ExtraHop

BETTER TOGETHER

An Executive's Guide to Integrating SecOps and NetOps

INTRODUCTION
Closing the Gap

Like development and operations organizations before the advent of DevOps, security operations (SecOps) and network operations (NetOps) teams have traditionally functioned as separate entities, working together only when necessary. As standalone operations, each team developed its own culture, tools, processes, skillsets, and terminology. And like siloed development and operations before DevOps, this approach worked well enough in the past.

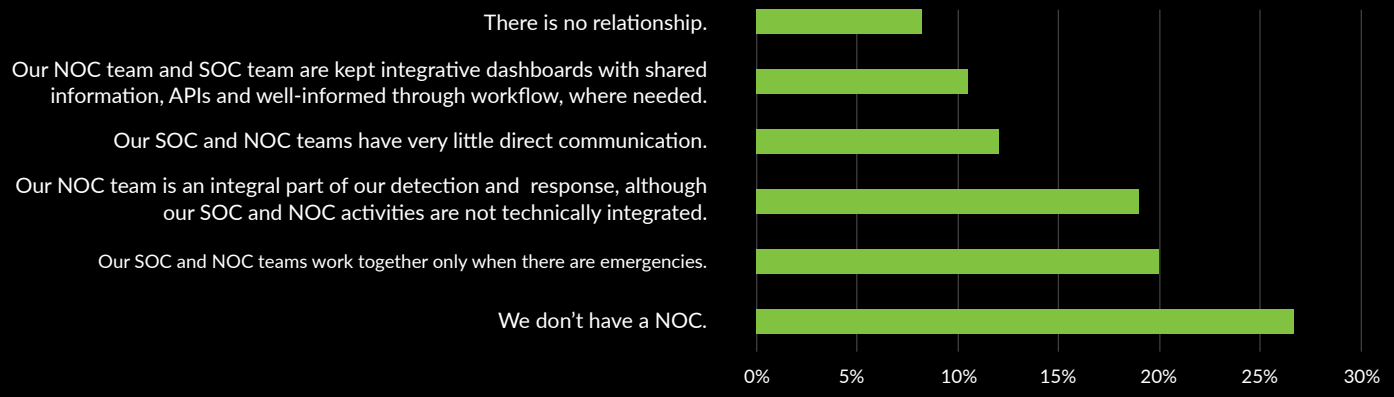
However, given today's increasing IT complexity and scale, it's become imperative to break down the barriers between the two groups and align them—including their tools, processes, and skills—around a common goal: delivering a fast and secure user experience while enabling business agility.

Read on for current statistics demonstrating the clear need to integrate NetOps and SecOps, followed by five compelling value drivers that executives can link to an integrated operations center.

SYNERGY DRIVES BETTER RESULTS

In a global SANS Institute survey on security operations centers, roughly 30 percent of SecOps teams already work together with NetOps. The authors state, "Synergy between the NOC and SOC in terms of shared information and shared goals can be a driving force for SOC efficiency and effectiveness."

What is your SOC's relationship to your network operations center (NOC)?



Source: *The Definition of SOC-cess? SANS 2018 Security Operations Center Survey*, Christopher Crawley and John Pescatore, SANS, August 2018

When NetOps and SecOps Stand Alone

What happens when cybersecurity and network teams don't collaborate?

Slow response to security events

34% of respondents

Finger pointing/ blame game

33% of respondents

Service downtime

27% of respondents

Loss of productivity

28% of respondents

Increase in security breaches/data loss

32% of respondents

Source: "A House Divided: The Cost of Dysfunction Between Network and Cybersecurity Teams," IDG, 2018

Aligning Against Cyberthreats

While high-profile breaches and attacks continue to make headlines on a regular basis, it's not only household names that are impacted. Every organization—regardless of size or industry—faces the same challenge: improve and adapt the organization's cybersecurity posture to keep pace with rapid change.

