4141 'B' St., Ste 307
Anchorage, AK 99503

Managed
SOC

Prevention Alone is No Longer Enough.

Cyberattacks against small and mid-sized companies are skyrocketing, causing grave financial damage measured in lost time, lost data, lost public trust, costly remediation, and rising cyber insurance rates.

Being a smaller organization no longer offers any measure of protection against attack. Verizon's 2023 *"Data Breach Investigations Report (DBIR)"* found very little difference in the attack surfaces between small and large firms. However, SMB and mid-size organizations are at risk on two fronts. First, they often lack the staff, money and tools that 24x7x365 security requires, making them an easy target. Second, it is relatively **easy and cheap for cybercriminals to leverage Ransomware-as-a-Service (RaaS)** or create sophisticated phishing scams that bypass traditional perimeter security defenses.

Once inside the network criminals can choose to act quickly, shutting down access to systems and data in search of a payday. Or they can lurk, watching and waiting for a more advantageous date to make their attack known.

If statistics prove anything, it seems that watching and waiting is common. IBM Security's 2023 *"Cost of a Data Breach"* report found **the average time for an organization to identify and contain a breach was 277 days.**

Yet these same breached businesses weren't necessarily negligent. **Most had invested in preventative tools like firewalls and antivirus.** They also had reliable IT support in the form of in-house or outsourced network operations center (NOC) services. ***Still, these preventative measures were not enough.***

To aid prevention, you must add the security operations center (SOC) services of detection, response and monitoring for more powerful protection.

Why Isn’t Prevention Good Enough?

Prevention, while critical, relies on traditional tools like firewalls and antivirus to **stop known threats.** Prevention is most often the purview of network operations center (NOC) services as the NOC team is responsible for ensuring the performance and regular maintenance of network devices and software. Security issues that arise often are dealt with reactively, most often after a network-impacting event.

In other words, **NOC services primarily focus on the smooth operational function of the network and its resources so that end-users enjoy a seamless, productive experience.** Meanwhile, **unknown threats often pass right through traditional security devices and software**, taking advantage of operational network performance requirements that speed traffic along to avoid costly bottlenecks that impact end-user productivity.

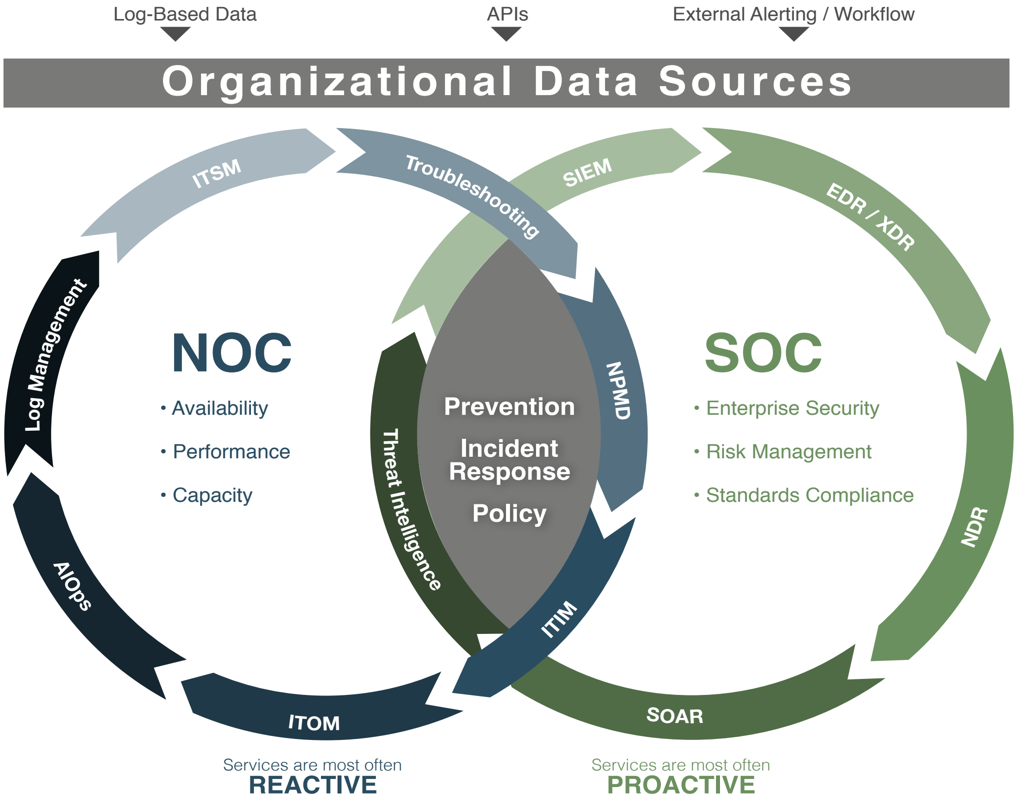

Fig. 1: Chart showing the responsibilities of NOC services vs. SOC services and how they intersect.

