Certification Guide

Intel Security Certified Product Specialist

Security Information Event Management (SIEM)

Why Get Intel Security Certified?

As technology and security threats continue to evolve, organizations are looking for employees with the most up-to-date certifications on the most current techniques and technologies. In a well cited IDC White Paper, over 70% of IT Managers surveyed felt certifications are valuable for their team and were worth the time and money to maintain. Becoming Intel Security certified distinguishes you from other security professionals and helps validate that you have mastery of the critical skills covered by the certification exams. Earning a certification also your commitment to continued learning and professional growth.

About Intel Security Certification Program

Currently, Intel offers two industry-recognized certifications as part of our Intel Security Certification Program: Intel Security Certified Product Specialist and Intel Security Certified Security Professional.

The Intel Security Certified Product Specialist certifications are designed for candidates who administer a specific McAfee product or suite of products, and have one to three years of experience with that product or product suite. This certification level allows candidates to demonstrate knowledge in the following key product areas:

- Installation
- Configuration
- Management
- Basic architecture and troubleshooting

The Intel Security Certified Security Professional certifications are designed for security practitioners, penetration testers, auditors, consultants, administrators — with one to three years of experience. This certification level allows candidates to demonstrate knowledge in the following high-level assessment areas:

- Profiling and inventorying
- Vulnerability identification
- Vulnerability exploitation
- Expanding influence

About This Guide

This guide is intended to help prepare you for the **Intel Security Certified Security Professional — Security Information Event Management (SIEM)** exam. For more information about other certification exams or about the Intel Security Certification program go to **www.mcafee.com** and select **For Enterprise**, **Services**, and then **Education Services**.

Highlights

This guide has been developed as a resource for your preparation to take the Intel Security Certified Product Specialist — SIEM Exam (MA0-104). The following information is provided:

- About the Intel Security Certification Program
- Exam details
- Suggested resources for exam preparation
- Knowledge domain topics
- Sample exam items

intel Security

Intel Security Certified Product Specialist — Security Information Event Management (SIEM)

This exam validates that the successful candidate has the knowledge and skills necessary to successfully install, configure, and manage a McAfee SIEM solution. It is intended for security professionals with one to three years of experience using McAfee SIEM products and associated technologies.

Exam Details

- Associated exam: MA0-104
- Associated Training: McAfee SIEM Administration 101 (4 days), McAfee SIEM Administration 201 (4 days)
- Number of Questions: 70
- Exam Duration: 140 Minutes
- Passing Score: 62%
- Exam Price: $150 USD (Exam prices are subject to change. Please visit the following link for exact pricing: **http://www.pearsonvue.com/intel/index.asp**

Exam Preparation

Suggested preparation for this exam is:

- 4 Days McAfee SIEM Administration 101 training (https://mcafee.netexam.com/catalog.html)
- 4 Days McAfee SIEM Administration 201 course (**www. mcafee.com/us/services/product-training/index.aspx**)
- Minimum of one year using McAfee SIEM
- Knowledge domains (see later in the guide)
- Sample questions (see later in the guide)

Certificate Registration

Intel Security has partnered with Pearson VUE, the global leader in computer-based testing, to administer our certification program. Pearson VUE makes the certification process easy from start to finish. With over 5,000 global locations, you can conveniently test your knowledge and become Intel Security Certified.

To register for an exam, go to: **http://www.pearsonvue.com/intel/index.asp**

Exam Duration

The Intel Security Certification Program has built in time to include the following actions during an exam challenge at each testing facility:

- Time to answer exam questions
- Time to review instructions and provide comments after completion

Intel Security reserves the right to change the exam content and time requirements at any time. The most accurate means of obtaining this information is to contact the exam delivery provider on the day of your exam challenge. A notification appears on your screen before the exam begins that shows the maximum time allowed for answering the questions in that exam.

Certification Transcripts

Individuals who have passed an Intel Security certification exam are granted access to the Intel Security Certification Program Candidate site. On the site, you will find:

- Your official Intel Security Certification Program transcript and access to the transcript sharing tool
- The ability to download custom certification logos
- Additional information and offers for Intel-certified individuals
- Your contact preferences and profile
- News and promotions

McAfee SIEM Administration (4 days)

Although formal training is not required prior to the exam, the **McAfee SIEM Administration 101** (4 days) and/or the **McAfee SIEM Administration 201** course is recommended.

The McAfee SIEM Administration 101 course provides in-depth training on how to set up and administer McAfee Security Information and Event Management (SIEM) solution. Using both lectures and practical lab exercises, the course shows you how to effectively implement the SIEM solution in a complex enterprise environment.

The McAfee SIEM Administration 201 course uses guided demonstrations and independent lab environments to configure and use McAfee SIEM appliances to resolve security challenges typically found in an enterprise environment.