To turn the tide against increasingly smart, fast, and more agile cybercriminals, executives must unite two critical groups around the common purpose of protecting the organization against attack. By creating a co-operational framework between SecOps and NetOps, you can focus your organization's resources and skills to:

- Improve security posture while enabling business agility
- Deliver a secure and high-quality end-user experience
- Respond to and mitigate threats faster
- Make the most of scarce IT and cybersecurity talent
- Drive productivity and effectiveness of the teams
- Reduce tool costs and maintenance efforts

Industry analysts agree that these two teams must work together cohesively in the future. Research firm EMA reports that increasing security requirements are already impacting NetOps teams, resulting in:[1]

- Increased collaboration with the IT security team
- Integrated security monitoring systems and network management tools
- Custom or role-based views into network management tools for IT security

The following value drivers indicate specific, quantifiable benefits resulting from a successful NetOps/SecOps integration, and can be used to prove out and evangelize organizational change.

1. *NetSecOps: Everything Network Managers Must Know About Collaborating With Security,* **Enterprise Management Associates, 2018**

DRIVER 1

Eliminating Redundant Tools and Efforts and Optimizing Budget

BEFORE

Given that NetOps and SecOps share many of the same instrumentation points and use cases—including network analytics, continuous packet capture, discovery of new devices, application dependency mapping, and more—there are often overlapping and duplicated processes and tools across the two teams.

This redundancy results in wasted efforts and higher operational costs as well as tool sprawl and overspend. For example, both teams require network analytics—one needs it for performance monitoring and troubleshooting, and the other for threat detection and investigation—and often rely on similar toolsets to analyze the same data. If multiple tools are decrypting the same streams for analysis, the opportunity for tool consolidation is obvious. Likewise, duplicating storage of the same data is a waste of budget.

AFTER

By integrating network and security operations, CIOs and CISOs have a unique opportunity to improve the effectiveness and efficiency of their operations while reducing costs. The two functions can align tool requirements, procurement, and usage in order to:

- Enhance collaboration and streamline processes and communication
- Improve tool utilization
- Reduce the number of tools to purchase, renew, and maintain
- Decrease budget spend on tools and data storage

SHARED TOOLS

- Network analytics
- Continuous packet capture
- Discovery of new devices
- Application dependency mapping

DRIVER 2

Optimizing Use of Scarce Security Talent

BEFORE

One of the most significant challenges facing virtually every IT security organization is finding and retaining top-notch talent. ESG Research found that 53 percent of organizations in 2018 experienced a problematic shortage of cybersecurity skills, up from 42 percent in 2016.[2]

When NetOps and SecOps teams are separate, there's no opportunity to cross-train team members and leverage expanded skillsets to scale resources and help meet increasing cybersecurity needs.

AFTER

With an integrated network and security operations center, teams can share best practices, processes, and culture to improve cross-functional skillsets and optimize the use of existing security resources. Training NetOps staff in security awareness equips more people to recognize incidents and support a surge (when needed), or rotate through to support the SecOps team.

This approach gives each team valuable expertise as well as a clear understanding of what's happening in your enterprise. In many cases, that expertise and insight have cross-functional value–for example, in recognizing both opportunities to improve security hygiene, and potential threats lurking behind behavioral anomalies.

Shared SecOps and NetOps Use Cases

New device/ asset discovery

Application dependency mapping

Policy compliance monitoring and reporting

Continuous packet capture for forensics and root-cause analysis

Anomaly detection for performance issues and threats

2. *ESG Research Report: Technology Spending Intentions Surveys (2016 – 2019)*, ESG Research

DRIVER 3

Improving Security Posture and Reducing Risk

BEFORE

Lack of coordination between NetOps and SecOps can result in delays deploying and updating security solutions, and increases the risk of misconfiguration. Even when a solution is operationalized, data silos slow down incident response times, directly impacting your organization's ability to stop a breach and mitigate damage.

