BOARD INFINITY

COURSE 1 OF 3 · CYBERSECURITY FUNDAMENTALS WITH CISCO TOOLS SPECIALIZATION

Understanding Cisco Cybersecurity Operations Fundamentals

Full course syllabus - every module, video lesson, reading and assignment, from the CIA triad to SIEM, incident response and network defense.

Board Infinity
Instructor · Offered on Coursera

3	36	12	1 week
Modules	Video lessons	Assignments	At 10 hours a week

INSIDE THE COURSE

01	Introduction to Cybersecurity Concepts	4 hours to complete
02	Security Monitoring and Response	4 hours to complete
03	Host and Network Security	4 hours to complete

Enroll on Coursera

https://www.coursera.org/learn/cisco-cybersecurity-operations-essentials

01 ABOUT THE COURSE

From the CIA triad to incident response.

Understanding Cisco Cybersecurity Operations Fundamentals gives you the foundational skills to detect and respond to threats in a modern security operation. Across three modules you build a grounding in core cybersecurity concepts, learn how security teams monitor and respond to incidents, and put host and network security measures to work.

Everything is delivered through short video lectures, readings and graded quizzes - 36 videos, 9 readings and 12 assignments in all. No prior cybersecurity experience is required, though basic familiarity with IT systems is beneficial.

WHO IT'S FOR

Aspiring cybersecurity professionals
Starting out in security - no prior cybersecurity experience is required.

IT professionals
Expanding their skills into security monitoring and incident response.

Students
Building a foundation in cybersecurity operations and threat detection.

Future SOC analysts
Preparing for entry-level cybersecurity operations roles.

WHAT YOU'LL LEARN

01 **Explain core cybersecurity concepts** Module 1
Explain key cybersecurity concepts, including the CIA triad, defense-in-depth, and threat landscapes

02 **Detect and evaluate security incidents** Modules 1-2
Identify and evaluate security incidents using SIEM tools, log analysis, and network monitoring

03 **Respond with a proven process** Module 2
Follow NIST-based incident response, separate false positives from true incidents, and plan mitigation

04 **Secure hosts and networks** Module 3
Implement host and network security measures, including firewalls, IDS/IPS, and endpoint security tools

02 SYLLABUS

Three modules, one security operations toolkit.

1 week to complete at 10 hours a week. Flexible schedule - learn at your own pace.

01 Introduction to Cybersecurity Concepts

Fundamentals, security technologies and threat detection

4 hours
12 videos

BY THE END OF THIS MODULE YOU CAN

- Explain cybersecurity, its key terms, the CIA triad and defense-in-depth
- Describe cybersecurity roles, ethical considerations and legal aspects
- Explain network and endpoint security, SIEM and cloud security essentials
- Identify attack vectors and apply basic intrusion and threat detection

CONTENTS: 12 videos (85 min) · 3 readings (30 min) · 4 assignments (105 min) · 1 plugin (15 min)

TOPICS: Cybersecurity Fundamentals · Security Technologies and Deployments · Threat Detection Techniques · Quick Course Check-In (plugin)

You'll leave with: a grounding in the core concepts, security technologies and threat detection techniques every security operation relies on.

02 Security Monitoring and Response

Data sources, incident response and threat mitigation

4 hours
12 videos

BY THE END OF THIS MODULE YOU CAN

- Identify security data sources and explain visibility and data collection
- Explain monitoring challenges like encryption and proxies, and threat hunting
- Apply NIST incident response and evaluate incidents through log analysis
- Use SIEM, Wireshark, host-based tools and basic malware analysis

CONTENTS: 12 videos (81 min) · 3 readings (30 min) · 4 assignments (105 min)

TOPICS: Security Data Sources · Incident Analysis and Response · Threat Mitigation Tools

You'll leave with: a working process for monitoring, evaluating and responding to security incidents - from the first alert to post-incident action.

03

Host and Network Security

Host defenses, network analysis and security policy

4 hours

12 videos

BY THE END OF THIS MODULE YOU CAN

- ✓ Apply antivirus, anti-malware and host-level intrusion detection/prevention
- ✓ Harden operating systems and apply application whitelisting and blacklisting
- ✓ Analyze network traffic and protocols, and spot network-based attack patterns
- ✓ Develop security policies, response and recovery plans, and continuous monitoring

CONTENTS 12 videos (84 min) · 3 readings (30 min) · 4 assignments (105 min)

TOPICS Host-Based Security Fundamentals | Network Security Analysis | Security Policies and Procedures

You'll leave with: the practical measures to secure hosts and networks, plus the policies, monitoring and training that keep an organization protected.

03 TOOLS & SKILLS

The themes that run through the course.

Cybersecurity fundamentals — Core theme

The CIA triad, defense-in-depth and the threat landscape - the thread through all three modules.
In this course: Module 1 builds the key terms, roles, ethics and legal aspects.

SIEM & log analysis — Monitoring

Security information and event management, log management and log analysis.
In this course: Modules 1 and 2, alongside threat hunting and NIST incident response.

Firewalls, IDS/IPS & endpoint security — Defenses

The host and network controls that detect, prevent and contain attacks.
In this course: Modules 1 and 3 - firewalls, IDS/IPS, antivirus, HIDS and OS hardening.

Packet & malware analysis — Analysis tools

Wireshark basics, traffic and protocol analysis, and basic malware analysis.
In this course: Introduced in Module 2, applied to network assessments in Module 3.

SKILLS YOU LEAVE WITH

Security foundations

- CIA triad & defense-in-depth
- Threat landscape & attack vectors
- Cybersecurity roles & ethics
- Cloud security essentials

Monitoring & response

- SIEM & log analysis
- Threat hunting
- NIST incident response
- False positives vs. true incidents

Network defense

- Firewalls & IDS/IPS
- Endpoint & malware protection
- Network traffic analysis
- Security policies & continuous monitoring

04 CERTIFICATE & CAREER

Finish with a shareable certificate.

Add it to LinkedIn
Add this credential to your LinkedIn profile, resume, or CV.

Share it anywhere
Share it on social media and in your performance review.

Earned, not attended
Awarded on completion of the graded quizzes in all three modules.

Course 1 of 3
Part of the Cybersecurity Fundamentals with Cisco Tools Specialization from Board Infinity.

ENTRY-LEVEL ROLES THESE SKILLS SUPPORT

SOC Analyst (Tier 1) · Cybersecurity Analyst · Incident Response Analyst · Security Monitoring Analyst · Network Security Analyst · Threat Intelligence Analyst

Board Infinity
Instructor · Offered on Coursera

Beginner level · Taught in English · 3 languages available · Flexible schedule

Ready to step into security operations?

Enrollment, lessons, grading and the certificate all happen on Coursera.

Enroll on Coursera

Course page: coursera.org/learn/cisco-cybersecurity-operations-essentials

Want a coach alongside the course?

Board Infinity 1:1 coaching is a separate, optional Board Infinity offering - it is not part of the Coursera course.
Details: https://www.boardinfinity.com/career-coaching/

Board Infinity is an independent education provider. Coursera and the Coursera logo are trademarks of Coursera, Inc. Cisco is a trademark of Cisco Systems, Inc. This independent educational resource is for informational and educational purposes only and is not affiliated with, endorsed by, sponsored by, or officially associated with Cisco Systems or any other company, organization, or certification body unless explicitly stated.