Gartner Research

Security Operations for Technical Professionals Primer for 2024

Dennis Xu, Steve Santos, Kevin Schmidt

Gartner

Security Operations for Technical Professionals Primer for 2024

Published 31 January 2024 - ID G00802639 - 4 min read

By Analyst(s): Dennis Xu, Steve Santos, Kevin Schmidt

Initiatives: Security Operations for Technical Professionals

> Security operations are critical to an effective security program. Gartner's 2024 technical professionals initiative will guide security and risk management technical professionals as they investigate threats, detect and respond to incidents, and manage exposures in their IT environments.

Scope

The security operations initiative covers the people, processes and technologies needed to identify and manage exposures, and monitor, detect and respond to cybersecurity threats and incidents.

Topics in this initiative include:

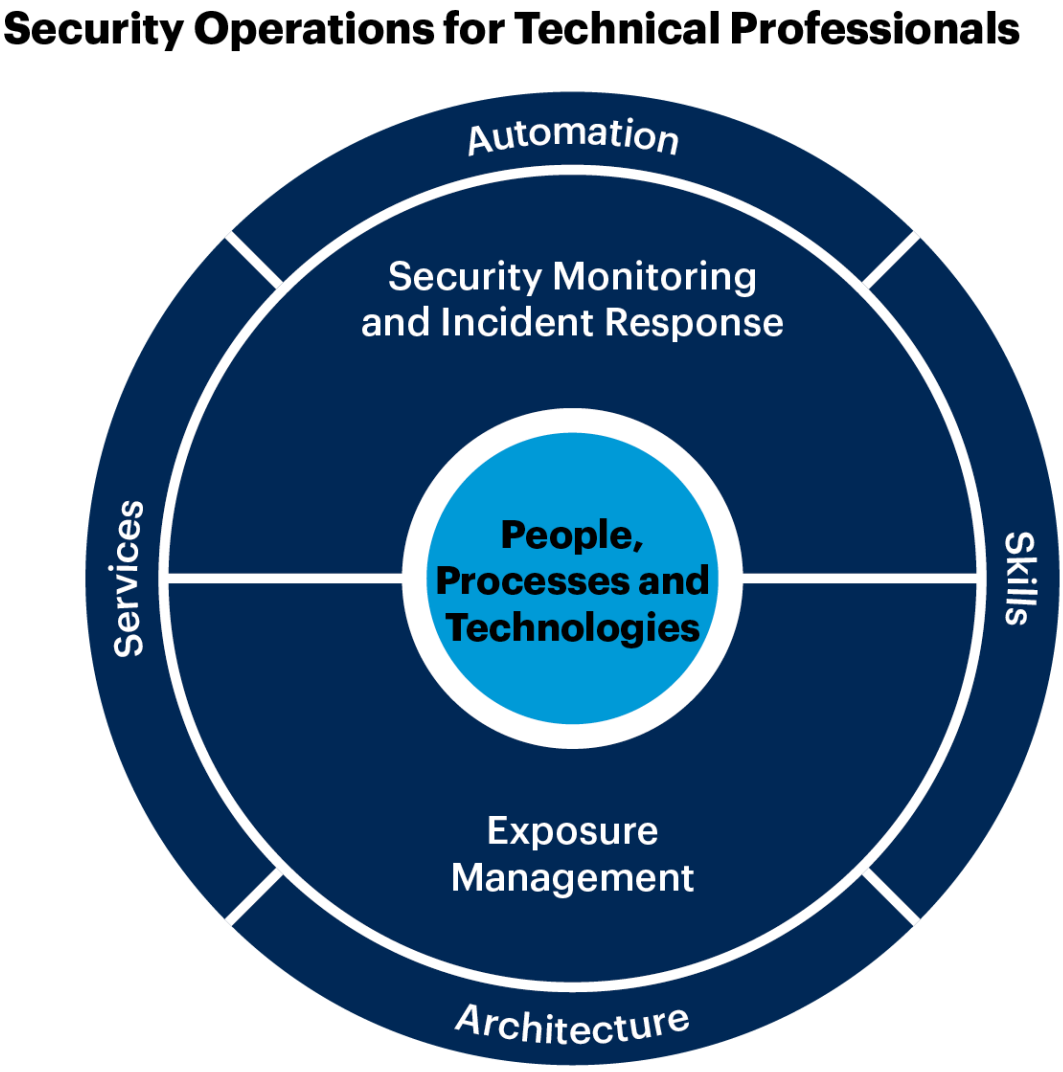
- **Security Monitoring and Incident Response:** Create and enhance the security operations program by selecting appropriate technologies and services, and streamlining detection and response processes.

- **Exposure Management:** Evaluate and select attack surface management, vulnerability assessment and other security assessment capabilities, and then deploy, operate and maintain these technologies and their adjacent processes.

Some content may not be available as part of your current Gartner subscription. Contact an account executive if you wish to discuss expanding your access to Gartner content.

Analysis

Figure 1: Security Operations for Technical Professionals Overview



Source: Gartner
802639_C

Increasing the use of threat detection and response capabilities continues to be a critical pillar in security programs because attackers inevitably find ways around strongly implemented preventive controls. Key responsibilities of the security operations team include the selection and implementation of a detection and response technology and service portfolio.

Operational burdens such as team scaling, complex workflow and system management can become bottlenecks for detecting threats in a meaningful time period. Furthermore, continued expansion of cloud usage, an increasingly distributed workforce and mass adoption of rapid software development practices have created additional demands on security monitoring functions. Building and evolving an effective security operations practice can help overcome those challenges and create a security program that is more robust overall.