COLLABORATION IS NEEDED FOR ...	BUT SILOS CREATE HURDLES
Policy compliance	Security teams create policies, however IT/NetOps is often responsible for implementing, reporting, and maintaining the systems that follow or enforce those policies. This leads to re-interpretation, drift, and even antagonism between teams, all of which are kindling for non-compliance.
Security hygiene	SecOps teams often lack the visibility needed to identify risks such as weak ciphers and vulnerable ports, protocols, and services—visibility the NetOps team possesses, if it knows what to look for.
Threat detection	SecOps and NetOps teams maintain different data repositories and monitoring systems. These silos delay detection and create visibility gaps where attackers can hide, increasing organizational risk.
Incident investigation	SecOps must rely on NetOps for the data it needs to investigate incidents, such as packet captures and server logs. Time spent waiting for this information results in longer dwell times, larger vulnerability windows, and potentially more damage from the incident.
Incident containment, mitigation, remediation	The span of control to fix a problem usually resides with the NetOps team (or other operational group, such as server or endpoint administration). Requiring a handoff of data and explanations between these teams and SecOps unnecessarily increases staff time-to-respond.

AFTER

With integrated network and security operations, organizations can improve their security posture through:

- Shared tools and data to close visibility gaps
- Processes that are tightly aligned and automated for faster incident response
- Closer collaboration on policy enforcement
- Shared skills and cross-functional learning

These improvements combine to reduce and harden the attack surface, and to accelerate discovery, containment, mitigation, and remediation of threats.

Fortune 500 Retailer Reduces MTTR for Performance and Security Incidents

A major retailer combined its NetOps and SecOps teams to create an integrated operations center that would overcome its security resource gap and improve collaboration. With its fully functional Security and Network Operations Center, the retailer:

- Significantly reduced mean time to resolution for performance disruptions and security incidents
- Improved the overall customer experience by proactively identifying and fixing issues
- Created a mechanism for sharing skills and a pathway for NetOps engineers to move into cybersecurity analyst functions

DRIVER 4

Gaining Visibility (and Confidence) in a Cloud-First World

BEFORE

Most organizations are continuing to migrate workloads to the cloud. Under the shared responsibility model, cloud providers secure the infrastructure and core services, but it's your responsibility to secure your applications and data and maintain performance.

However, increased use of the cloud, as well as network encryption, hinder network visibility for both NetOps and SecOps. In fact, only 37 percent of cybersecurity teams report having complete network visibility.[3]

As with on-premises deployments, NetOps teams must have visibility into network traffic to manage performance and diagnose root causes of issues in cloud environments. In the same way, SecOps needs visibility into network traffic in the cloud in order to identify exfiltration attempts, perform network security forensics, and implement and monitor microsegmentation.

Without full visibility, organizations tend to delay cloud adoption altogether, or find themselves caught in the costly and colloquially dubbed "Great Stall" after their initial workloads migrate but before their teams are comfortable managing this new infrastructure. SecOps, meanwhile, often hits the brakes on cloud adoption due to their concerns about misconfiguration and undetected vulnerabilities.

AFTER

With the right tools delivering visibility and analysis across enterprise cloud deployments, integrated network and security operations teams both get the insight and capabilities they need to manage performance and security, including:

- Real-time access to deep, packet-level insight from on-premises and cloud networks
- Pre-processing of traffic that is more cost-efficient to share with log analysis and SIEM tools
- Monitoring and visibility tools that can be easily shared across multiple teams

3. *A House Divided: The Cost of Dysfunction Between Network and Cybersecurity Teams*, IDG, 2018

Integrated SecOps and NetOps Delivers Tangible Benefits

38%
OPEX reduction

34%
Streamlined workflows

37%
Risk reduction

31%
CAPEX efficiencies

31%
Responsiveness to change in the business

Source: *NetSecOps: Everything Network Managers Must Know About Collaborating With Security*, Enterprise Management Associates, 2018

DRIVER 5

Responding to Change

BEFORE

As the IT environment rapidly shifts to distributed systems across the datacenter and cloud and more organizations migrate workloads to the cloud environment, both SecOps and NetOps need to have a strategy for visibility that can adapt to these changes.

