Make Your Security Operations Center (SOC) More Efficient

The secret to advanced threat preparedness may actually lie within your organization—your current people, processes, and technologies.

38% to 100% boost in effectiveness with collaboration.

Outcomes

Despite the cyberskills shortage, there are ways to improve security operations results.

Faster time to detect

By getting insights earlier, in context, from more contributors.

Higher confidence

Since multiple sources can validate decisions as needed.

Fewer errors

Through accurate, automated sharing of critical data.

Faster time to correct

Via clear guidance on the right actions, delivered to the right people to act.

People

Good communication, transparency, and accountability enables teamwork across the many contributors to incident management.

CISO

The CISO Office's engineers and architects have the dominant responsibility end to end, from prevention to analysis to remediation.

Operations

Endpoint and network administrators as well as application support roles are critical for containment and remediation.

IR

SOC analysts and incident responders, including third parties, play a major role in prevention, not just detection and analysis.

Process

Respondents say they are willing to automate or semi-automate many tasks they used to perform manually.

Top semi-automated tasks

58%
Cross-product orchestration to quarantine systems.

57%
Copy a file to an external store.
Restore a file.

55%
Delete a backdoor account.
Shutdown or reboot a system.

Top automated tasks

43%
Clear browser/ cache cookies.

37%
Malware sandbox submission.

36%
Stop/start a windows service.
Network isolation.

33%
Kill process.

Technology

Incident management tools can collaborate through cross-tool orchestration, remote commands, shared threat intelligence, unified management, and bi-directional integration.

4 tools

The average number of tools used was 4.

6–15 tools

20% of companies used more than 6—as many as 15.

Security Investment Priorities

While better tools remain critical, respondents rated collaboration as their third highest priority for threat management spending.

40%
Better detection tools.

33%
Better preventative tools.

32%
Improved collaboration between SOC analysts, Incident Responders, & Endpoint Administrators.

Collaboration connects people, processes, and technologies, enabling organizations to tackle more threats in less time with fewer resources.

Visit www.mcafee.com/collaboration for the full report.

McAfee is now part of Intel Security.