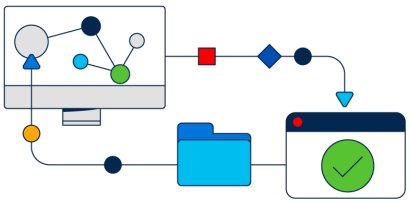

200-201 CBROPS Exam Topics Customize Your Study Plan

To earn your CyberOps Associate certification, you must pass the **200-201 CBROPS** exam. This 120-minute exam tests your knowledge of security concepts, security monitoring, host-based analysis, network intrusion analysis, and security policies and procedures.

The following topics are likely to be included on the **200-201 CBROPS** exam. The topics are subject to change at any time to reflect the latest technologies aligned to Cisco's products.

Cisco Cert Prep Tip: Print out this document and use it as you assess your strengths and challenges in preparing your study plan.

Exam Topics:

Section: 1.0 Security Concepts

1.1 Describe the CIA triad	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
1.2 Compare security deployments	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
1.2.a Network, endpoint, and application security systems	Y / N			☐
1.2.b Agentless and agent-based protections	Y / N			☐
1.2.c Legacy antivirus and antimalware	Y / N			☐
1.2.d SIEM, SOAR, and log management	Y / N			☐
1.3 Describe security terms	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
1.3.a Threat intelligence (TI)	Y / N			☐
1.3.b Threat hunting	Y / N			☐
1.3.c Malware analysis	Y / N			☐
1.3.d Threat actor	Y / N			☐
1.3.e Run book automation (RBA)	Y / N			☐

1.3 Describe security terms cont.	Need to Study?	Complete by:	Resource:	Completed
1.3.f Reverse engineering	Y / N			☐
1.3.g Sliding window anomaly detection	Y / N			☐
1.3.h Principle of least privilege	Y / N			☐
1.3.i Zero trust	Y / N			☐
1.3.j Threat intelligence platform (TIP)	Y / N			☐
1.4 Compare security concepts	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
1.4.a Risk (risk scoring/risk weighting, risk reduction, risk assessment)	Y / N			☐
1.4.b Threat	Y / N			☐
1.4.c Vulnerability	Y / N			☐
1.4.d Exploit	Y / N			☐
1.5 Describe the principles of the defense-in-depth strategy	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐
1.6 Compare access control models	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
1.6.a Discretionary access control	Y / N			☐
1.6.b Mandatory access control	Y / N			☐
1.6.c Nondiscretionary access control	Y / N			☐
1.6.d Authentication, authorization, accounting	Y / N			☐
1.6.e Rule-based access control	Y / N			☐
1.6.f Time-based access control	Y / N			☐
1.6.g Role-based access control	Y / N			☐
1.7 Describe terms as defined in CVSS	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
1.7.a Attack vector	Y / N			☐
1.7.b Attack complexity	Y / N			☐
1.7.c Privileges required	Y / N			☐
1.7.d User interaction	Y / N			☐
1.7.e Scope	Y / N			☐
1.8 Identify the challenges of data visibility (network, host, and cloud) in detection	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐

1.9 Identify potential data loss from provided traffic profiles	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
1.10 Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
1.11 Compare rule-based detection vs. behavioral and statistical detection	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐

Section: 2.0 Security Monitoring

2.1 Compare attack surface and vulnerability	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
2.2 Identify the types of data provided by these technologies	Need to Study?	Complete by:	Resource:	Completed
2.2.a TCP dump	Y / N			☐
2.2.b NetFlow	Y / N			☐
2.2.c Next-gen firewall	Y / N			☐
2.2.d Traditional stateful firewall	Y / N			☐
2.2.e Application visibility and control	Y / N			☐
2.2.f Web content filtering	Y / N			☐
2.2.g Email content filtering	Y / N			☐
2.3 Describe the impact of these technologies on data visibility	Need to Study?	Complete by:	Resource:	Completed
2.3.a Access control list	Y / N			☐
2.3.b NAT/PAT	Y / N			☐
2.3.c Tunneling	Y / N			☐
2.3.d TOR	Y / N			☐
2.3.e Encryption	Y / N			☐
2.3.f P2P	Y / N			☐
2.3.g Encapsulation	Y / N			☐
2.3.h Load balancing	Y / N			☐

