HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	3A-NI-04, 3B-NI-03	2.3 Describe the impact of these technologies on data visibility 2.3.g Encapsulation
5.3.6 De-encapsulation Example	K0001; K0034; K0174; K0255; K0332;	HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3	3A-NI-04, 3B-NI-03	2.3 Describe the impact of these technologies on data visibility 2.3.g Encapsulation
5.3.7 Lab - Introduction to Wireshark	K0001; K0034; K0174; K0255; K0332;	HS-ETS1.	ITEA.2	IT-NET 3 CCR.ELA-Literacy.RST. 11-12.8.	3A-NI-04, 3B-NI-03	2.3 Describe the impact of these technologies on data visibility 2.3.g Encapsulation
5.3.8 Check Your Understanding - Data Encapsulation	K0001; K0034; K0174; K0255; K0332;	HS-PS4-1., HS-PS4-5.	ITEA.8.H, ITEA.17.L	IT-NET 3		2.3 Describe the impact of these technologies on data visibility 2.3.g Encapsulation
5.4 Network Protocols Summary						
5.4.1 What Did I Learn in this Module?						
5.4.2 Module 5: Network Protocols Quiz						
6.0 Introduction						
6.0.1 Why Should I Take this Module?						
6.0.2 What Will I Learn in this Module?						
6.1 Ethernet						
6.1.1 Ethernet Encapsulation	K0061; K0274; K0417;	HS-ETS1.	ITEA.9.I, ITEA.10.I	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame
6.1.2 Ethernet Frame Fields	K0061; K0274; K0417;	HS-ETS1.	ITEA.9.I, ITEA.10.I	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame
6.1.3 MAC Address Format	K0061; K0274; K0417;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame
6.1.4 Check Your Understanding - Ethernet Frame Fields	K0061; K0274; K0417;			CCR.ELA-Literacy.RST. 11-12.9.	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
6.2 IPv4						
6.2.1 The Network Layer	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.2.2 IP Encapsulation	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.2.3 Characteristics of IP	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.2.4 Connectionless	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.2.5 Best Effort	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.2.6 Media Independent	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.2.7 Check Your Understanding - IP Characteristics	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.2.8 IPv4 Packet Header	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.2.9 IPv4 Packet Header Fields	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.2.10 Check Your Understanding - IPv4 Packet	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 0	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4
6.3 IP Addressing Basics						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
6.3.1 Network and Host Portions	K0061; K0274; K0417; K0471; K0491; K0627;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.3.2 The Subnet Mask	K0061; K0274; K0417; K0471; K0491; K0627;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.3.3 The Prefix Length	K0061; K0274; K0417; K0471; K0491; K0627;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.3.4 Determining the Network: Logical AND	K0061; K0274; K0417; K0471; K0491; K0627;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.3.5 Video – Network, Host, and Broadcast Addresses	K0061; K0274; K0417; K0471; K0491; K0627;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.3.6 Subnetting Broadcast Domains	K0061; K0274; K0417; K0471; K0491; K0627;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.3.7 Check Your Understanding - IPv4 Address Structure	K0061; K0274; K0417; K0471; K0491; K0627;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.4 Types of IPv4 Addresses						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
6.4.1 IPv4 Address Classes and Default Subnet Masks	K0061; K0274; K0417; K0471; K0491; K0627;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.4.2 Reserved Private Addresses	K0061; K0274; K0417; K0471; K0491; K0627;	HS-PS2-2.	ITEA.3.J, ITEA.11.P	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.5 Network Design and Access Layer Summary						
6.5.1 Host Forwarding Decision	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.5.2 Default Gateway	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.5.3 A Host Routes to the Default Gateway	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.5.4 Host Routing Tables	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6
6.5.5 Check Your Understanding - How a Host Routes	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.a Ethernet frame 4.8.b IPv4 4.8.c IPv6

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
6.6 IPv6						
6.6.1 Need for IPv6	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.c IPv6
6.6.2 IPv6 Addressing Formats	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.c IPv6
6.6.3 Rule 1 – Omit Leading Zeros	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.c IPv6
6.6.4 Rule 2- Double Colon	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.c IPv6
6.6.5 IPv6 Prefix Length	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.c IPv6
6.6.6 Video – Layer 2 and Layer 3 Addressing	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3 CCR.ELA-Literacy.WHST.11-12.7.	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.c IPv6
6.6.7 Check Your Understanding - IPv6 Address Representation	K0061; K0274; K0417;	HS-PS3-3., HS-PS4-5.	ITEA.11.N.	IT-NET 3 CCR.ELA-Literacy.WHST.11-12.7.	3A-NI-04, 3B-NI-03	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.c IPv6
6.7 Ethernet and IP Protocol Summary						
6.7.1 What Did I Learn in this Module?						
6.7.2 Module 6: Ethernet and IP Protocol Quiz						
7.0 Introduction						
7.0.1 Why Should I Take this Module?						
7.0.2 What Will I Learn in this Module?						
7.1 ICMP						
7.1.1 ICMPv4 Messages	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
7.1.2 ICMPv6 RS and RA Messages	A0055	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP
7.2 Ping and Traceroute Utilities						
7.2.1 Video - Network Testing and Verification with Windows CLI Commands	K0111;	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP
7.2.2 Ping - Test Connectivity	K0111;	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP
7.2.3 Ping the Loopback	K0111;	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP
7.2.4 Ping the Default Gateway	K0111;	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP
7.2.5 Ping a Remote Host	K0111;	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP
7.2.6 Traceroute - Test the Path	K0111;	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP
7.2.7 ICMP Packet Format	K0111;	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP
7.2.8 Packet Tracer – Verify IPv4 and IPv6 Addressing	K0111;	HS-ETS1.	ITEA.10.I	IT-NET 3	3A-NI-04, 3A-NI-05, 3A-NI-07	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.f ICMP
7.3 Connectivity Verification Summary						
7.3.1 What Did I Learn in this Module?						
7.3.2 Module 7: Connectivity Verification Quiz						
8.0 Introduction						
8.0.1 Why Should I Take this Module?						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
8.0.2 What Will I Learn in this Module?						
8.1 MAC and IP						
8.1.1 Destination on Same Network	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-ETS1.	ITEA.17.	IT-NET 3	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.j ARP
8.1.2 Destination on Remote Network	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-ETS1.	ITEA.17.	IT-NET 3	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.j ARP
8.2 ARP						
8.2.1 ARP Overview	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.7 Identify key elements in an intrusion from a given PCAP file 4.7.a Source address 4.7.b Destination address
8.2.2 ARP Functions	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.7 Identify key elements in an intrusion from a given PCAP file 4.7.a Source address 4.7.b Destination address
8.2.3 Video - ARP Operation - ARP Request	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3 CCR.ELA-Literacy.RST. 11-12.7.	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.7 Identify key elements in an intrusion from a given PCAP file 4.7.a Source address 4.7.b Destination address
8.2.4 Video - ARP Operation - ARP Reply	K0001, K0061, K0255, K0485, K0486,	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3 CCR.ELA-Literacy.RST. 11-12.7.	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.7 Identify key elements in an intrusion from a given PCAP file 4.7.a Source address 4.7.b Destination address

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	K0560, K0565					
8.2.5 Video - ARP Role in Remote Communication	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3 CCR.ELA-Literacy.RST. 11-12.7.	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.7 Identify key elements in an intrusion from a given PCAP file 4.7.a Source address 4.7.b Destination address
8.2.6 Removing Entries from an ARP Table	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.7 Identify key elements in an intrusion from a given PCAP file 4.7.a Source address 4.7.b Destination address
8.2.7 ARP Tables on Networking Devices	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.7 Identify key elements in an intrusion from a given PCAP file 4.7.a Source address 4.7.b Destination address
8.2.8 Lab - Using Wireshark to Examine Ethernet Frames	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.7 Identify key elements in an intrusion from a given PCAP file 4.7.a Source address 4.7.b Destination address
8.3 ARP Issues						
8.3.1 ARP Issues - ARP Broadcasts and ARP Spoofing	K0001, K0061, K0255, K0485, K0486, K0560, K0565	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.j ARP
8.3.2 Video - ARP Spoofing	K0001, K0061, K0255, K0485, K0486,	HS-PS3-3., HS-PS4-5.	ITEA.9.I, ITEA.10.I	IT-NET 3	3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.j ARP

