



TURN IT UP

CISCO *Live!*

#CiscoLive



The bridge to possible

Ignite your career in cybersecurity operations

Cisco's CyberOps Associate Certification

Akaki Shelia, Cisco CyberOps Exam Program Manager
BRKCR-2302

CISCO *Live!*

#CiscoLive



CISCO *Live!*

Job Opportunities Outpace the Number of Qualified Candidates

3.5M cybersecurity
job openings by 2021



Agenda

- Introduction
- Certification Overview
- How to Prepare for the Exam
- Exam Topics
- Sample Question
- Conclusion

Cisco Certifications

Associate Level

Professional Level

Expert Level

Engineering



Software



CyberOps



World of Infrastructure Engineers



Automation

Software-defined infrastructure programmability



Multi-Cloud

New expectations for speed, scale, and security



AI/ML and Business Insights

For increased performance, reliability, and security

World of Software Developers



Application Economy

Speed of development, shift from IT to LOB, cloud offers quick and easy



Internet of Things

Connectivity increases value, edge computing and analytics



DevOps and Cloud

Powerful developer tools, APIs and open source, CI/CD and DevOps are enablers

World of Cybersecurity Operations



Threat management

Monitoring, analysis, and response, before, during, and after attacks



Security Orchestration and Automation Response (SOAR)

Aligns threat management, response, and automation



Security Incident Event Management (SIEM)

Real-time visibility and automatic notifications

Cisco's Associate Certifications

Associate Level

Knowledge Domains

Engineering



- Network fundamentals
- Network access
- IP connectivity and services
- Security fundamentals
- Automation and programmability

Software



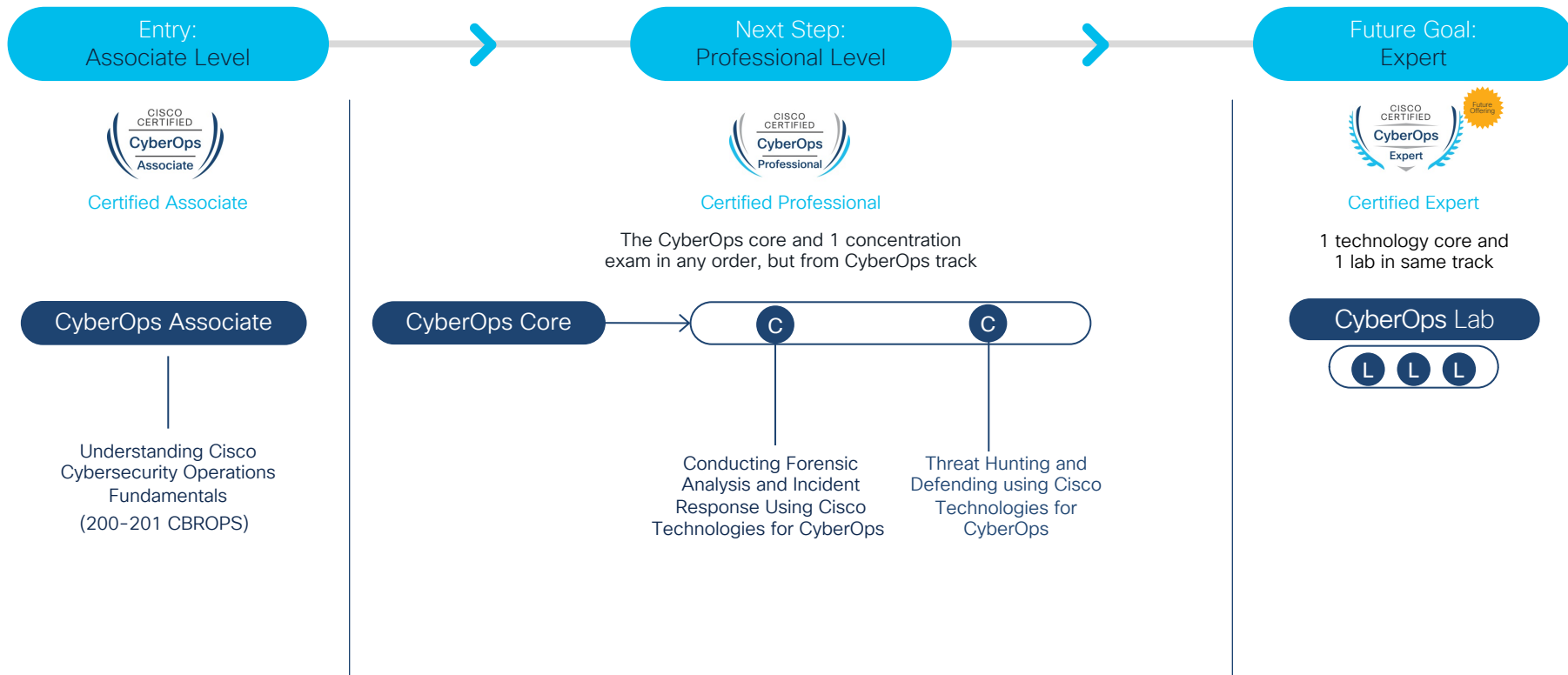
- Understanding and Using APIs
- Software Development and Design
- Application Deployment and Security
- Infrastructure and Automation
- Network Fundamentals