2.4 Describe the uses of these data types in security monitoring	Need to Study?	Complete by:	Resource:	Completed
2.4.a Full packet capture	Y / N			☐
2.4.b Session data	Y / N			☐
2.4.c Transaction data	Y / N			☐
2.4.d Statistical data	Y / N			☐
2.4.e Metadata	Y / N			☐
2.4.f Alert data	Y / N			☐
2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
2.6 Describe web application attacks, such as SQL injection, command injections, and crosssite scripting	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
2.7 Describe social engineering attacks	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/ symmetric)	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
2.11 Identify the certificate components in a given scenario	Need to Study?	Complete by:	Resource:	Completed
2.11.a Cipher-suite	Y / N			☐
2.11.b X.509 certificates	Y / N			☐
2.11.c Key exchange	Y / N			☐
2.11.d Protocol version	Y / N			☐
2.11.e PKCS	Y / N			☐

Section: 3.0 Host-Based Analysis

3.1 Describe the functionality of these end-point technologies in regard to security monitoring	Need to Study?	Complete by:	Resource:	Completed
3.1.a Host-based intrusion detection	Y / N			☐
3.1.b Antimalware and antivirus	Y / N			☐
3.1.c Host-based firewall	Y / N			☐
3.1.d Application-level allow listing/block listing	Y / N			☐
3.1.e Systems-based sandboxing (such as Chrome, Java, Adobe Reader)	Y / N			☐
3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐
3.3 Describe the role of attribution in an investigation	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
3.3.a Assets	Y / N			☐
3.3.b Threat actor	Y / N			☐
3.3.c Indicators of compromise	Y / N			☐
3.3.d Indicators of attack	Y / N			☐
3.3.e Chain of custody	Y / N			☐
3.4 Identify type of evidence used based on provided logs	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
3.4.a Best evidence	Y / N			☐
3.4.b Corroborative evidence	Y / N			☐
3.4.c Indirect evidence	Y / N			☐
3.5 Compare tampered and untampered disk image	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐
3.6 Interpret operating system, application, or command line logs to identify an event	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐
3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
3.7.a Hashes	Y / N			☐
3.7.b URLs	Y / N			☐
3.7.c Systems, events, and networking	Y / N			☐

Section: 4.0 Network Intrusion Analysis

4.1 Map the provided events to source technologies	Need to Study?	Complete by:	Resource:	Completed
4.1.a IDS/IPS	Y / N			☐
4.1.b Firewall	Y / N			☐
4.1.c Network application control	Y / N			☐
4.1.d Proxy logs	Y / N			☐
4.1.e Antivirus	Y / N			☐
4.1.f Transaction data (NetFlow)	Y / N			☐
4.2 Compare impact and no impact for these items	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
4.2.a False positive	Y / N			☐
4.2.b False negative	Y / N			☐
4.2.c True positive	Y / N			☐
4.2.d True negative	Y / N			☐
4.2.e Benign	Y / N			☐
4.3 Compare deep packet inspection with packet filtering and stateful firewall operation	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐
4.4 Compare inline traffic interrogation and taps or traffic monitoring	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐
4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐
4.6 Extract files from a TCP stream when given a PCAP file and Wireshark	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐
4.7 Identify key elements in an intrusion from a given PCAP file	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
4.7.a Source address	Y / N			☐
4.7.b Destination address	Y / N			☐
4.7.c Source port	Y / N			☐
4.7.d Destination port	Y / N			☐
4.7.e Protocols	Y / N			☐
4.7.f Payloads	Y / N			☐