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	K0560, K0565					
8.4 Address Resolution Protocol Summary						
8.4.1 What Did I Learn in this Module?						
8.4.2 Module 8: Address Resolution Protocol Quiz						
9.0 Introduction						
9.0.1 Why Should I Take this Module?						
9.0.2 What Will I Learn in this Module?						
9.1 Transport Layer Characteristics						
9.1.1 Role of the Transport Layer	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.1.2 Transport Layer Responsibilities	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.1.3 Transport Layer Protocols	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.1.4 Transmission Control Protocol (TCP)	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.1.5 TCP Header	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.1.6 TCP Header Fields	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.1.7 User Datagram Protocol (UDP)	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.1.8 UDP Header	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
9.1.9 UDP Header Fields	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.1.10 Socket Pairs	K0061	HS-ETS1-2.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.1.11 Check Your Understanding – Compare TCP and UDP Characteristics	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.4.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.2 Transport Layer Session Establishment						
9.2.1 TCP Server Processes	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.2.2 TCP Connection Establishment	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.2.3 Session Termination	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.2.4 TCP Three-way Handshake Analysis	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.2.5 Video – TCP 3-Way Handshake	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.2.6 Lab – Using Wireshark to Observe the TCP 3-Way Handshake	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.2.7 Check Your Understanding – TCP Connection and Termination Process	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.3 Transport Layer Reliability						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
9.3.1 TCP Reliability - Guaranteed and Ordered Delivery	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.3.2 Video - TCP Reliability – Sequence Numbers and Acknowledgements	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.3.3 TCP Reliability - Data Loss and Retransmission	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.3.4 Video - TCP Reliability – Data Loss and Retransmission	K0221	HS-ETS1-2.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.3.5 TCP Flow Control - Window Size and Acknowledgments	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.3.6 TCP Flow Control - Maximum Segment Size (MSS)	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.3.7 TCP Flow Control - Congestion Avoidance	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.3.8 Lab - Exploring Nmap	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.3.9 Check Your Understanding - Reliability and Flow Control	K0221	HS-ETS1-2.	ITEA.17.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
9.4 The Transport Layer Summary						
9.4.1 What Did I Learn in this Module?						
9.4.2 Module 9: The Transport Layer Quiz						
10.0 Introduction						
10.0.1 Welcome						
10.0.2 Introduction						
10.1 DHCP						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
10.1.1 Dynamic Host Configuration Protocol	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.1.2 DHCP Operation	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.1.3 DHCP Message Format	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.1.4 Check Your Understanding - DHCP	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.2 DNS						
10.2.1 DNS Overview	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS
10.2.2 The DNS Domain Hierarchy	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS
10.2.3 The DNS Lookup Process	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS
10.2.4 DNS Message Format	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS
10.2.5 Dynamic DNS	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS
10.2.6 The WHOIS Protocol	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS
10.2.7 Lab - Using Wireshark to Examine a UDP DNS Capture	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3 CCR.ELA-Literacy.RST.11-12.8.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS
10.3 NAT						
10.3.1 IPv4 Private Address Space	K0332; K0452	HS-ETS1.	ITEA.9.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.3.2 What is NAT?	K0332; K0452	HS-ETS1.	ITEA.9.	IT-NET 4	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
10.3.3 How NAT Works	K0332; K0452	HS-ETS1.	ITEA.9.	IT-NET 5	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.3.4 Port Address Translation	K0332; K0452	HS-ETS1.	ITEA.9.	IT-NET 6	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.4 File Transfer and Sharing Services						
10.4.1 FTP and TFTP	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.4.2 SMB	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.4.3 Lab - Using Wireshark to Examine TCP and UDP Captures	K0332; K0452	HS-ETS1.	ITEA.2	IT-NET 3 CCR.ELA-Literacy.RST. 11-12.3.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
10.5 Email						
10.5.1 Email Protocols	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP
10.5.2 SMTP	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP
10.5.3 POP3	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP
10.5.4 IMAP	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP
10.6 HTTP						
10.6.1 Hypertext Transfer Protocol and Hypertext Markup Language	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.i HTTP/HTTPS/HTTP2
10.6.2 The HTTP URL	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.i HTTP/HTTPS/HTTP2
10.6.3 HTTP Operation	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.i HTTP/HTTPS/HTTP2
10.6.4 HTTP Status Codes	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.i HTTP/HTTPS/HTTP2

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
10.6.5 HTTP/2	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.i HTTP/HTTPS/HTTP2
10.6.6 Securing HTTP – HTTPS	K0444	HS-ETS1.	ITEA.2	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.i HTTP/HTTPS/HTTP2
10.6.7 Lab - Using Wireshark to Examine HTTP and HTTPS Traffic	K0332	HS-ETS1.	ITEA.2	IT-NET 3 CCR.ELA-Literacy.RST. 11-12.8.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.i HTTP/HTTPS/HTTP2
10.7 Network Services Summary						
10.7.1 What Did I Learn in this Module?						
10.7.2 Module 10: Network Services Quiz						
11.0 Introduction						
11.0.1 Why Should I Take this Module?						
11.0.2 What Will I Learn in this Module?						
11.1 Network Devices						
11.1.1 End Devices	K0011; K0057; K0114; K0516;	HS-ETS1-3.	ITEA.17.O.	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.1.2 Video - End Devices	K0011; K0057; K0114; K0516;	HS-ETS1-3.	ITEA.17.O.	IT-NET 3 CCR.ELA-Literacy.RST. 11-12.7.	3A-NI-04; 3A-NI-05;	
11.1.3 Routers	K0011; K0057; K0114; K0516;	HS-PS3-3., HS-PS4-5.	ITEA.9.	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.1.4 Check Your Understanding - Match Layer 2 and Layer 3 Addressing	K0011; K0057; K0114; K0516;	HS-PS3-3., HS-PS4-5.	ITEA.9.	CCR.ELA-Literacy.RST. 11-12.9.	3A-NI-04; 3A-NI-05;	
11.1.5 Packet Forwarding Decision Process	K0011; K0057; K0114; K0516;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.1.6 Routing Information	K0011; K0057; K0114; K0516;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.1.7 End-to-End Packet Forwarding	K0011; K0057;	HS-PS3-3., HS-PS4-5.	ITEA.2.X.	IT-NET 3	3A-NI-04; 3A-NI-05;	

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	K0114; K0516;					
11.1.8 Video - Static and Dynamic Routing	K0011; K0057; K0114; K0516;	HS-PS3-3., HS-PS4-5.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-05;	
11.1.9 Hubs, Bridges, LAN Switches	K0011; K0057; K0114; K0516;	HS-PS3-3., HS-PS4-5.	ITEA.17.O	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.1.10 Switching Operation	K0011; K0057; K0114; K0516;	HS-PS3-3., HS-PS4-5.	ITEA.17.O	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.1.11 Video - MAC Address Tables on Connected Switches	K0011; K0057; K0114; K0516;	HS-PS3-3., HS-PS4-5.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-05;	
11.1.12 VLANs	K0011; K0057; K0114; K0516;	HS-PS3-3., HS-PS4-5.		IT-NET 3.7	3A-NI-04; 3A-NI-05;	
11.1.13 STP	K0011; K0057; K0114; K0516;	HS-ETS1.	ITEA.2.	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.1.14 Multilayer Switching	K0011; K0057; K0114; K0516;	HS-ETS1.	ITEA.8.	IT-NET 1	3A-NI-04; 3A-NI-05;	
11.2 Wireless Communications						
11.2.1 Video - Wireless Communications	K0108, K0274		ITEA.8.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-05;	
11.2.2 Wireless versus Wired LANs	K0108, K0274	HS-ETS1-2.	ITEA.11.	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.2.3 802.11 Frame Structure	K0108, K0274	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.2.4 CSMA/CA	K0108, K0274	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.2.5 Wireless Client and AP Association	K0108, K0275	HS-ETS1-4.	ITEA.8.	IT-NET 4	3A-NI-04; 3A-NI-05;	
11.2.6 Passive and Active Discover Mode	K0108, K0276	HS-ETS1-4.	ITEA.8.	IT-NET 5	3A-NI-04; 3A-NI-05;	