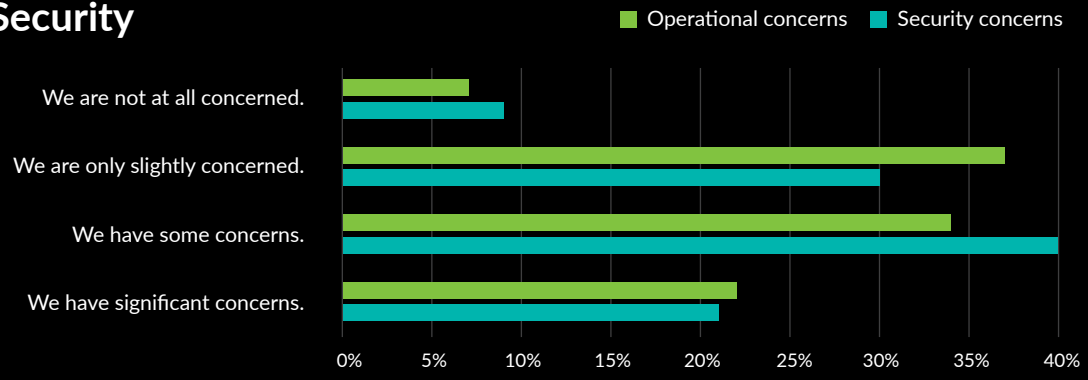
Another requirement is the new Transport Layer Security (TLS) 1.3 specification, which mandates Perfect Forward Secrecy. According to EMA, 40 percent of organizations are already implementing TLS 1.3 for internal traffic, which can negatively impact the ability of both SecOps and NetOps to passively analyze traffic for malicious activity or troubleshoot performance issues.

AFTER

As they consider how to secure and manage the performance of workloads in the cloud, SecOps and NetOps teams have an opportunity to start fresh with tools that span hybrid environments and serve the needs of both teams. Similarly, as TLS 1.3 adoption increases, SecOps and NetOps teams can work together on a solution that preserves visibility into transaction payloads for both security analytics and performance troubleshooting.

TLS 1.3 Adoption Affects Operations and Security

In a survey on TLS 1.3 adoption in the enterprise, 56 percent of all respondents expressed either some or significant operational concerns for implementing TLS 1.3, while 61 percent expressed either some or significant security concerns.



Source: *TLS 1.3 Adoption in the Enterprise*, Enterprise Management Associates, 2019

