THE CONVERGENCE OF SECURITY AND NETWORK OPERATIONS

More complex business networks, including cloud services and infrastructure, mobile applications, virtual desktops, SDN/NFV, and IoT systems, are taxing both security and network operations teams. At the same time, increasingly sophisticated and persistent attacks are challenging traditional organizational roles and structures.

Evolving technology can and will play a role: embedded and more automated workflows, AI for faster alert management and analysis, as well as more actionable, better integrated threat intelligence. But protection from today's attacks will require more than improved technology. Just as technology needs to evolve, so do the working relationships between security and network operations teams.

NATURAL POINT OF CONVERGENCE

Advanced attacks repeatedly traverse the network, from external command and control, lateral movement looking to exploit vulnerabilities, to the actual exfiltration of valuable data. Visibility into the security of the network is a natural point of convergence between security teams and network operations. Security architects, engineers and SOC analysts take the lead in cyber security, but network teams play a critical role in mitigation and restoring systems to good health. For containment and remediation, security analysts often must work closely with — and in some cases hand off tasks to — network and endpoint administrators.

ARBOR® NETWORKS
The Security Division of NETSCOUT

Primary/Equal Threat Management Responsibility

Who in your organization has primary/equal responsibility for each of these threat management scenarios?

And this covers only the back-end of the defense lifecycle. It should come as no surprise that a recent State of the Network survey found that 97% of the network team respondents are spending more time troubleshooting security issues; 70% reported spending up to 10 hours of a 40 hour work week.

	PREVENTION	DETECTION	TRIAGE	ANALYSIS	CONTAINMENT	REMEDIATION
Security Engineer/Architect (CISO office)	53% ①	48% ①	48% ①	45% ①	48% ①	45% ①
Incident Responder	36% ②	29% ③	24%	24%	22%	22%
SOC Analyst	33% ③	36% ②	33% ②	36% ②	27%	26% ③
Network Administrator/ Engineer	25%	27%	27% ③	27% ③	31% ②	35% ②
Endpoint Administrator	21%	22%	26%	25%	28% ③	23%

SOURCE: Intel/McAfee: How Collaboration Can Optimize Security Operations

STATE OF COLLABORATION

How do security and IT teams themselves see their current cooperation?

ESG Research and ISSA collaborate annually on The State of Cyber Security Professional Careers, a global survey of 437 security and IT professionals that found the more senior the respondent the better the perceived relationship: 48% of managers thought the relationship was very good. But when one asked those on the frontlines of cyber security the results were not as encouraging. Only 32% of the staff level security and IT professionals thought their working relationship was very good.

The top three challenges between security and IT teams:

- Prioritizing tasks between the two groups
- Coordinating processes
- Aligning goals

Technology can help support collaboration with better data sharing and common, automated workflows across distinct security and network teams. Adaptable dashboards or UIs may be built around a specific user's role but working from shared, agreed upon data and definitions.

But improving collaboration will also require new processes and changes in the working relationships between security and network teams.

> **"When an emergency security incident strikes, weak collaboration and poor coordination among critical business functions will magnify and stigmatize any inefficiency in the IR process, impacting the organization's ability to minimize damage and downtime. When we train our customers' incident response teams, 90% of our efforts go to stronger interlock and collaboration between key stakeholders."**
>
> **ISMAEL VALENZUELA, IR/FORENSICS, TECHNICAL PRACTICE MANAGER, FOUNDSTONE® SERVICES**

SOURCE: Intel/McAfee: How Collaboration Can Optimize Security Operation

IMPROVING COLLABORATION

A fundamental step in fostering better coordination between teams is agreement upon definitions for some of the basics: what is a security incident and how are security levels or priorities assigned? Another is regular, iterative communications to help prioritize incidents and focus efforts — especially during, but not limited to, incidence response.

Some of the structural, organizational steps that are being taken to foster better coordination between teams include:

- Increasing security's participation in IT planning
- Adopting new processes or IT frameworks such as COBIT, ITIL, NIST-800, etc.
- Moving select tasks from IT to the security team

Regular participation of security in IT planning goes a long way toward increasing transparency and trust between teams. It also helps security 'get in on the ground floor' of new IT initiatives for planning, testing and deployment. Similarly, frameworks such as COBIT and ITIL can formalize workflows and foster regular communications. These too help build trust between organizations and team members.

A WORK IN PROGRESS

Effective security has always been a group responsibility. The increasing complexities of large networks and the capabilities of advanced attackers are challenging existing organizational roles and structures. Yet effective cyber security has always required a collective effort. The convergence of security and network operations teams will continue to be a work in progress. Like the evolution of technology and tools, security and network operations teams need to continue to evolve their working relationship.

● ● ○

To learn more, read the "AIF for Advanced Threat Use Case" at arbornetworks.com/spectrum to see how Arbor Network's ATLAS Intelligence Feed (AIF) threat indicator policies can detect and defeat today's advanced attack campaigns.

The Security Division of NETSCOUT

arbornetworks.com

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA: +1 866 212 7267
T: +1 781 362 4300

North American Sales
Toll Free: +1 855 773 9200

Europe
T: +44 207 127 8147

Asia Pacific
T: +65 6664 3140

Latin & Central America
T: +52 55 4624 4842