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
11.2.7 Check Your Understanding – Steps in the Client and AP Process	K0108, K0274	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05;	
11.2.8 Wireless Devices -AP, LWAP, and WLC	K0108, K0274	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-05;	
11.2.9 Check Your Understanding - Identify the LAN Device	K0108, K0274	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05;	
11.4 Network Communication Devices Summary						
11.4.1 What Did I Learn in this Module?						
11.4.11 Module 11: Network Communication Devices Quiz						
12.0 Introduction						
12.0.1 Why Should I Take this Module?						
12.0.2 What Will I Learn in this Module?						
12.1 Network Topologies						
12.1.1 Network Representations	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
12.1.2 Topology Diagrams	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
12.1.3 Networks of Many Sizes	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
12.1.4 LANs and WANs	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
12.1.5 The Three-Layer Network Design Model	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
12.1.6 Video - Three-Layer Network Design	K0179, K0486	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
12.1.7 Common Security Architectures	K0179, K0486	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
12.1.8 Check your Understanding - Identify the Network Topology	K0179, K0486	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
12.1.9 Packet Tracer - Identify Packet Flow	K0179, K0486	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
12.2 Security Devices						
12.2.1 Video - Security Devices	K0049; K0202; K0487;	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.2 Identify the types of data provided by these technologies 2.2.d Traditional stateful firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.2.2 Firewalls	K0049; K0202; K0487;	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.2 Identify the types of data provided by these technologies 2.2.d Traditional stateful firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.2.3 Firewall Type Descriptions	K0049; K0202; K0487;	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.2 Identify the types of data provided by these technologies 2.2.d Traditional stateful firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.2.4 Check Your Understanding - Identify the Type of Firewall	K0049; K0202; K0487;	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.2 Identify the types of data provided by these technologies 2.2.d Traditional stateful firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
12.2.5 Intrusion Prevention and Detection Devices	K0049; K0202; K0487;	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.2 Identify the types of data provided by these technologies 2.2.d Traditional stateful firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.2.6 Advantages and Disadvantages of IDS and IPS	K0049; K0202; K0487;	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.2 Identify the types of data provided by these technologies 2.2.d Traditional stateful firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.2.7 Types of IPS	K0049; K0202; K0487;	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.2 Identify the types of data provided by these technologies 2.2.d Traditional stateful firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.2.8 Specialized Security Appliances	K0049; K0202; K0487;	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.2 Identify the types of data provided by these technologies 2.2.d Traditional stateful firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
12.2.9 Check Your Understanding - Compare IDS and IPS Characteristics	K0049; K0202; K0487;	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.2 Identify the types of data provided by these technologies 2.2.d Traditional stateful firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.3 Security Services						
12.3.1 Video - Security Services	K0158	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.3.2 Traffic Control with ACLs	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
12.3.3 ACLs: Important Features	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.3.4 Packet Tracer - ACL Demonstration	K0158	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.3.5 SNMP	K0452, K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
12.3.6 NetFlow	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.3.7 Port Mirroring	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.3.8 Syslog Servers	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
12.3.9 NTP	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.3.10 AAA Servers	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.3.11 VPN	K0158	HS-ETS1-4.	ITEA.8.	IT-NET 3	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
12.3.12 Check Your Understanding - Identify the Network Security Device or Service	K0158	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.6 Compare access control models 1.6.d Authentication, authorization, accounting 2.3 Describe the impact of these technologies on data visibility 2.3.a Access control list 2.3.b NAT/PAT 2.3.c Tunneling 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.b Firewall
12.4 Network Security Infrastructure Summary						
12.4.1 What Did I Learn in this Module?						
12.4.2 Module 12: Network Security Infrastructure Quiz						
13.0 Introduction						
13.0.1 Why Should I Take this Module?						
13.0.2 What Will I Learn in this Module?						
13.1 Who is Attacking Our Network?						
13.1.1 Threat, Vulnerability, and Risk	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.1.2 Hacker vs. Threat Actor	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.1.3 Evolution of Threat Actors	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.1.4 Cybercriminals	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
13.1.5 Cybersecurity Tasks	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.1.6 Cyber Threat Indicators	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.1.7 Threat Sharing and Building Cybersecurity Awareness	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.1.8 Check Your Understanding – What Color is my Hat?	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 10	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.2 Threat Actor Tools						1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.2.1 Introduction of Attack Tools	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 10	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.2.2 Evolution of Security Tools	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 10	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.2.3 Categories of Attacks	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	IT 10	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.2.4 Check Your Understanding - Classify Cyber Attacks	K0005; K0049; K0162; K0408; K0436;	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-05; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.3 Describe security terms 1.3.d Threat actor 1.4 Compare security concepts (a - d)
13.3 Attackers and Their Tools Summary						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
13.3.1 What Did I Learn in this Module?						
13.3.2 Module 13: Attackers and Their Tools Quiz						
14.0 Introduction						
14.0.1 Why Should I Take this Module?						
14.0.2 What Will I Learn in this Module?						
14.1 Malware						
14.1.1 Types of Malware	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.1.2 Viruses	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.1.3 Trojan Horses	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.1.4 Trojan Horse Classification	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.1.5 Worms	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.1.6 Worm Components	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
14.1.7 Ransomware	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.1.8 Other Malware	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.1.9 Common Malware Behaviors	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.1.10 Check Your Understanding - Malware	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.1.11 Lab - Anatomy of Malware	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-05; 3A-NI-06;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.2 Common Network Attacks - Reconnaissance, Access, and Social Engineering						
14.2.1 Types of Network Attacks	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting 2.7 Describe social engineering attacks
14.2.2 Reconnaissance Attacks	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting 2.7 Describe social engineering attacks

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
14.2.3 Video - Reconnaissance Attacks	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting 2.7 Describe social engineering attacks
14.2.4 Access Attacks	K0005; K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting 2.7 Describe social engineering attacks
14.2.5 Video – Access and Social Engineering Attacks	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting 2.7 Describe social engineering attacks
14.2.6 Social Engineering Attacks	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting 2.7 Describe social engineering attacks
14.2.7 Strengthening the Weakest Link	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting 2.7 Describe social engineering attacks
14.2.8 Lab – Social Engineering	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-05; 3A-NI-06;	2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting 2.7 Describe social engineering attacks
14.3 Network Attacks - Denial of Service, Buffer Overflows, and Evasion						
14.3.1 Video - Denial of Service Attacks	K0161; K0162; K0177; K0191;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 2.8 Describe endpoint-based attacks, such as

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	K0362; K0480;					buffer overflows, command and control (C2), malware, and ransomware
14.3.2 DoS and DDoS Attacks	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.3.3 Components of DDoS Attacks	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.3.4 Video – Mirai Botnet	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.3.5 Buffer Overflow Attack	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.3.6 Evasion Methods	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	IT 08 1	3A-NI-05; 3A-NI-06;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.3.7 Check Your Understanding - Identify the Types of Network Attacks	K0161; K0162; K0177; K0191; K0362; K0480;	HS-ETS1-3.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-05; 3A-NI-06;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
14.4 Common Threats and Attacks Summary						
14.4.1 What Did I Learn in this Module?						
14.4.2 Module 14: Common Threats and Attacks Quiz						
15.0 Introduction						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
15.0.1 Why Should I Take this Module?						
15.0.2 What Will I Learn in this Module?						
15.0.3 Class Activity – What's Going On?		HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9.	3A-AP-22; 3A-IC-29; 3A-NI-06;	
15.1 Introduction to Network Monitoring						
15.1.1 Network Security Topology	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	IT 10	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.a Network, endpoint, and application security systems 4.4 Compare inline traffic interrogation and taps or traffic monitoring
15.1.2 Network Monitoring Methods	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	IT 10	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.a Network, endpoint, and application security systems 4.4 Compare inline traffic interrogation and taps or traffic monitoring
15.1.3 Network Taps	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	IT 10	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.a Network, endpoint, and application security systems 4.4 Compare inline traffic interrogation and taps or traffic monitoring
15.1.4 Traffic Mirroring and SPAN	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	IT 10	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.a Network, endpoint, and application security systems 4.4 Compare inline traffic interrogation and taps or traffic monitoring
15.2 Introduction to Network Monitoring Tools						
15.2.1 Network Security Monitoring Tools	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	IT 10	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 2.2 Identify the types of data provided by these technologies 2.2.b NetFlow 4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic
15.2.2 Network Protocol Analyzers	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	IT 10	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 2.2 Identify the types of data provided by these technologies 2.2.b NetFlow 4.5 Compare the characteristics of data obtained from taps or traffic monitoring and