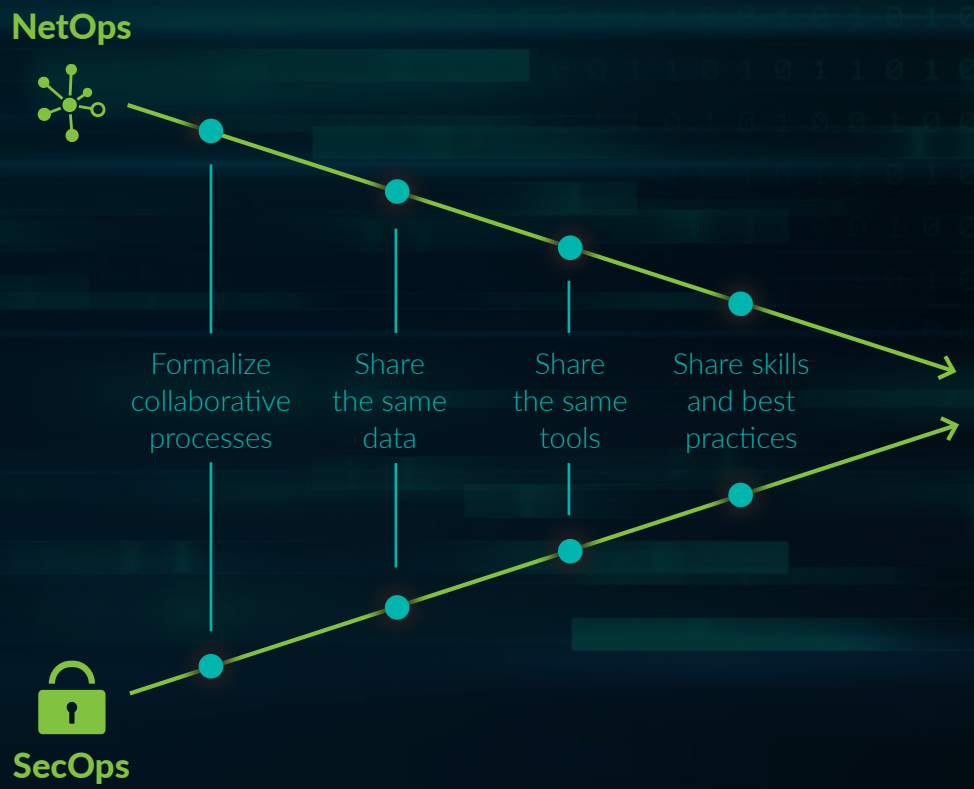
Evolving to an Integrated Network and Security Operations Center

Many organizations are already taking steps to converge network and security operations. In fact, 40 percent of organizations report that their network operations are already fully converged with IT security—although in smaller organizations this may be because the functions were never separated in the first place. Shared tools and processes cover these critical points of collaboration:[4]

- Infrastructure design and deployment
- Event/incident monitoring
- Incident response
- Change management/patch management
- Policy verification/validation

Organizations need not approach the integration of NetOps and SecOps as an all-or-nothing proposition. Instead of attempting to move directly from isolated silos to full convergence, organizations can take a phased approach, with intermediate steps that break down silos over time and foster the ongoing development of collaborative processes.

Executive leadership is key in this process, but technology plays a role as well. As organizations unplug redundant tools, they create budget for new shared capabilities, that in turn help the converged teams operate more efficiently. For example, a packet capture tool that requires labor-intensive manual efforts could be replaced with a solution for real-time packet analysis with retention that automates analysis and provides insight in seconds.



4. *NetSecOps: Everything Network Managers Must Know About Collaborating With Security*, Enterprise Management Associates, 2018

Five Essential Capabilities for Your Security and Network Operations Platform

Network traffic analysis (NTA) is an emerging technology that can deliver tremendous value to both NetOps and SecOps teams as they work together. However, not all NTA solutions offer all the capabilities that enterprises need for efficient and effective SecOps and NetOps. Organizations should look for an enterprise-class NTA solution with these capabilities:

1
Real-time network data analysis

For accurate detection, investigation, and response within a usable timeframe, the NTA solution should conduct analytics and deliver answers in real time, at scale.

2
Complete east-west transaction visibility

To provide high-fidelity insight into threat behaviors, an NTA tool needs to see and analyze the actual contents of network conversations. That means full L2-L7 visibility, application protocol decoding, and decryption of modern cryptographic standards (e.g. TLS 1.3).

3
Safe, controlled decryption to eliminate darkspace

Inside enterprise networks, nearly all traffic today is encrypted, creating blind spots for SecOps and NetOps teams. To provide complete visibility, an NTA tool must be able to decrypt traffic for analysis without compromising data security.

4
Behavioral analysis

Analyzing behavior is the only way to detect previously unknown malicious attack activities. That's why every NTA needs the ability to track application, device, and user activity, and compare new observations against historical and peer behaviors.

5
Guided investigation

Guided workflows can help any user hunt threats quickly without needing to be an expert.

ExtraHop Reveal(x)

ExtraHop Reveal(x) is the only network traffic analysis product that provides complete visibility, real-time detection, and guided investigation at scale, helping to support an integrated security and network operations center.