Some compromises are inevitable. Nonetheless, a malicious actor compromising your system will negatively impact the organization. A well-designed and well-executed incident response program is critical because it reduces incident impact and incurred costs when such an event occurs. Organizations continue to struggle with staffing and skills for effective security monitoring and incident response.

Security operations teams must also implement strong exposure identification, prioritization and remediation practices to reduce their attack surface. However, not all security issues are identified through vulnerability assessments. Additional attack surface management practices (such as external attack surface monitoring) and exposure validation practices (such as breach-and-attack simulation, penetration testing and red teams) are also essential. These help to provide input into a strong security operations program.

Some clients' internal teams do not have the capacity to handle the threat detection and incident response requirements at scale, while also growing their security operations capability. Achieving coverage and effectiveness across an increasingly complex technology, business and threat landscape is often best accomplished with a hybrid team approach that includes more tactical roles for service providers. You will need to determine the type of security operations functions that are best handled internally, and those that are better taken care of by an external partner. Our insights help you find this balance.

Topics

Gartner provides the knowledge needed to effectively implement and execute on security operations programs.

Our research in this area addresses the following topics:

Security Monitoring and Incident Response

Security monitoring and incident response encompasses threat detection, security monitoring, security automation and the creation of a security operations program (including an incident response program). It also covers the day-to-day execution and evolution of these programs. Being prepared for incident response is likely to be one of the more cost-effective security measures that any organization can take.

Questions Your Peers Are Asking

- How should we implement threat detection and incident-response capabilities?
- How should we build performance and growth into our security operations?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- A Guidance Framework for Architecting and Deploying a Modern SIEM Solution
- How to Create an Incident Response Plan
- 4 Essentials to Effectively Execute an Incident Response Process
- Quick Answer: How Can Security Operations Teams Leverage ChatGPT?

Planned Research

- How to use MITRE ATT&CK to improve threat detection capabilities
- How to work with an MDR provider to improve security
- Common SOAR scenarios and use case identification
- How to use threat intelligence for security monitoring and incident response

Exposure Management

Exposure management is the aggregation of attack surface management (ASM), vulnerability management, and security controls validation tools and capabilities. Exposure management includes the evaluation and selection of tools such as external attack surface management (EASM), cyber asset attack surface management (CAASM), vulnerability scanners, vulnerability prioritization tools, automated pentesting, and breach and attack simulation (BAS). It also covers the deployment, operation and maintenance of these technologies, and process best practices to improve their efficacy.

Questions Your Peers Are Asking

- How should we identify and assess our attack surface?
- How should we assess, manage and prioritize vulnerabilities?
- How should we structure our security testing practices to validate controls?

Recommended Content

Some recommended content may not be available as part of your current Gartner subscription.

- A Guidance Framework for Developing and Implementing Vulnerability Management
- Using Security Testing to Grow and Evolve Your Security Operations
- GTP Client Webinar: What Is Attack Surface Management?
- Decoding Vulnerability Management: A Stand-Alone Tool vs. a Technique in Endpoint Protection

Planned Research

- Guidance framework for implementing attack surface management (ASM)
- Practical implementation of security validation tools to validate exposure
- Exposure management: how to get ASM, VM and security validation integrated to quantify exposure risks

Suggested First Steps

- Charting Your Journey to a Modern SOC in 3 Steps
- The Journey to SOC in Three Steps: Step 1 Planning and Prioritizing Objectives
- The Journey to SOC in Three Steps: Step 2 Building the Detection Stack and Establishing Security Operations

Essential Reading

- How to Create and Maintain Security Monitoring Use Cases for Your SIEM
- A Guidance Framework for Developing and Implementing Vulnerability Management Use
- Adversary-Generated Threat Intelligence to Improve Threat Detection and Response

Document Revision History

Security Operations for Technical Professionals Primer for 2023 - 14 February 2023

Security Operations for Technical Professionals Primer for 2022 - 4 February 2022

Security Operations for Technical Professionals Primer for 2021 - 4 February 2021

Security Operations for Technical Professionals Primer for 2020 - 23 January 2020

Security Operations for Technical Professionals Primer for 2019 - 5 February 2019

Related Priorities

Initiative Name	Description
Identity & Access Management (Tech Professionals)	Use this initiative to modernize IAM and establish trustworthy digital identities with the right access to the right resources for the right reasons in changing and distributed IT environments.
Security Tech & Infrastructure(Tech Professionals)	This initiative describes the processes and technology required to protect organizations' modern digital infrastructure against cyberattack.

Actionable, objective insight

Explore these additional, complimentary resources and tools for security leaders:

Conference

Gartner Security & Risk Management Summit

Explore how to build cybersecurity resilience in a complex world.

View Agenda

How We Help

Gartner for Cybersecurity Leaders

Reframe your role, align your security strategy and build programs that balance protection with organization needs.

View Insights

Roadmap

The IT Roadmap for Cybersecurity

Learn best practices to create a resilient, scalable and agile cybersecurity strategy.

Access Roadmap

Infographic

Top Trends in Cybersecurity for 2024

Discover insights and actions for security and risk management leaders.

View Infographic

Already a client?
Get access to even more resources in your client portal. Log In

Connect With Us

Get actionable, objective insight that drives smarter decisions and stronger performance on your mission-critical priorities. Contact us to become a client:

U.S.: 1 855 811 7593

International: +44 (0) 3330 607 044

Become a Client

Learn more about Gartner for IT Leaders
gartner.com/en/information-technology

Stay connected to the latest insights

Gartner®