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
						transactional data (NetFlow) in the analysis of network traffic
15.2.3 NetFlow	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	IT 10	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 2.2 Identify the types of data provided by these technologies 2.2.b NetFlow 4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic
15.2.4 SIEM and SOAR	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	IT 10	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 2.2 Identify the types of data provided by these technologies 2.2.b NetFlow 4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic
15.2.5 SIEM Systems	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	IT 10	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 2.2 Identify the types of data provided by these technologies 2.2.b NetFlow 4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic
15.2.6 Check Your Understanding - Identify the Network Monitoring Tool	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9.	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 2.2 Identify the types of data provided by these technologies 2.2.b NetFlow 4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
15.2.7 Packet Tracer - Logging Network Activity	K0054; K0180; K0620;	HS-ETS1-1.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9.	3A-AP-22; 3A-IC-29; 3A-NI-06;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 2.2 Identify the types of data provided by these technologies 2.2.b NetFlow 4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic
15.3 Network Monitoring and Tools Summary						
15.3.1 What Did I Learn in this Module?						
15.3.2 Module 15: Network Monitoring and Tools Quiz						
16.0 Introduction						
16.0.1 Why Should I Take this Module?						
16.0.2 What Will I Learn in this Module?						
16.1 IP PDU Details						
16.1.1 IPv4 and IPv6	K0005; K0009; K0062; K0301;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6
16.1.2 The IPv4 Packet Header	K0005; K0009; K0062; K0301;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6
16.1.3 Video - Sample IPv4 Headers in Wireshark	K0005; K0009; K0062; K0301;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6
16.1.4 The IPv6 Packet Header	K0005; K0009; K0062; K0301;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6
16.1.5 Video - Sample IPv6 Headers in Wireshark	K0005; K0009; K0062; K0301;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6
16.2 IP Vulnerabilities						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
16.2.1 IP Vulnerabilities	K0005, K0013; K0362; K0627;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6 4.8.f ICMP
16.2.2 ICMP Attacks	K0005, K0013; K0362; K0627;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6 4.8.f ICMP
16.2.3 Video - Amplification, Reflection, and Spoofing Attacks	K0005, K0013; K0362; K0627;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6 4.8.f ICMP
16.2.4 Amplification and Reflection Attacks	K0005, K0013; K0362; K0627;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6 4.8.f ICMP
16.2.5 Address Spoofing Attacks	K0005, K0013; K0362; K0627;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6 4.8.f ICMP

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
16.2.6 Check Your Understanding - IP Vulnerabilities and Threats	K0005, K0013; K0362; K0627;	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST. 11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.b IPv4 4.8.c IPv6 4.8.f ICMP
16.3 TCP and UDP Vulnerabilities						
16.3.1 TCP Segment Header	K0061; K0221; K0471; K0555; K0565;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
16.3.2 TCP Services	K0061; K0221; K0471; K0555; K0565;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
16.3.3 TCP Attacks	K0061; K0221; K0471; K0555; K0565;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
16.3.4 UDP Segment Header and Operation	K0061; K0221; K0471; K0555; K0565;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
16.3.5 UDP Attacks	K0061; K0221; K0471; K0555; K0565;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
16.3.6 Check Your Understanding - TCP and UDP Vulnerabilities	K0061; K0221; K0471; K0555; K0565;	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.d TCP 4.8.e UDP
16.4 Attacking the Foundation Summary						
16.4.1 What Did I Learn in this Module?						
16.4.2 Module 16: Attacking the Foundation Quiz						
17.0 Introduction						
17.0.1 Why Should I Take this Module?						
17.0.2 What Will I Learn in this Module?						
17.1 IP Services						
17.1.1 ARP Vulnerabilities	K0005; K0009; K0162	HS-ETS1-2.	ITEA.9.	IT 7	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS 4.8.j ARP
17.1.2 ARP Cache Poisoning	K0005; K0009; K0162	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS 4.8.j ARP
17.1.3 DNS Attacks	K0005; K0009; K0162	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS 4.8.j ARP
17.1.4 DNS Tunneling	K0005; K0009; K0162	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS 4.8.j ARP
17.1.5 DHCP	K0005; K0009; K0162	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS 4.8.j ARP
17.1.6 DHCP Attacks	K0005; K0009; K0162	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS 4.8.j ARP
17.1.7 Lab - Exploring DNS Traffic	K0005; K0009; K0162	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.g DNS 4.8.j ARP

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
17.2 Enterprise Services						
17.2.1 HTTP and HTTPS	K0005; K0009; K0447;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP 4.8.i HTTP/HTTPS/HTTP2
17.2.2 Common HTTP Exploits	K0005; K0009; K0447;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP 4.8.i HTTP/HTTPS/HTTP2
17.2.3 Email	K0005; K0009; K0447;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP 4.8.i HTTP/HTTPS/HTTP2
17.2.4 Web-Exposed Databases	K0005; K0009; K0447;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP 4.8.i HTTP/HTTPS/HTTP2
17.2.5 Client-side Scripting	K0005; K0009; K0447;	HS-ETS1-2.	ITEA.9.	IT 8	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP 4.8.i HTTP/HTTPS/HTTP2
17.2.6 Lab - Attacking a MySQL Database	K0005; K0009; K0447;	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP 4.8.i HTTP/HTTPS/HTTP2

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
17.2.7 Lab - Reading Server Logs	K0005; K0009; K0447;	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP 4.8.i HTTP/HTTPS/HTTP2
17.2.8 Check Your Understanding – Network Services Attacks	K0005; K0009; K0447;	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting 4.8 Interpret the fields in protocol headers as related to intrusion analysis 4.8.h SMTP/POP3/IMAP 4.8.i HTTP/HTTPS/HTTP2
17.3 Attacking What We Do Summary						
17.3.1 Packet Tracer - Compare In-Band and Out-of-Band Management Access	K0005; K0009; K0447;	HS-ETS1-2.	ITEA.9.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
17.3.2 Module 17: Attacking What We Do Quiz						
18.0 Introduction						
18.0.1 Why Should I Take this Module?						
18.0.2 What Will I Learn in this Module?						
18.1 Defense-in-Depth						
18.1.1 Assets, Vulnerabilities, Threats	K0005; K0009; K0013; K0112;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-05; 3A-NI-06; 3A-NI-08;	1.4 Compare security concepts 1.4.b Threat 1.4.c Vulnerability 1.5 Describe the principles of the defense-in-depth strategy 3.3 Describe the role of attribution in an investigation 3.3.a Assets 5.1 Describe management concepts 5.1.a Asset management
18.1.2 Identify Assets	K0005; K0009; K0013; K0112;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-05; 3A-NI-06; 3A-NI-08;	1.4 Compare security concepts 1.4.b Threat 1.4.c Vulnerability 1.5 Describe the principles of the defense-in-depth strategy 3.3 Describe the role of attribution in an investigation 3.3.a Assets 5.1 Describe management concepts 5.1.a Asset management