CyberOps



- Security Concepts
- Security Monitoring
- Host-Based Analysis
- Network Intrusion Analysis
- Security Policies and Procedures

Cisco CyberOps Certification Track



Recertification Options



- 1 Take an exam
- 2 Complete continuing education activities, such as:
 - Attend Cisco Live sessions
 - Complete online training courses
 - Complete instructor-led training
 - Within 3 years of cert date
- 3 Or a mix of both!

<https://www.cisco.com/c/en/us/training-events/training-certifications/recertification-policy.html>

How to prepare for the exam



Exam Blueprint:

CyberOps Associate Exam (200-201)

<https://learningnetwork.cisco.com/s/cbrops-exam-topics>

Task
Verbs

Understanding Cisco Cybersecurity Operations Fundamentals v1.0 (200-201)

Exam Description: The Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) exam is a 120-minute assessment that is associated with the Cisco Certified CyberOps Associate certification. The CBROPS exam tests a candidate's knowledge and skills related to security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures. The course, Understanding Cisco Cybersecurity Operations Fundamentals, helps candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

- 20%
- 1.0 **Security Concepts**
 - 1.1 Describe the CIA triad
 - 1.2 Compare security deployments
 - 1.2.a Network, endpoint, and application security systems
 - 1.2.b Agentless and agent-based protections
 - 1.2.c Legacy antivirus and antimalware
 - 1.2.d SIEM, SOAR, and log management
 - 1.3 Describe security terms
 - 1.3.a Threat intelligence (TI)
 - 1.3.b Threat hunting
 - 1.3.c Malware analysis
 - 1.3.d Threat actor
 - 1.3.e Run book automation (RBA)
 - 1.3.f Reverse engineering
 - 1.3.g Sliding window anomaly detection
 - 1.3.h Principle of least privilege
 - 1.3.i Zero trust
 - 1.3.j Threat intelligence platform (TIP)

Blueprint Verbs

What level is each task – depth of knowledge

Design

Troubleshoot

Configure

Describe

Exam preparation on the Cisco Learning Network

<https://learningnetwork.cisco.com/s/cyberops-associate>



Cisco Certified CyberOps Associate Certification and Training

The new Cisco Certified CyberOps Associate program focuses on the latest operational skills and knowledge you need for real-world jobs in security operations centers (SOCs). SOC analysts serve as the front line of defense against cybersecurity threats - preventing and detecting threats to defend your organization. Certification as a cybersecurity operations associate validates your skills in this vital function.

Exam

Discussions

Webinars & Videos

Additional Resources

Required Exams

200-201 CBROPS: Understanding Cisco Cybersecurity Operations Fundamentals

The Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) exam is a 120-minute assessment for the Cisco Certified CyberOps Associate certification and is aligned with the associate-level cybersecurity operations analyst job role. The CBROPS exam tests a candidate's knowledge and skills related to security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures. The course, Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS), helps candidates to prepare for this exam.





Exam Topics

Study Material

More Details

CyberOps Training Videos

The Cisco Learning Network





   


Certifications ▾ Communities ▾ Webinars & Videos ▾ Study Resources ▾ About/Help ▾ Store

Cisco Certified CyberOps Training Videos


Welcome to the Cisco Certified CyberOps Associate Training Videos page. Here you will find listings for upcoming webinars and a collection of free recordings from previous webinars conducted on the Cisco Learning Network.

