Where Are You in the Security Operations Journey?

With expanding attack surfaces and increasing threats, security operations (SecOps) is critical for every organization.

AI-powered attacks execute 36,000 scans per second.[1]

Attack surfaces face 97B+ exploitation attempts globally.[2]

67% of security teams say alert volume exceeds analyst capacity.[3]

Identifying Your Stage in the SecOps Journey

As their security operations mature, organizations move through distinct stages. Each stage has different priorities, constraints, and risks. By identifying your stage, you can determine the capabilities you need to reduce exposure, improve response, and scale effectively.

Foundational security operations

Security is handled by IT or small security teams with limited tools and coverage.

- Security staffed by IT or one to three generalists
- Limited monitoring, reactive alert handling
- Minimal correlation across data sources

Need:
Ready-to-use foundational capabilities that enable centralized monitoring, basic correlation, and triage without increasing operational burden

Developing security operations

Security incorporates limited SOC capabilities with a dedicated team of three or four analysts who often struggle because of alert volume and solution complexity.

- Multiple security tools with limited integration
- Growing telemetry with limited prioritization
- Investigations are manual and time-consuming

Need:
Better alert prioritization and investigation workflows, correlated threat detection across data sources, and proactive threat identification and exposure awareness

Advanced SecOps

Security includes an established SOC staffed with more than five analysts who face serious threat volume and workload challenges.

- Large telemetry volumes across multivendor environments
- Defined processes but heavy manual execution
- Scaling depends on automation, not more analysts

Need:
End-to-end orchestration and automation to standardize workflows, coordinated responses across tools and teams, and the application of AI-assisted decisioning, so the SOC can operate at machine speed and scale

Managed SOC

Teams at any stage may extend capabilities through managed or co-managed services to accelerate maturity and reduce operational burden.

- 24×7 monitoring requirements
- Limited internal staffing or coverage gaps

Need:
Expert partner that can provide monitoring, threat detection, and remediation guidance, stringent response SLAs, coverage scalability, use case additions, and surge capacity for major incidents or new initiatives

The Fortinet SOC Platform

Designed to support teams at every stage of the security operations journey, the Fortinet SOC Platform combines modular solutions that work independently or together across environments and operating models.

To learn more about how the Fortinet SOC Platform can help you, download the solution brief.

DOWNLOAD NOW

[1] Fortinet, 2025 Global Threat Landscape Report, 2025. https://www.fortinet.com/resources/reports/threat-landscape-report
[2] Fortinet, 2025 Global Threat Landscape Report, 2025. https://www.fortinet.com/resources/reports/threat-landscape-report
[3]Enterprise Strategy Group, The Quantified Benefits of Fortinet Security Operations Solutions, January 2025. https://www.fortinet.com/content/dam/fortinet/assets/reports/esg-economic-validation-fortinet-automated-soc.pdf