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
18.1.3 Identify Vulnerabilities	K0005; K0009; K0013; K0112;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-05; 3A-NI-06; 3A-NI-08;	1.4 Compare security concepts 1.4.b Threat 1.4.c Vulnerability 1.5 Describe the principles of the defense-in-depth strategy 3.3 Describe the role of attribution in an investigation 3.3.a Assets 5.1 Describe management concepts 5.1.a Asset management
18.1.4 Identify Threats	K0005; K0009; K0013; K0112;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-05; 3A-NI-06; 3A-NI-08;	1.4 Compare security concepts 1.4.b Threat 1.4.c Vulnerability 1.5 Describe the principles of the defense-in-depth strategy 3.3 Describe the role of attribution in an investigation 3.3.a Assets 5.1 Describe management concepts 5.1.a Asset management
18.1.5 The Security Onion and The Security Artichoke	K0005; K0009; K0013; K0112;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-05; 3A-NI-06; 3A-NI-08;	1.4 Compare security concepts 1.4.b Threat 1.4.c Vulnerability 1.5 Describe the principles of the defense-in-depth strategy 3.3 Describe the role of attribution in an investigation 3.3.a Assets 5.1 Describe management concepts 5.1.a Asset management
18.2 Security Policies, Regulations, and Standards						
18.2.1 Business Policies	K0009; K0157; K0222;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts 5.1.a Asset management 5.1.c Mobile device management
18.2.2 Security Policy	K0009; K0157; K0222;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts 5.1.a Asset management 5.1.c Mobile device management
18.2.3 BYOD Policies	K0009; K0157; K0222;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts 5.1.a Asset management 5.1.c Mobile device management

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
18.2.4 Regulatory and Standards Compliance	K0009; K0157; K0222;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts 5.1.a Asset management 5.1.c Mobile device management
18.3 Understanding Defense Summary						
18.3.1 What Did I Learn in this Module?						
18.3.2 Module 18: Understanding Defense Quiz						
19.0 Introduction						
19.0.1 Why Should I Take this Module?						
19.0.2 What Will I Learn in this Module?						
19.1 Access Control Concepts						
19.1.1 Communications Security: CIA	K0007; K0033; K0056; K0158; K0488;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.1 Describe the CIA triad 1.3 Describe security terms 1.3.i Zero trust 1.6 Compare access control models 1.6.d Authentication, authorization, accounting
19.1.2 Zero Trust Security	K0007; K0033; K0056; K0158; K0488;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.1 Describe the CIA triad 1.3 Describe security terms 1.3.i Zero trust 1.6 Compare access control models 1.6.d Authentication, authorization, accounting
19.1.3 Access Control Models	K0007; K0033; K0056; K0158; K0488;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.1 Describe the CIA triad 1.3 Describe security terms 1.3.i Zero trust 1.6 Compare access control models 1.6.d Authentication, authorization, accounting
19.1.4 Check Your Understanding - Identify the Access Control Model	K0007; K0033; K0056; K0158; K0488;	HS-ETS1-3.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.1 Describe the CIA triad 1.3 Describe security terms 1.3.i Zero trust 1.6 Compare access control models 1.6.d Authentication, authorization, accounting
19.2 AAA Usage and Operation						
19.2.1 AAA Operation	K0007; K0033; K0056; K0158; K0488;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 1.6 Compare access control models 1.6.d Authentication, authorization, accounting

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
19.2.2 AAA Authentication	K0007; K0033; K0056; K0158; K0488;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 1.6 Compare access control models 1.6.d Authentication, authorization, accounting
19.2.3 AAA Accounting Logs	K0007; K0033; K0056; K0158; K0488;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 1.6 Compare access control models 1.6.d Authentication, authorization, accounting
19.2.4 Check Your Understanding - Identify the Characteristic of AAA	K0007; K0033; K0056; K0158; K0488;	HS-ETS1-3.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 1.6 Compare access control models 1.6.d Authentication, authorization, accounting
19.3 Access Control Summary						
19.3.1 What Did I Learn in this Module?						
19.3.2 Module 19: Access Control Quiz						
20.0 Introduction						
20.0.1 Why Should I Take this Module?						
20.0.2 What Will I Learn in this Module?						
20.1 Information Sources						
20.1.1 Network Intelligence Communities	K0312; K0352; K0358, K0409; K0460; K0462; K0593	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
20.1.2 Cisco Cybersecurity Reports	K0312; K0352; K0358, K0409; K0460; K0462; K0593	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
20.1.3 Security Blogs and Podcasts	K0094; K0312; K0352; K0358, K0409; K0460;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	K0462; K0593					
20.2 Threat Intelligence Services						
20.2.1 Cisco Talos	K0312; K0352; K0358, K0409; K0460; K0462; K0593	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.a Threat intelligence (TI) 1.3.j Threat intelligence platform (TIP)
20.2.2 FireEye	K0312; K0352; K0358, K0409; K0460; K0462; K0593	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.a Threat intelligence (TI) 1.3.j Threat intelligence platform (TIP)
20.2.3 Automated Indicator Sharing	K0312; K0352; K0358, K0409; K0460; K0462; K0593	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.a Threat intelligence (TI) 1.3.j Threat intelligence platform (TIP)
20.2.4 Common Vulnerabilities and Exposures (CVE) Database	K0005; K0312; K0352; K0358, K0409; K0460; K0462; K0593	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.a Threat intelligence (TI) 1.3.j Threat intelligence platform (TIP)
20.2.5 Threat Intelligence Communication Standards	K0312; K0352; K0358, K0409; K0460; K0462; K0593	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.a Threat intelligence (TI) 1.3.j Threat intelligence platform (TIP)
20.2.6 Threat Intelligence Platforms	K0312; K0352; K0358, K0409; K0460;	HS-ETS1-3.	ITEA.17.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.a Threat intelligence (TI) 1.3.j Threat intelligence platform (TIP)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	K0462; K0593					
20.2.7 Check Your Understanding - Identify the Threat Intelligence Information Source	K0312; K0352; K0358, K0409; K0460; K0462; K0593	HS-ETS1-3.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.a Threat intelligence (TI) 1.3.j Threat intelligence platform (TIP)
20.3 Threat Intelligence Summary						
20.3.1 Packet Tracer - Skills Integration Challenge						
20.3.2 Module 20: Threat Intelligence Quiz						
21.0 Introduction						
21.0.1 Why Should I Take this Module?						
21.0.2 What Will I Learn in this Module?						
21.0.3 Class Activity - Creating Codes		HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3B-NI-04; 3B-NI-04; 3B-DA-05;	
21.1 Integrity and Authenticity						
21.1.1 Securing Communications	K0019; K0196; K0403;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
21.1.2 Cryptographic Hash Functions	K0019; K0196; K0403;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
21.1.3 Cryptographic Hash Operation	K0019; K0196; K0403;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
21.1.4 MD5 and SHA	K0019; K0196; K0403;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.10 Describe the impact of certificates on

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
						security (includes PKI, public/private crossing the network, asymmetric/symmetric)
21.1.5 Origin Authentication	K0019; K0196; K0403;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
21.1.6 Lab – Hashing Things Out	K0019; K0196; K0403;	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)
21.2 Confidentiality						
21.2.1 Data Confidentiality	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.2 Symmetric Encryption	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.3 Asymmetric Encryption	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.4 Asymmetric Encryption - Confidentiality	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.5 Asymmetric Encryption - Authentication	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
						techniques, such as tunneling, encryption, and proxies
21.2.6 Asymmetric Encryption - Integrity	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.7 Diffie-Hellman	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.8 Video - Cryptography	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.9 Check Your Understanding - Classify the Encryption Algorithms	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.9.	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.10 Lab - Encrypting and Decrypting Data Using OpenSSL	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.11 Lab - Encrypting and Decrypting Data Using a Hacker Tool	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
21.2.12 Lab - Examining Telnet and SSH in Wireshark	K0049, K0211; K0295;	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.3 Describe the impact of these technologies on data visibility 2.3.e Encryption 2.9 Describe evasion and obfuscation