All upcoming events

Share    




Jul 14




Outbound functionality:
DLP (AMER/EMEAR)

Jul 14, 2020
08:00 AM To 09:00 AM
EST
Webex




Jul 15




Outbound functionality:
DLP (APJ/GCT)

Jul 14, 2020
10:00 PM To 11:00 PM
EST
Webex



Jul 16




AMP for Endpoints
Protection Lattice
(AMER/EMEAR)

Jul 16, 2020
08:00 AM To 09:00 AM
AMT
Webex

Page 1 / 4 [Previous](#) [Next](#)

Training videos



Cisco Certified CyberOps Associate

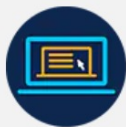
<https://learningnetwork.cisco.com/s/cyberops-associate-training-videos>

Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0

www.cisco.com/go/vILT

What you'll learn in this course

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) v1.0 course teaches you security concepts, common network and application operations and attacks, and the types of data needed to investigate security incidents. This course teaches you how to monitor alerts and breaches, and how to understand and follow established procedures for response to alerts converted to incidents. Through a combination of lecture, hands-on labs, and self-study, you will learn the essential skills, concepts, and technologies to be a contributing member of a cybersecurity operations center (SOC) including understanding the IT infrastructure, operations, and vulnerabilities. This course helps you prepare for the Cisco Certified CyberOps Associate certification and the role of a Junior or Entry-level cybersecurity operations analyst in a SOC.



Buy e-learning



Find a class



Private group training



Take your exam from home!

<https://www.cisco.com/go/onlineTesting>

CyberOps Associate

200-201

- Single
- 120-minute exam tests entry level developer skills

Domains

- Security Concepts
- Security Monitoring
- Host-Based Analysis
- Network Intrusion Analysis
- Security Policies and Procedures

CyberOps Associate

Domain

Security Concepts

Tasks

- 1.1 Describe the CIA triad
- 1.2 Compare security deployments
- 1.3 Describe security terms
- 1.4 Compare security concepts
- 1.5 Describe the principles of the defense-in-depth strategy
- 1.6 Compare access control models
- 1.7 Describe terms as defined in CVSS
- 1.8 Identify the challenges of data visibility (network, host, and cloud) in detection
- 1.9 Identify potential data loss from provided traffic profiles
- 1.10 Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs
- 1.11 Compare rule-based detection vs. behavioral and statistical detection

1.4 – Compare Security Concepts



RISK
WEAK PASSWORD



THREAT
STOLEN CREDENTIAL



VULNERABILITY
SYSTEM ACCESS USING
STOLEN CREDENTIALS



EXPLOIT
DICTIONARY ATTACK

Let's see what we learned

Drag and drop the security concept on the left onto the example of that concept on the right.

