CyberOps, Minor Update 1.2

Products and technologies are evolving faster than ever before. To ensure that our certification programs remain relevant to current practice and keep up with the fast pace of change, we are committed to an annual maintenance review. Minor updates ensure exam topics are clear, introduce new topics, and phase out older products and solutions that are less relevant today. The aim is to make the minor adjustments needed to match the evolution of technologies while ensuring the changes are minimal so that they do not disrupt a candidate's study plans.

The CyberOps Associate and Professional just completed the 1.2 minor update to keep the domains closely aligned with today's commonly adopted technologies and solutions and to recognize the role of AI in monitoring and analysis. To reflect these latest minor updates to the program, effective January 21, 2025, the Cisco CyberOps Associate and Cisco CyberOps Professional certification names will change to Cisco Cybersecurity Associate and Cisco Cybersecurity Professional.

Below is a summary of the blueprint changes that will go live on January 21, 2025.

200-201 CBROPS	
v1.1 to v1.2	
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)~~
1.3.k	Threat modeling
1.3.l	DevSecOps
3.1	Describe the functionality of these endpoint technologies in regard to security monitoring utilizing rules, signatures and predictive AI
3.1.a	Host-based instruction detection
3.1.b	Antimalware and antivirus
3.1.c	Host-based firewall
~~3.1.d~~	~~Application-level allow-listing/block-listing~~
~~3.1.e~~	~~Systems-based sandboxing (such as Chrome, Java, Adobe Reader)~~

350-201 CBRCOR

Cisco and Cisco logo are trademarks or registered of Cisco and/or its affiliates in the U.S. and other countries.
To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.
Cisco © and/or its affiliates. All rights reserved.

CyberOps, Minor Update 1.2

v1.1 to v1.2	
2.1	Recommend AI-powered data analytic techniques to meet specific needs or answer specific questions
2.12	Apply AI-driven threat intelligence using tools
2.14	Describe the different mechanisms to detect and enforce data loss prevention techniques
2.14.a	Host ~~endpoint-based~~
2.14.b	Network~~-based~~
2.14.c	Application~~-based~~
2.14.d	Cloud~~-based~~
3.4	Interpret the sequence of events during an attack based on predictive AI analysis of traffic patterns

300-215 CBRFIR

v1.1 to v1.2	
1.6	Describe the role of:
1.6.a	Hex editors (HxD, Hiew, and Hexfiend) in DFIR investigations
1.6.b	Disassemblers and debuggers (such as, Ghidra, Radare, and Evans Debugger) to perform basic malware analysis
1.6.c	Deobfuscation tools (such as, XORBruteForces, xortool, and unpacker)
1.6.d	Memory forensics tools
2.3	Evaluate output(s) to identify IOC on a host
2.3.a	Process analysis
2.3.b	Log analysis including cloud-native application logs
2.3.c	Network traffic analysis for anomaly detection

300-220 CBRTHD

v1.1
No changes

Cisco and Cisco logo are trademarks or registered of Cisco and/or its affiliates in the U.S. and other countries.
To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.
Cisco © and/or its affiliates. All rights reserved.