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
						techniques, such as tunneling, encryption, and proxies
21.3 Public Key Cryptography						
21.3.1 Using Digital Signatures	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric) 2.11 Identify the certificate components in a given scenario (a - e)
21.3.2 Digital Signatures for Code Signing	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric) 2.11 Identify the certificate components in a given scenario (a - e)
21.3.3 Digital Signatures for Digital Certificates	K0049, K0427, K0428	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric) 2.11 Identify the certificate components in a given scenario (a - e)
21.4 Authorities and the PKI Trust System						
21.4.1 Public Key Management	K0056;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.4.2 The Public Key Infrastructure	K0056;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.4.3 The PKI Authorities System	K0056;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.4.4 The PKI Trust System	K0056;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.4.5 Interoperability of Different PKI Vendors	K0056;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.4.6 Certificate Enrollment, Authentication, and Revocation	K0056;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.4.7 Lab – Certificate Authority Stores	K0056;	HS-ETS1-4.	ITEA.8.	CCR.ELA-Literacy.RST.11-12.3.	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.5 Applications and Impacts of Cryptography						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
21.5.1 PKI Applications	K0056;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.5.2 Encrypted Network Transactions	K0277; K0487;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.5.3 Encryption and Security Monitoring	K0277; K0487;	HS-ETS1-4.	ITEA.8.	IT 10	3B-NI-04; 3B-NI-04; 3B-DA-05;	2.11 Identify the certificate components in a given scenario (a - e)
21.6 Cryptography Summary						2.11 Identify the certificate components in a given scenario (a - e)
21.7.1 What Did I Learn in this Module?						2.11 Identify the certificate components in a given scenario (a - e)
21.7.2 Module 21: Public Key Cryptography Quiz						2.11 Identify the certificate components in a given scenario (a - e)
22.0 Introduction						
22.0.1 Why Should I Take this Module?						
22.0.2 What Will I Learn in this Module?						
22.1 Antimalware Protection						
22.1.1 Endpoint Threats	K0188; K0191; K0259;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.b Agentless and agent-based protections 1.3.c Malware analysis 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox) 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control
22.1.2 Endpoint Security	K0188; K0191; K0259;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.b Agentless and agent-based protections 1.3.c Malware analysis 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox) 4.1 Map the provided events to source technologies

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
						4.1.b Firewall 4.1.c Network application control
22.1.3 Host-Based Malware Protection	K0188; K0191; K0259;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.b Agentless and agent-based protections 1.3.c Malware analysis 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox) 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control
22.1.4 Network-Based Malware Protection	K0188; K0191; K0259;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.b Agentless and agent-based protections 1.3.c Malware analysis 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox) 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
22.1.5 Check Your Understanding - The Troubleshooting Process	K0188; K0191; K0259;	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.b Agentless and agent-based protections 1.3.c Malware analysis 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox) 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control
22.2 Host-Based Intrusion Prevention						
22.2.1 Host-Based Firewalls	K0046; K0324; K0472; K0488; K0630;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS
22.2.2 Host-Based Intrusion Detection	K0046; K0324; K0472; K0488; K0630;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS
22.2.3 HIDS Operation	K0046; K0324; K0472; K0488; K0630;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS
22.2.4 HIDS Products	K0046; K0324; K0472; K0488; K0630;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS
22.2.5 Check your Understanding - Identify the Host-Based Intrusion Protection Terminology	K0046; K0324; K0472; K0488; K0630;	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 4.1 Map the provided events to source technologies 4.1.a IDS/IPS

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
22.3 Application Security						
22.3.1 Attack Surface	K0009; K0070; K0324; K0624;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.1 Compare attack surface and vulnerability 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)
22.3.2 Application Block Listing and Allow Listing	K0009; K0070; K0324; K0624;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.1 Compare attack surface and vulnerability 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)
22.3.3 System-Based Sandboxing	K0009; K0070; K0324; K0624;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.1 Compare attack surface and vulnerability 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)
22.3.4 Video - Using a Sandbox to Launch Malware	K0009; K0070; K0324; K0624;	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.1 Compare attack surface and vulnerability 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring (a - e) 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)
22.4 Endpoint Protection Summary						
22.4.1 What Did I Learn in this Module?						
22.4.2 Module 22: Endpoint Protection Quiz						
23.0 Introduction						
23.0.1 Why Should I Take this Module?						
23.0.2 What Will I Learn in this Module?						
23.1 Network and Server Profiling						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
23.1.1 Network Profiling	K0540; K0550;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.g Sliding window anomaly detection 1.4 Compare security concepts 1.4.a Risk (risk scoring/risk weighting, risk reduction, risk assessment) 1.4.c Vulnerability 5.7 Identify these elements used for network profiling (a - d) 5.8 Identify these elements used for server profiling (a - e)
23.1.2 Server Profiling	K0540; K0550;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.g Sliding window anomaly detection 1.4 Compare security concepts 1.4.a Risk (risk scoring/risk weighting, risk reduction, risk assessment) 1.4.c Vulnerability 5.7 Identify these elements used for network profiling (a - d) 5.8 Identify these elements used for server profiling (a - e)
23.1.3 Network Anomaly Detection	K0480; S0280;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.g Sliding window anomaly detection 1.4 Compare security concepts 1.4.a Risk (risk scoring/risk weighting, risk reduction, risk assessment) 1.4.c Vulnerability 5.7 Identify these elements used for network profiling (a - d) 5.8 Identify these elements used for server profiling (a - e)
23.1.4 Network Vulnerability Testing	K0013; K0480, S0079	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.g Sliding window anomaly detection 1.4 Compare security concepts 1.4.a Risk (risk scoring/risk weighting, risk reduction, risk assessment) 1.4.c Vulnerability 5.7 Identify these elements used for network profiling (a - d) 5.8 Identify these elements used for server profiling (a - e)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
23.1.5 Check Your Understanding - Identify the Elements of Network Profiling	K0480, S0079	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.g Sliding window anomaly detection 1.4 Compare security concepts 1.4.a Risk (risk scoring/risk weighting, risk reduction, risk assessment) 1.4.c Vulnerability 5.7 Identify these elements used for network profiling (a - d) 5.8 Identify these elements used for server profiling (a - e)
23.2 Common Vulnerability Scoring System (CVSS)						
23.2.1 CVSS Overview	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.7 Describe terms as defined in CVSS (1.7 a - e)
23.2.2 CVSS Metric Groups	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.7 Describe terms as defined in CVSS (1.7 a - e)
23.2.3 CVSS Base Metric Group	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.7 Describe terms as defined in CVSS (1.7 a - e)
23.2.4 The CVSS Process	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.7 Describe terms as defined in CVSS (1.7 a - e)
23.2.5 CVSS Reports	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.7 Describe terms as defined in CVSS (1.7 a - e)
23.2.6 Other Vulnerability Information Sources	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.7 Describe terms as defined in CVSS (1.7 a - e)
23.2.7 Check Your Understanding - Identify CVSS Metrics	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.7 Describe terms as defined in CVSS (1.7 a - e)
23.3 Secure Device Management	K0013; K0040; K0402; K0536;					