4.8 Interpret the fields in protocol headers as related to intrusion analysis	Need to Study?	Complete by:	Resource:	Completed
4.8.a Ethernet frame	Y / N			☐
4.8.b IPv4	Y / N			☐
4.8.c IPv6	Y / N			☐
4.8.d TCP	Y / N			☐
4.8.e UDP	Y / N			☐
4.8.f ICMP	Y / N			☐
4.8.g DNS	Y / N			☐
4.8.h SMTP/POP3/IMAP	Y / N			☐
4.8.i HTTP/HTTPS/HTTP2	Y / N			☐
4.8.j ARP	Y / N			☐
4.9 Interpret common artifact elements from an event to identify an alert	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
4.9.a IP address (source / destination)	Y / N			☐
4.9.b Client and server port identity	Y / N			☐
4.9.c Process (file or registry)	Y / N			☐
4.9.d System (API calls)	Y / N			☐
4.9.e Hashes	Y / N			☐
4.9.f URI / URL	Y / N			☐
4.10 Interpret basic regular expressions	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐

Section: 5.0 Security Policies and Procedures

5.1 Describe management concepts	Need to Study?	Complete by:	Resource:	Completed
5.1.a Asset management	Y / N			☐
5.1.b Configuration management	Y / N			☐
5.1.c Mobile device management	Y / N			☐
5.1.d Patch management	Y / N			☐
5.1.e Vulnerability management	Y / N			☐
5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
	Y / N			☐

5.3 Apply the incident handling process (such as NIST.SP800-61) to an event	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
5.4 Map elements to these steps of analysis based on the NIST.SP800-61	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
5.4.a Preparation	Y / N			☐
5.4.b Detection and analysis	Y / N			☐
5.4.c Containment, eradication, and recovery	Y / N			☐
5.4.d Post-incident analysis (lessons learned)	Y / N			☐
5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800-61)	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
5.5.a Preparation	Y / N			☐
5.5.b Detection and analysis	Y / N			☐
5.5.c Containment, eradication, and recovery	Y / N			☐
5.5.d Post-incident analysis (lessons learned)	Y / N			☐
5.6 Describe concepts as documented in NIST.SP800-86	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
5.6.a Evidence collection order	Y / N			☐
5.6.b Data integrity	Y / N			☐
5.6.c Data preservation	Y / N			☐
5.6.d Volatile data collection	Y / N			☐
5.7 Identify these elements used for network profiling	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
5.7.a Total throughput	Y / N			☐
5.7.b Session duration	Y / N			☐
5.7.c Ports used	Y / N			☐
5.7.d Critical asset address space	Y / N			☐
5.8 Identify these elements used for server profiling	**Need to Study?**	**Complete by:**	**Resource:**	**Completed**
5.8.a Listening ports	Y / N			☐
5.8.b Logged in users/service accounts	Y / N			☐
5.8.c Running processes	Y / N			☐
5.8.d Running tasks	Y / N			☐
5.8.e Applications	Y / N			☐

5.9 Identify protected data in a network	Need to Study?	Complete by:	Resource:	Completed
5.9.a PII	Y / N			☐
5.9.b PSI	Y / N			☐
5.9.c PHI	Y / N			☐
5.9.d Intellectual property	Y / N			☐
5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐
5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)	Need to Study?	Complete by:	Resource:	Completed
	Y / N			☐

CBROPS Study Resources

Cisco certifications empower you to understand real-world issues and address them quickly and effectively. Get started on the path to certification success and enjoy your personal and professional journey.

CBROPS Course Overview

http://cs.co/CyberOpsCourseOverview

Prepare for your certification with official Cisco training courses.

Exam Review Tool

http://cs.co/cyberops-associate

Put your skills to the test with practice questions designed to identify knowledge gaps.

CyberOps Community Forum

http://cs.co/CyberOpsCommunity

Join your community for a chance to ask questions, share ideas and connect with your peers.

CyberOps Prep

http://cs.co/cyberops-prep

Access your ultimate self-study resource including webinars, quizzes and resources.

CBROPS Study Materials

http://cs.co/learning-plan-detail-standard

Add these study materials to your Learning Plan.

CBROPS Preparation Bundle

http://cs.co/cbrops-elearning

Save on the official e-learning course, exam review tool and exam voucher for the CyberOps Associate.