To register for either or both of these courses, go to: **https://mcafee.netexam.com/catalog.html**

Practical (Hands-on) Experience

A minimum of one year of experience using McAfee SIEM and associated technologies. Recommended hands-on activities include but are not limited to:

- Solution Planning
- Installation/upgrade
- Configuration
- Management
- Troubleshooting

Technical ServicePortal

The Technical ServicePortal provides a single point of access to valuable tools and resources, such as:

- Documentation
- Security bulletins
- Technical articles
- Product downloads
- Tools

To access the ServicePortal, go to: **https://support.mcafee.com**

Expert Center Community

The Expert Center is a community for McAfee product users. Here you will find valuable information for your McAfee products, such as

- Instructional videos and whitepapers
- Discussion feeds for experts and other users
- Guidelines to establish baselines, and to harden your IT environment
- Ways to expedite monitoring, response, and remediation processes

To access the Expert Center, go to: **https://community.mcafee.com/community/business/expertcenter**

Exam Knowledge Domains

Networking

- Networking technology theory, principles and practices
- Data networking standards and
- protocols
- LAN and WAN technologies
- Network administration
- Network and routing protocols
- Baseline conditions
- Perimeter security
- Internal network security
- Basic infrastructure
- Sniffing/network monitoring
- TCP/IP and NAT/PAT

Systems

- Client/server technology
- Group policy overview and security templates
- Web permissions and authorization
- Redundancy/fault tolerance/ high availability
- Drive encryption
- System administration
- Virtual environments
- Processors (CPUs)
- Baseline conditions
- System access and navigation
- Multi-server environments
- Operating systems

Applications

- Databases
- Redundancy
- Web protocols
- Baseline conditions

Policies and Procedures

- Permissions, delegation, and auditing
- Policies governing user access
- Role permissions
- System testing procedures
- Proactive Protection Scan policy
- Network password procedures
- Company security policies
- Device usage policies
- Change control procedures
- Product specific maintenance procedures
- Incident response procedures
- Role specific escalation procedures
- Corporate security controls
- Corporate security strategy
- Device access control

Architect and Integration/Best Practices

- Level of security required
- Problem isolation/tools required
- Industry security standard

Security Foundation

- Firewall
- Computer viruses, spyware, and malware, spam
- Network threat prevention technologies
- Spyware protection technologies
- Firewall technologies and intrusion prevention
- Heuristic-based protection
- Authentication
- Vulnerabilities and remediation techniques
- Malware incidents
- Internal threats and attacks
- External threats and attacks
- Security protocols
- Cryptography
- Network security policies
- Network access control
- Common threats and vulnerabilities

Architecture and Integration Best Practices

- Level of security required
- Security monitoring
- Problem isolation tools/ practices

Security Foundation

- Computer viruses, spyware, and malware, spam
- Network threat prevention technologies
- Firewall technologies and intrusion prevention
- Heuristic-based protection
- Authentication
- Vulnerabilities and remediation techniques
- Malware incidents
- Internal and external threats and attacks
- Security protocols
- Cryptography
- Network security policies and access control
- Common threats and vulnerabilities

Operation and Administration

- Password management
- Network and support management tools and procedures
- Patch management
- Security alerts, front-line analysis and escalation
- Intrusion detection systems
- Monitoring tools
- Problem determination
- Incident and issue categorization
- Basic product functions
- Product policy configuration
- Product report generation
- Version controls
- Detailed product functions
- Protected materials

Sample Exam Items

The following exam items are provided for review. These items are similar in style and content to those referenced in the Intel Security Certified Product Specialist — SIEM exam. The answers are provided after the questions.

1. **Which feature is accessed via the Receiver Properties?**
   - **A** Alarms
   - **B** Data Source Profiles
   - **C** Watchlists
   - **D** Asset Management
2. **Default Event Aggregation occurs on which of the following fields?**
   - **A** Signature ID
   - **B** Username
   - **C** Destination Port
   - **D** Source Port
3. **Which of the following components make up the functional SIEM stack?**
   - **A** Data Processing
   - **B** Correlation
   - **C** Mitigation
   - **D** Policy Updating
4. **Which of the following statements are NOT true concerning Global Threat Intelligence (GTI) Watchlists?**
   - **A** They are comprised of third-party threat advisories.
   - **B** They are comprised of Watchlists containing suspicious and malicious IP addresses
   - **C** They are used as a scoring source
   - **D** They are licensed from McAfee
5. **ELM storage pools require what percentage of allocated space for mirroring overhead?**
   - **A** Firewall Rule
   - **B** Firewall Group
   - **C** Firewall Options
   - **D** Firewall Catalogs
6. **Specific event and network flow statistics were gathered from a network over a specific 12 hour period.**
   Firewall produced 450,000 total events
   Unix Servers produced 62,000 total events
   Web Applications produced 1,200,500 total events
   Routers produced 150,000,000 total flows
   With these statistics in mind, what is the total EPS for the network?
   - **A** 3,511
   - **B** 3,472
   - **C** 3,500
   - **D** 3,510
7. **Which of the following time zones is the default setting for the McAfee Enterprise Security Manager (ESM) system clock?**
   - **A** International Date Line West
   - **B** Eastern Standard Time
   - **C** Greenwich Mean Time
   - **D** Geo-Location

8. **While investigating malware, an analyst can narrow the search quickly by using which of the following watchlists in the McAfee SIEM?**
   - **A** Botnet – Control Channel
   - **B** Malware Detections
   - **C** GTI Suspicious and Malicious
   - **D** Passive DNS – Malware Domain
9. **Which of the following statements about Child Data Sources is NOT true?**
   - **A** They will have VIPS, policy and Agent rights
   - **B** They will be displayed on the Receiver Properties > Data Sources table
   - **C** They will appear on the System Navigation tree
   - **D** They do not count towards the total number of data sources
10. **Which of the following appliances contains an event database?**
   - **A** ESM
   - **B** ADM
   - **C** ELM
   - **D** DEM

Answer Key

1. B
2. A
3. B
4. A
5. C
6. A
7. C
8. C
9. D
10. A

Intel Security
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com