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
23.3.1 Risk Management	K0002; K0038; K0048; K0074; K0214;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts (5.1 a - e)
23.3.2 Check Your Understanding - Identify the Risk Response	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST. 11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts (5.1 a - e)
23.3.3 Vulnerability Management	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts (5.1 a - e)
23.3.4 Asset Management	K0618; K0619;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts (5.1 a - e)
23.3.5 Mobile Device Management	K0070; K0269; K0438; S0075;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts (5.1 a - e)
23.3.6 Configuration Management	K0073; K0275;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts (5.1 a - e)
23.3.7 Enterprise Patch Management	K0074; K0625;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts (5.1 a - e)
23.3.8 Patch Management Techniques	K0074; K0625;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts (5.1 a - e)
23.3.9 Check Your Understanding - Identify Device Management Activities	K0013; K0040; K0402; K0536;	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST. 11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.1 Describe management concepts (5.1 a - e)
23.4 Information Security Management Systems						
23.4.1 Security Management Systems	K0074; K0276;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
23.4.2 ISO-27001	K0087;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
23.4.3 NIST Cybersecurity Framework	K0045; K0126;	HS-ETS1-4.	ITEA.10.	IT 08 2	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
23.4.4 Check Your Understanding - Identify the Stages in the NIST Cybersecurity Framework	K0045; K0126;	HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
23.5 Endpoint Vulnerability Assessment Summary		HS-ETS1-4.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
23.5.1 What Did I Learn in this Module?						
23.5.2 Module 23 - Endpoint Vulnerability Quiz						
24.0 Introduction						
24.0.1 Why Should I Take this Module?						
24.0.2 What Will I Learn in this Module?						
24.1 Monitoring Common Protocols						
24.1.1 Syslog and NTP	K0001; K0061; K0174; K0332; K0417; K0447; K0565;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
24.1.2 NTP	K0001; K0061; K0174; K0332; K0417; K0447; K0565;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
24.1.3 DNS	K0001; K0061; K0174; K0332; K0417; K0447; K0565;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
24.1.4 HTTP and HTTPS	K0001; K0061; K0174; K0332; K0417; K0447; K0565;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
24.1.5 Email Protocols	K0001; K0061; K0174; K0332; K0417; K0447; K0565;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
24.1.6 ICMP	K0001; K0061; K0174; K0332; K0417; K0447; K0565;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
24.1.7 Check Your Understanding - Identify the Monitored Protocol	K0001; K0061; K0174; K0332; K0417; K0447; K0565;	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	
24.2 Security Technologies						
24.2.1 ACLs	K0033; K0488;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.3 Describe the impact of these technologies on data visibility (a - h)
24.2.2 NAT and PAT	K0059; K0075	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.3 Describe the impact of these technologies on data visibility (a - h)
24.2.3 Encryption, Encapsulation, and Tunneling	K0059; K0076; K0196	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.3 Describe the impact of these technologies on data visibility (a - h)
24.2.4 Peer-to-Peer Networking and Tor	K0059; K0077	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.3 Describe the impact of these technologies on data visibility (a - h)
24.2.5 Load Balancing	K0059; K0078	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.3 Describe the impact of these technologies on data visibility (a - h)
24.2.6 Check Your Understanding - Identify the Impact of the Technology on Security and Monitoring	K0059; K0079	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-06; 3A-NI-07; 3A-NI-08;	2.3 Describe the impact of these technologies on data visibility (a - h)
24.3 Troubleshooting Commands						
24.3.1 What Did I Learn in this Module?						
24.3.2 Module Module 24: Technologies and Protocols Quiz						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
25.0 Introduction						
25.0.1 Why Should I Take this Module?						
25.0.2 What Will I Learn in this Module?						
25.1 Types of Security Data						
25.1.1 Alert Data	K0038; S0178; K0394;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.4 Describe the uses of these data types in security monitoring 2.4.a Full packet capture 2.4.b Session data 2.4.c Transaction data 2.4.d Statistical data 2.4.f Alert data
25.1.2 Session and Transaction Data	K0536; S0252; S0178; K0394;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.4 Describe the uses of these data types in security monitoring 2.4.a Full packet capture 2.4.b Session data 2.4.c Transaction data 2.4.d Statistical data 2.4.f Alert data
25.1.3 Full Packet Captures	K0062; K0394; K0301;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.4 Describe the uses of these data types in security monitoring 2.4.a Full packet capture 2.4.b Session data 2.4.c Transaction data 2.4.d Statistical data 2.4.f Alert data
25.1.4 Statistical Data	K0394; K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.4 Describe the uses of these data types in security monitoring 2.4.a Full packet capture 2.4.b Session data 2.4.c Transaction data 2.4.d Statistical data 2.4.f Alert data
25.1.5 Check Your Understanding - Identify Types of Network Monitoring Data	K0394; K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.4 Describe the uses of these data types in security monitoring 2.4.a Full packet capture 2.4.b Session data 2.4.c Transaction data 2.4.d Statistical data 2.4.f Alert data
25.2 End Device Logs						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
25.2.1 Host Logs	K0132; K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring 3.1.a Host-based intrusion detection 3.1.c Host-based firewall 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.d Proxy logs
25.2.2 Syslog	K0132; K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring 3.1.a Host-based intrusion detection 3.1.c Host-based firewall 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.d Proxy logs
25.2.3 Server Logs	K0132; K0363; K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring 3.1.a Host-based intrusion detection 3.1.c Host-based firewall 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.d Proxy logs
25.2.4 SIEM and Log Collection	K0132; K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring 3.1.a Host-based intrusion detection 3.1.c Host-based firewall 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.d Proxy logs

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
25.2.5 Check Your Understanding - Identify Windows Event Security Levels	K0132; K0536, S0252, S0270	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST. 11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.2 Compare security deployments 1.2.d SIEM, SOAR, and log management 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring 3.1.a Host-based intrusion detection 3.1.c Host-based firewall 4.1 Map the provided events to source technologies 4.1.a IDS/IPS 4.1.d Proxy logs
25.3 Network Logs	K0132; K0536, S0252, S0270					
25.3.1 Tcpdump	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
25.3.2 NetFlow	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)
25.3.3 Application Visibility and Control	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
25.3.4 Content Filter Logs	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)
25.3.5 Logging from Cisco Devices	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
25.3.6 Proxy Logs	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)
25.3.7 Next-Generation Firewalls	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
25.3.8 Check Your Understanding - Identify the Security Technology from the Data Description	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)
25.3.9 Check Your Understanding - Identify the NextGen Firewall Event Types	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
25.3.10 Packet Tracer - Explore a NetFlow Implementation	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)
25.3.11 Packet Tracer - Logging from Multiple Sources	K0132; K0447; K0452; K0516; K0487; K0536; S0252; S0270;	HS-ETS1-2.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.8 Identify the challenges of data visibility (network, host, and cloud) in detection 2.2 Identify the types of data provided by these technologies 2.2.a TCP dump 2.2.b NetFlow 2.2.c Next-gen firewall 2.2.e Application visibility and control 2.2.f Web content filtering 2.2.g Email content filtering 4.1 Map the provided events to source technologies 4.1.b Firewall 4.1.c Network application control 4.1.d Proxy logs 4.1.f Transaction data (NetFlow)
25.4 Network Security Data Summary						
25.4.1 What Did I Learn in this Module?						
25.4.2 Module 25: Network Security Data Quiz						
26.0 Introduction						
26.0.1 Why Should I Take this Module?						
26.0.2 What Will I Learn in this Module?						
26.1 Sources of Alerts						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
26.1.1 Security Onion	K0040;	HS-ETS1-3.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.10 - reference to 5-tuples of information 2.4 Describe the uses of these data types in security monitoring 2.4.f Alert data 4.9 Interpret common artifact elements from an event to identify an alert 4.9.a IP address (source / destination) 4.9.b Client and server port identity
26.1.2 Detection Tools for Collecting Alert Data	K0040;	HS-ETS1-3.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.10 - reference to 5-tuples of information 2.4 Describe the uses of these data types in security monitoring 2.4.f Alert data 4.9 Interpret common artifact elements from an event to identify an alert 4.9.a IP address (source / destination) 4.9.b Client and server port identity
26.1.3 Analysis Tools	K0040;	HS-ETS1-3.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.10 - reference to 5-tuples of information 2.4 Describe the uses of these data types in security monitoring 2.4.f Alert data 4.9 Interpret common artifact elements from an event to identify an alert 4.9.a IP address (source / destination) 4.9.b Client and server port identity
26.1.4 Alert Generation	K0040;	HS-ETS1-3.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.10 - reference to 5-tuples of information 2.4 Describe the uses of these data types in security monitoring 2.4.f Alert data 4.9 Interpret common artifact elements from an event to identify an alert 4.9.a IP address (source / destination) 4.9.b Client and server port identity
26.1.5 Rules and Alerts	K0040;	HS-ETS1-3.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.10 - reference to 5-tuples of information 2.4 Describe the uses of these data types in security monitoring 2.4.f Alert data 4.9 Interpret common artifact elements from an event to identify an alert 4.9.a IP address (source / destination) 4.9.b Client and server port identity