Complete visibility

Reveal(x) automatically discovers and classifies every device communicating across the network, with real-time, out-of-band decryption so security and network teams can see hidden attackers and crucial transaction details without compromising compliance or privacy. With full east-west visibility from the data center to the cloud to the edge, you'll understand your enterprise from the inside, out.

Real-time detection

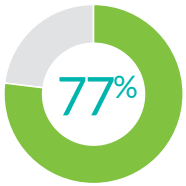
Our cloud-based machine learning uses over 4,700 features to detect suspicious behavior in real time. Reveal(x) automatically discovers and classifies all devices, focusing the scrutiny on the assets most critical to your business. High-fidelity detections correlated with risk scores and threat intelligence help you easily prioritize your time for greater operational efficiency and confident response.

Guided investigation

The Reveal(x) workflow takes you from security event to associated packet in a few clicks, erasing hours spent manually collecting and parsing data. Immediate answers enable immediate, confident responses. Robust integrations with security tools including Phantom, Splunk, Palo Alto, and others help you rise above the noise of alerts, automate investigations, and act in time to protect your customers.

An IDC study of ExtraHop customers shows the value of the platform for SecOps[5]:

Improvement in time to detect threats



Improvement in time to resolve threats

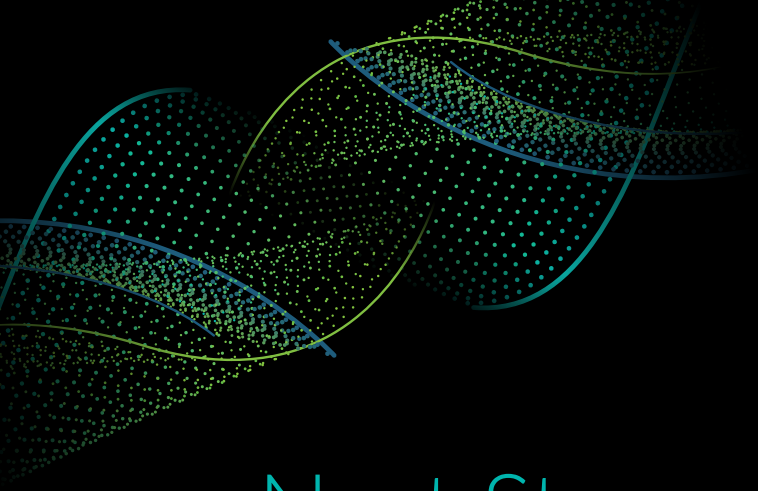
Reduction in staff time to resolve threats

> ExtraHop has provided us the visibility we need to troubleshoot complex application and infrastructure issues. I couldn't be happier with the product.

ENTERPRISE SECURITY ENGINEER IN THE FINANCE INDUSTRY

Source: Gartner Peer Insights, Gartner, Inc., March 2019

5. *ExtraHop Delivers Better User Experience and Security for Enterprises*, IDC, August 2018



Next Steps

By integrating SecOps and NetOps, CIOs and CISOs can improve the effectiveness and efficiency of their operations and drive significant operational, risk management, and economic benefits for their organization. The right platform can enhance those benefits while enabling gradual convergence through shared data and capabilities.

Learn more about the ExtraHop shared SecOps and NetOps platform at www.extrahop.com.

About ExtraHop Networks

ExtraHop is on a mission to stop advanced threats with security that can't be undermined, outsmarted, or compromised. Our dynamic cyber defense platform, Reveal(x) 360, helps organizations detect and respond to advanced threats—before they can compromise your business. We apply cloud-scale AI to petabytes of traffic per day, performing line-rate decryption and behavioral analysis across all infrastructure, workloads, and data-in-flight. With complete visibility from ExtraHop, organizations can detect malicious behavior, hunt advanced threats, and forensically investigate incidents with confidence. When you don't have to choose between protecting your business and moving it forward, that's security uncompromised.

ExtraHop