Threat

Risk Reduction

Vulnerability

Exploit

password enforcement policy

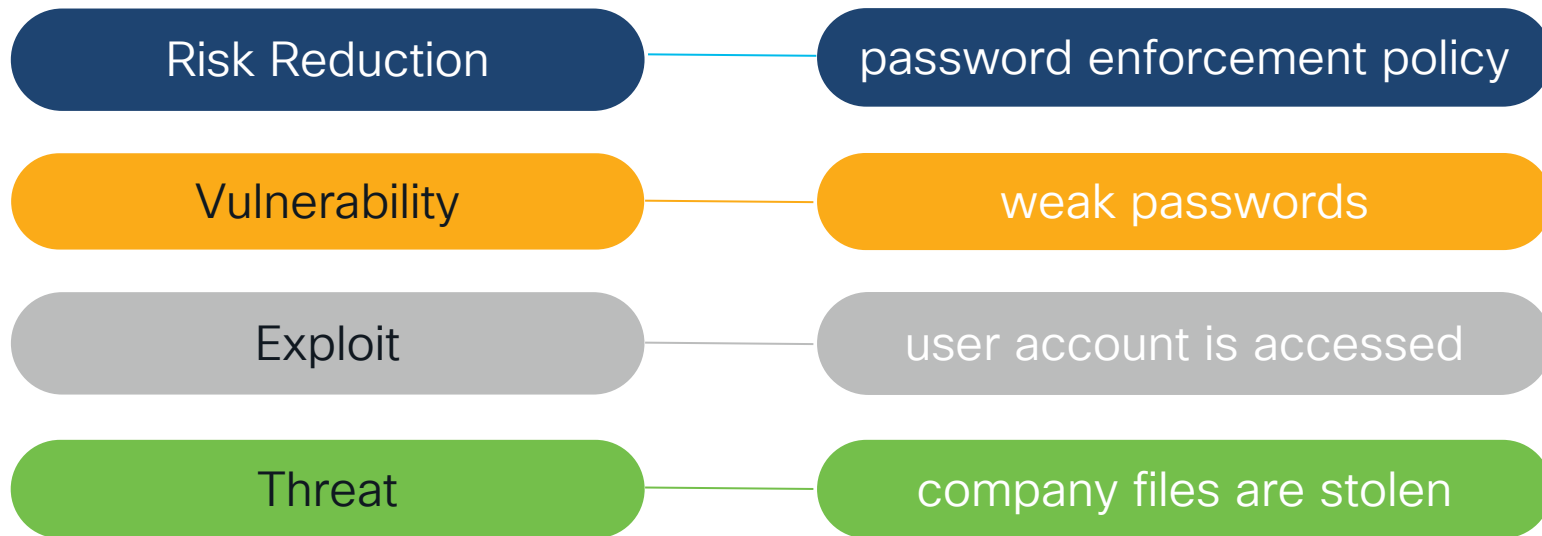
weak passwords

user account is accessed

company files are stolen

Let's see what we learned

Drag and drop the security concept on the left onto the example of that concept on the right.



1.5 – Describe the principles of the defense-in-depth strategy



A business realizes an attack has occurred and the business needs to secure their network.

1.5 – Describe the principles of the defense-in-depth strategy



Think first, then execute



Enact emergency response plan



Start containment



Turn on defense-in-depth tools



Enforcement



Recovery

What is the principle of defense-in-depth?

1

using tools to
recover infected
devices

2

using multiple
layers of
protection with
alerting

3

using firewalls
to alert and
secure the
network

4

using security
policies to
maintain strong
passwords

What is the principle of defense-in-depth?

1

using tools to
recover infected
devices

2

using multiple
layers of
protection with
alerting

3

using firewalls
to alert and
secure the
network

4

using security
policies to
maintain strong
passwords

1.8 – Identify the challenges of data visibility in detection



CLOUD TOOLS



TRUSTING 3RD PARTIES
BUT LACK VISIBILITY



HAVE YOUR TOOLS
INSIDE TO PROTECT

CyberOps Associate

Domain

Security Monitoring

Tasks

- 2.1 Compare attack surface and vulnerability
- 2.2 Identify the types of data provided by these technologies
- 2.3 Describe the impact of these technologies on data visibility
- 2.4 Describe the uses of these data types in security monitoring
- 2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle
- 2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting
- 2.7 Describe social engineering attacks
- 2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware
- 2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies
- 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