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
26.1.6 Snort Rule Structure	K0040;	HS-ETS1-3.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.10 - reference to 5-tuples of information 2.4 Describe the uses of these data types in security monitoring 2.4.f Alert data 4.9 Interpret common artifact elements from an event to identify an alert 4.9.a IP address (source / destination) 4.9.b Client and server port identity
26.1.7 Lab - Snort and Firewall Rules	K0040;	HS-ETS1-3.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.10 - reference to 5-tuples of information 2.4 Describe the uses of these data types in security monitoring 2.4.f Alert data 4.9 Interpret common artifact elements from an event to identify an alert 4.9.a IP address (source / destination) 4.9.b Client and server port identity
26.2 Overview of Alert Evaluation						
26.2.1 The Need for Alert Evaluation	K0040;	HS-ETS1-3.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.2 Compare impact and no impact for these items (a - e)
26.2.2 Evaluating Alerts	K0040;	HS-ETS1-3.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.2 Compare impact and no impact for these items (a - e)
26.2.3 Deterministic Analysis and Probabilistic Analysis	K0040;	HS-ETS1-3.	ITEA.10.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.2 Compare impact and no impact for these items (a - e)
26.2.4 Check your Understanding -- Identify Deterministic and Probabilistic Scenarios	K0040;	HS-ETS1-3.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.2 Compare impact and no impact for these items (a - e)
26.2.5 Check Your Understanding - Identify the Alert Classification	K0040;	HS-ETS1-3.	ITEA.10.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.2 Compare impact and no impact for these items (a - e)
26.3 Troubleshoot Common Network Problems Summary						
26.3.1 What Did I Learn in this Module?						
26.3.2 Module 26: Evaluating Alerts Quiz						
27.0 Introduction						
27.0.1 Why Should I Take this Module?						
27.0.2 What Will I Learn in this Module?						
27.1 A Common Data Platform						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
27.1.1 ELK	K0038; K0195; S0106; S0125; S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
27.1.2 Data Reduction	K0038; K0195; S0106; S0125; S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
27.1.3 Data Normalization	K0038; K0195; S0106; S0125; S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
27.1.4 Data Archiving	K0038; K0195; S0106; S0125; S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
27.1.5 Lab - Convert Data into a Universal Format	K0038; K0195; S0106; S0125; S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	
27.2 Investigating Network Data						
27.2.1 Working in Sguil	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.2 Sguil Queries	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.3 Pivoting from Sguil	K0236; K0278; K0338; K0364;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	S0079, S0252					event to identify an alert 4.9.d System (API calls)
27.2.4 Event Handling in Sguil	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.5 Working in ELK	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.6 Queries in ELK	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.7 Investigating Process or API Calls	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.8 Investigating File Details	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.9 Lab – Regular Expression Tutorial	K0236; K0278; K0338; K0364;	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	S0079, S0252					event to identify an alert 4.9.d System (API calls)
27.2.10 Lab - Extract an Executable from a PCAP	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.11 Video - Interpret HTTP and DNS Data to Isolate Threat Actor	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.12 Lab - Interpret HTTP and DNS Data to Isolate Threat Actor	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.13 Video - Isolate Compromised Host Using 5-Tuple	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.7.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.14 Lab - Isolate Compromised Host Using 5-Tuple	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.2.15 Lab - Investigate a Malware Exploit	K0236; K0278; K0338; K0364;	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
	S0079, S0252					event to identify an alert 4.9.d System (API calls)
27.2.16 Lab - Investigating an Attack on a Windows Host	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	4.6 Extract files from a TCP stream when given a PCAP file and Wireshark 4.7 Identify key elements in an intrusion from a given PCAP file (a - f) 4.9 Interpret common artifact elements from an event to identify an alert 4.9.d System (API calls)
27.3 Enhancing the Work of the Cybersecurity Analyst						
27.3.1 Dashboards and Visualizations	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.e Run book automation (RBA)
27.7.2 Workflow Management	K0236; K0278; K0338; K0364; S0079, S0252	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	1.3 Describe security terms 1.3.e Run book automation (RBA)
27.4 Working with Network Security Data Summary						
27.4.1 What Did I Learn in this Module?						
27.4.2 Module 27: Working with Network Security Data Quiz						
28.0 Introduction						
28.0.1 Why Should I Take this Module?						
28.0.2 What Will I Learn in this Module?						
28.1 Evidence Handling and Attack Attribution						
28.1.1 Digital Forensics	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
28.1.2 The Digital Forensics Process	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.1.3 Check Your Understanding - Identify the Steps in the Digital Forensics Process	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.1.4 Types of Evidence	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.1.5 Check Your Understanding - Identify the Type of Evidence	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.1.6 Evidence Collection Order	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.1.7 Chain of Custody	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
						image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.1.8 Data Integrity and Preservation	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.1.9 Attack Attribution	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.1.10 The MITRE ATT&CK Framework	K0017; K0133; K0304; K0573;	HS-ETS1-3.	ITEA.12.	IT 10	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	3.3 Describe the role of attribution in an investigation (a - e) 3.4 Identify type of evidence used based on provided logs (a - c) 3.5 Compare tampered and untampered disk image 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.2 The Cyber Kill Chain						
28.2.1 Steps of the Cyber Kill Chain	K0177; K0234;	HS-ETS1-4.	ITEA.13.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.2.2 Reconnaissance	K0177; K0234;	HS-ETS1-4.	ITEA.13.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
28.2.3 Weaponization	K0177; K0234;	HS-ETS1-4.	ITEA.13.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.2.4 Delivery	K0177; K0234;	HS-ETS1-4.	ITEA.13.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.2.5 Exploitation	K0177; K0234; K0440; K0481; K0507; K0522;	HS-ETS1-4.	ITEA.13.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.2.6 Installation	K0177; K0234;	HS-ETS1-4.	ITEA.13.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.2.7 Command and Control	K0177; K0234;	HS-ETS1-4.	ITEA.13.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.2.8 Actions on Objectives	K0177; K0234;	HS-ETS1-4.	ITEA.13.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.2.9 Check Your Understanding - Identify the Kill Chain Step	K0177; K0234;	HS-ETS1-4.	ITEA.13.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.3 The Diamond Model of Intrusion Analysis						

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
28.3.1 Diamond Model Overview	K0046; K0324; K0472;	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.3.2 Pivoting Across the Diamond Model	K0046; K0324; K0472;	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.3.3 The Diamond Model and the Cyber Kill Chain	K0046; K0324; K0472;	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.3.4 Check Your Understanding - Identify the Diamond Model Features	K0046; K0324; K0472;	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
28.4 Incident Response						
28.4.1 Establishing an Incident Response Capability	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.2 Check Your Understanding - Identify the Incident Response Plan Elements	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.3 Incident Response Stakeholders	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
						5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.4 NIST Incident Response Life Cycle	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.5 Preparation	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.6 Detection and Analysis	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.7 Containment, Eradication, and Recovery	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
						5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.8 Post-Incident Activities	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.9 Incident Data Collection and Retention	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.10 Reporting Requirements and Information Sharing	A0097	HS-ETS1-4.	ITEA.17.	IT 09	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.11 Check Your Understanding - Identify the Incident Handling Term	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.9.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d)

Module	NICE	NGSS	ITEA	DODEA	CSTA	Exam Objectives
						5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.4.12 Lab - Incident Handling	A0097	HS-ETS1-4.	ITEA.17.	CCR.ELA-Literacy.RST.11-12.3.	3A-NI-04; 3A-NI-05; 3A-NI-06; 3A-NI-08;	5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61 5.3 Apply the incident handling process (such as NIST.SP800-61) to an event 5.4 Map elements to these steps of analysis based on the NIST.SP800-61(a - d) 5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP80061) (a - d) 5.6 Describe concepts as documented in NIST.SP800-86 (a - d)
28.5 Digital Forensics and Incident Analysis and Response Summary						
28.5.1 What Did I Learn in this Module?						
28.5.2 Module 26: Evaluating Alerts Quiz						
28.6 Prepare for Your Exam and Launch Your Career!						
28.6.1 Certification Preparation and Discount Vouchers						
28.6.2 Career Resources and Employment Opportunities						