Many of today’s threats -- including zero-day exploits, recycled threats, and modified existing code – fall into the unknown category.

This is because they are truly novel or are too well camouflaged to be immediately recognized and stopped by traditional tools. As a result, these **unknown threats fall outside the scope of NOC services, including managed NOC services.**

To detect and stop unknown threats, you must add proactive intelligence to your arsenal in the form of managed SOC services.

We Detect and Stop Threats

Threat intelligence changes the game. Detection and response tools, unlike prevention tools, are smarter, typically built with capabilities driven by data science, and are a more effective ally for teams hunting unknown threats.

They help harness great intel to ensure rapid detection of malicious activity on your network that often slips past traditional perimeter defenses. **Detection and response is where Structured's Managed Security Operations Center (SOC) services deliver tangible value,** measured in:

- Stronger security across the organization.
- Lower levels of IT team fatigue and burnout.
- A more productive workforce.
- Improved ROI for IT tools.
- Increased customer trust.
- Better regulatory compliance adherence, which can translate to cyber insurance savings.

Structured Managed SOC services offer a complete Threat Detection and Response platform, including endpoint detection and response (EDR/XDR), intrusion detection (IDS), threat intelligence management (TIP), and event logging with next-gen security information and event management (SIEM). Further, our proactive platform integrates with any cyber threat intelligence (CTI) feed, including the most advanced systems.

Once threats are detected and logged, they are stopped with customized scripts, quarantined machines, and human intervention. Our specialized SOC analysts work each alert to validate real threats – separating them from the noise – creating fast remediation.

Perhaps best, our Managed SOC services are designed with individual client outcomes in mind. While they are built on standardized, trusted enterprise technology, they are flexible and adaptable to your unique environment.

We understand that an automated response, escalation or script that works well for one organization might cripple another, which is why we collaborate with you and your team from the outset to define and implement a successful program.

We also work with you after any incident to provide recommendations for larger remediation and security improvements.

Equipped with the tools, expertise and delivery framework to provide business-aligned and secure IT solutions, Managed SOC Services from Structured holistically support your enterprise from the ground to the cloud.

Enjoy peace of mind knowing that you have a large, highly skilled team of dedicated professionals monitoring, protecting and managing your mission-critical assets and data around the clock, all year long.

Advantage YOU

Structured’s Managed SOC services stem from a carefully curated and multifaceted approach involving prevention, detection, response and ongoing monitoring that includes both humans and data-science-driven machines.

We rely on advanced technology, human intervention, best practices and proven processes to protect and manage your network and data every minute of every day, minimizing risk, maximizing uptime, and maintaining compliance standards.

Compliance Services

With Structured’s Managed SOC services, we include a Ransomware Readiness/Resilience Assessment delivered by our Governance, Risk and Compliance (GRC) team.

Proactive incident prevention is critical for our clients. As network perimeters change with the addition of each new IoT technology, user device, SaaS application, and evolution of internet service, it is important to periodically review equipment configurations and solution effectiveness.

For many, 3rd party compliance services are mandatory to comply with regulatory requirements.

If you have a compliance mandate - or if you are simply vested in making your environment as secure as possible -- additional services can be added into a bundle as requested. This can dramatically improve your security posture and identify areas within your organization outside of the technology stack that need remediation.

- Ransomware Readiness/Resilience Assessment
- Pen Testing / Purple Team Exercises
- Vulnerability Scanning
- Virtual CISO / Policy Creation
- Cloud Security Posture Assessment
- Tabletop Exercises
- Compromise Assessment

About Structured

Structured is an award-winning solution provider delivering secure, cloud-connected digital infrastructure and managed services.

For nearly 30 years, we've helped clients through all phases of digital transformation by securely bridging people, business and technology. Customers trust us to provide valuable insight throughout the process of selecting and implementing secure and scalable IT strategies, platforms, processes and policies that meet modern expectations and drive measurable improvements throughout the enterprise.

Throughout this journey, they rely on us to provide design guidance, engineering assistance, and product recommendations that adhere to industry best practices, boost ROI, and – most importantly – maximize information security and regulatory compliance.

ALASKA MUNICIPAL LEAGUE

Alaskans face unprecedented cybersecurity risks, including increasingly sophisticated adversaries, widespread vulnerabilities in commonly used hardware and software, and broad dependencies on network technologies for day-to-day operation of critical infrastructure.

AML has negotiated an agreement with Structured, a local solution provider, for Managed SOC Services. These services are available to all eligible entities, including local governments, Tribal governments, and political subdivisions (public) of the state.

AICPA SOC aicpa.org/soc4so SOC for Service Organizations | Service Organizations ™

Structured Managed Services maintains the prestigious American Institute of CPAs (AICPA) SOC 2 certification.

Interested in Managed SOC? Get in touch!

Danny Maxwell, PMP

Territory Director
dmaxwell@structured.com
O: +1.907.230.2922