2.1 Compare attack surface and vulnerability



Attack surface



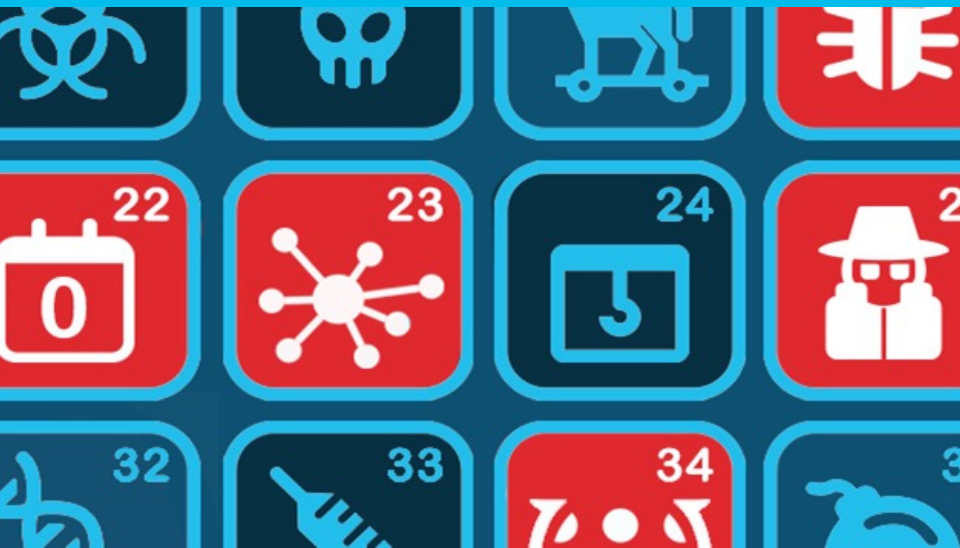
Vulnerability

2.6 Describe Web Application Attacks

SQL Injection

Command Injections

Cross-Site Scripting



SQL Injection

This HTML form solicits login information from an application user:

```
<form action="/cgi-bin/login" method=post>
```

```
Username: <input type=text name=username>
```

```
Password: <input type=password name=password>
```

```
<input type=submit value=Login>
```

User enters information and browser submits a strong:

```
username=submittedUser&password=submittedPassword
```

If an application accepts user-supplied data without any validation, an attacker could submit a maliciously crafted username and password:

```
username=admin%27%29+--+&password=+
```

Once this string is received and URL-decoded, the app will attempt to build a SQL:

```
select * from Users where (username = 'admin') -- and password = ' ')
```


Command Injection

```
int main(char* argc, char** argv) {  
    char cmd[CMD_MAX] = "/usr/bin/cat ";  
    strcat(cmd, argv[1]);  
    system(cmd);  
}
```

Cross-Site Scripting

Enter a new URL to shrink

URL:

Optional custom keyword:

Enter a new URL to shrink

URL:

Optional custom keyword:

The diagram uses red arrows and numbers to show the attack flow. A red arrow points from the 'Optional custom keyword' field in Step 1 to the 'URL' field in Step 2. Another red arrow points from the 'Optional custom keyword' field in Step 2 to the 'URL' field in Step 1. A large red number '1' is next to Step 1, and a large red number '2' is next to Step 2.

CyberOps Associate

Domain

Host-Based Analysis

Tasks

- 3.1 Describe the functionality of these endpoint technologies in regard to security monitoring
- 3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario
- 3.3 Describe the role of attribution in an investigation
- 3.4 Identify type of evidence used based on provided logs
- 3.5 Compare tampered and untampered disk image
- 3.6 Interpret operating system, application, or command line logs to identify an event
- 3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)

3.1 Endpoint Technologies



Host-based
intrusion detection



Antimalware &
Antivirus



Host-based firewall



Application-level
allow listing and
block listing



Systems-based
sandboxing

Host-based Intrusion Detection



Intrusion detection is the ability to detect attacks against a network . The network can be made up of network devices such as routers, printers, firewalls, and servers. Intrusion protection should provide the following active defense mechanisms:

- Detection – Identifies malicious attacks
- Prevention – Stops the detected attack from executing.
- Reaction – Immunizes the system from future attacks.

Host-based intrusion detection system (HIDS)

A host-based intrusion detection system (HIDS) audits host log files and host file systems and resources. An advantage of HIDS is that it can monitor operating system processes and protect critical system resources. This means it can notify network managers when some external process tries to modify a system file in a way that may include a hidden back door program.

Anti-malware



One of the largest threats to an endpoint is malware. Malware can come from many sources, but often it gets onto a device when users click a link from an email or the web. Once inside your environment, malware seeks to infect as much data and as many processes as it can. Viruses, ransomware, spyware, worms are examples of common malware.

Endpoint technologies protect endpoints by preventing malware from getting onto the environment. Anti-malware capabilities include"

- Machine learning – leveraging large-scale data to determine the malicious nature of files.
- Threat intelligence – leveraging both historical and real-time data from threats to automatically block known malefactors.
- Sandboxing – isolating suspect files into a safe environment.

Host-based Firewalls



Firewalls monitor incoming and outgoing network traffic and decide whether to allow or block specific traffic based on a defined set of security rules.

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet. A firewall can be hardware, software, or both.

3.3 Describe the role of attribution in an investigation

- Assets
- Threat actor
- Indicators of compromise
- Indicators of attack
- Chain of custody

CyberOps Associate

Domain

Network Intrusion Analysis

Tasks

- 4.1 Map the provided events to source technologies
- 4.2 Compare impact and no impact for these items
- 4.3 Compare deep packet inspection with packet filtering and stateful firewall operation
- 4.4 Compare inline traffic interrogation and taps or traffic monitoring
- 4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic
- 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
- 4.8 Interpret the fields in protocol headers as related to intrusion analysis
- 4.9 Interpret common artifact elements from an event to identify an alert
- 4.10 Interpret basic regular expressions

4.1 Map the provided events to source technologies

Event Sources:

- Firewalls
- IPS
- AAA Servers
- DNS
- DHCP
- Netflow

Firewall



Firepower Management Center

Analysis / Connections / Security Intelligence Events

Overview

Analysis

Policies

Devices

Objects

AMP

Intelligence



Deploy



admin ▾

[Bookmark This Page](#) | [Reporting](#) | [Dashboard](#) | [View Bookmarks](#) | [Search](#)

Security Intelligence Events [\(switch workflow\)](#)

2020-09-14 14:40:00 - 2020-09-15 15:46:00

Static

No Search Constraints [\(Edit Search\)](#)

Security Intelligence with Application Details

Table View of Security Intelligence Events

Jump to...

	<input type="checkbox"/>	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client
▼	<input type="checkbox"/>	2020-09-14 19:23:17	2020-09-14 19:23:20	Allow	IP Monitor	192.168.1.194		193.29.15.129	RUS	TID IPv4 Monitor			8 (Echo Request) / icmp	0 (No Code) / icmp	<input type="checkbox"/> ICMP	<input type="checkbox"/> ICMP c
▼	<input type="checkbox"/>	2020-09-14 19:23:03	2020-09-14 19:23:08	Allow	IP Monitor	192.168.1.150		193.29.15.129	RUS	TID IPv4 Monitor			8 (Echo Request) / icmp	0 (No Code) / icmp	<input type="checkbox"/> ICMP	<input type="checkbox"/> ICMP c
▼	<input type="checkbox"/>	2020-09-14 19:22:12	2020-09-14 19:22:26	Allow	IP Monitor	192.168.1.150		88.166.23.127	FRA	TID IPv4 Monitor			8 (Echo Request) / icmp	0 (No Code) / icmp	<input type="checkbox"/> ICMP	<input type="checkbox"/> ICMP c
▼	<input type="checkbox"/>	2020-09-14 19:22:01	2020-09-14 19:22:06	Allow	IP Monitor	192.168.1.194		88.166.23.127	FRA	TID IPv4 Monitor			8 (Echo Request) / icmp	0 (No Code) / icmp	<input type="checkbox"/> ICMP	<input type="checkbox"/> ICMP c
▼	<input type="checkbox"/>	2020-09-14 19:20:17		Allow	DNS Monitor	192.168.1.150		10.83.48.30		TID Domain Name Monitor			60845 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:20:02		Allow	DNS Monitor	192.168.1.150		10.83.48.30		TID Domain Name Monitor			35636 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:19:51		Allow	DNS Monitor	192.168.1.194		10.83.48.30		TID Domain Name Monitor			44059 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:19:46		Allow	DNS Monitor	192.168.1.150		10.83.48.30		TID Domain Name Monitor			58691 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:19:31		Allow	DNS Monitor	192.168.1.150		10.83.48.30		TID Domain Name Monitor			40524 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:19:16		Allow	DNS Monitor	192.168.1.150		10.83.48.30		TID Domain Name Monitor			60617 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:19:00		Allow	DNS Monitor	192.168.1.150		10.83.48.30		TID Domain Name Monitor			41503 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:18:37		Allow	DNS Monitor	192.168.1.194		10.83.48.30		TID Domain Name Monitor			53529 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:06:50		Allow	DNS Monitor	192.168.1.150		10.83.48.30		TID Domain Name Monitor			60791 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:06:34		Allow	DNS Monitor	192.168.1.150		10.83.48.30		TID Domain Name Monitor			51452 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli
▼	<input type="checkbox"/>	2020-09-14 19:06:19		Allow	DNS Monitor	192.168.1.150		10.83.48.30		TID Domain Name Monitor			59635 / udp	53 (domain) / udp	<input type="checkbox"/> DNS	<input type="checkbox"/> DNS cli



Netflow

<div> <div>Filter</div> <div> <div>Domain</div> <div>Client or Server Host Group : DMZ</div> </div> <div> <div>: Default Domain</div> <div></div> </div> <div> <div>Direction : Inbound</div> <div></div> </div> <div> <div>Time</div> <div>: From Oct 19, 2015 4:58:00 AM to Oct 19, 2015 4:59:00 AM</div> </div> </div> <div> <div>«</div> <div>»</div> <div>C</div> </div>									
Top Conversations - 12 records									
#	% of Bytes	Host	Host Role	Peer	Port	Average Traffic (bps)	Bytes	Flows	Host Bytes Ratio
1	98.83% <div></div>	10.3.1.120	Server	10.3.2.202	80/tcp (http)	3.42M	24.48M	1	27.86% <div></div>
2	0.57% <div></div>	10.3.1.110	Server	241.88.180.189	443/tcp (https)	19.91k	145.86k	1	0% <div></div>
3	0.57% <div></div>	10.3.1.110	Server	135.234.152.130	443/tcp (https)	19.75k	144.69k	1	0% <div></div>
4	0.02% <div></div>	10.3.1.150	Server	10.100.12.22	8000/tcp (VMware-vMotion)	755	5.53k	1	48.83% <div></div>
5	<0.01% <div></div>	10.3.1.201	Server	10.100.12.22	3389/tcp (remote-desktop)	75	567	1	63.37% <div></div>
6	<0.01% <div></div>	10.3.1.201	Server	10.1.1.4	icmp	67	504	1	0% <div></div>
7	<0.01% <div></div>	10.3.1.201	Server	10.1.1.1	icmp	37	280	1	0% <div></div>
8	<0.01% <div></div>	lancope-smc1 (10.3.1.100)	Client	google-public-dns-a.googl (8.8.8.8)	53/udp (dns)	9	138	1	50% <div></div>
9	0% <div></div>	10.3.1.201	Client	qj-in-f139.1e100.net (173.194.206.139)	80/tcp (http)			1	100% <div></div>

4.2 Compare impact and no impact for these items

- False positive
- False negative
- True positive
- True negative

CyberOps Associate

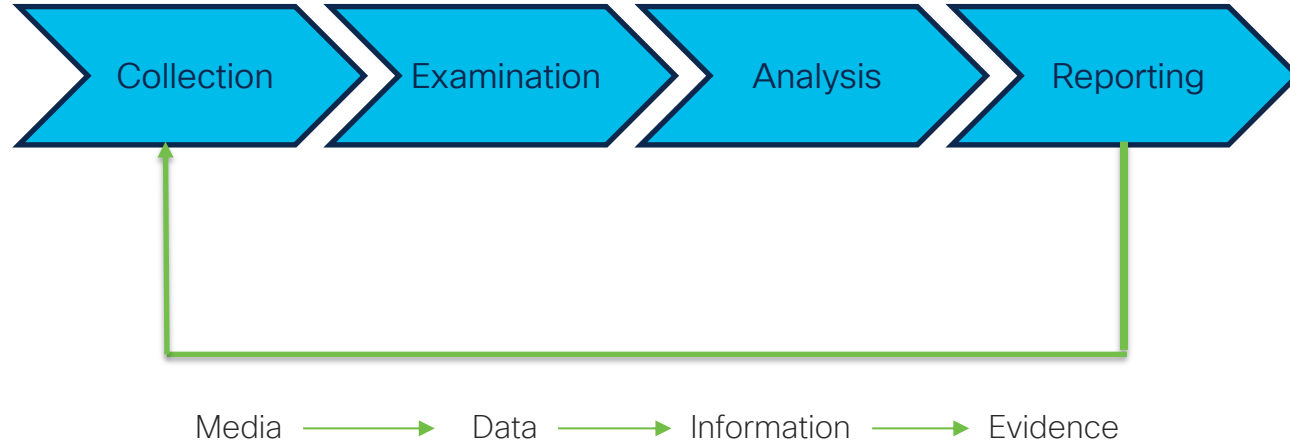
Domain

Security Policies and Procedures

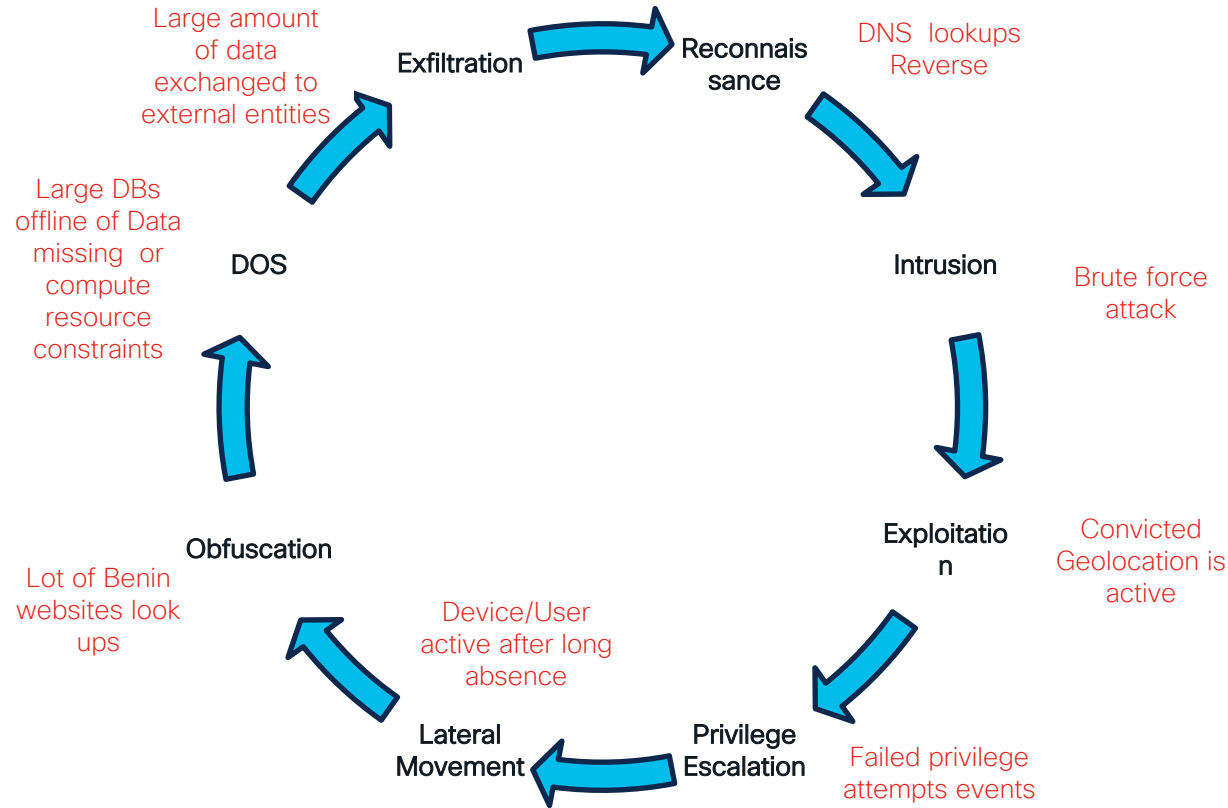
Tasks

- 5.1 Describe management concepts
- 5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61
- 5.3 Apply the incident handling process to an event
- 5.4 Map elements to these steps of analysis based on the NIST.SP800-61 Compare controller-level to device-level management
- 5.5 Map the organization stakeholders against the NIST IR categories
- 5.6 Describe concepts as documented in NIST.SP800-86
- 5.7 Identify these elements used for network profiling
- 5.8 Identify these elements used for server profiling
- 5.9 Identify protected data in a network
- 5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion
- 5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

5.6 Describe concepts as documented in NIST.SP800-86



5.10 Classify intrusion events into categories



CyberOps Associate

200-201

- Single
- 120-minute exam tests entry level developer skills

Domains

- Security Concepts
- Security Monitoring
- Host-Based Analysis
- Network Intrusion Analysis
- Security Policies and Procedures



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive





TURN IT UP

CISCO *Live!*

#CiscoLive