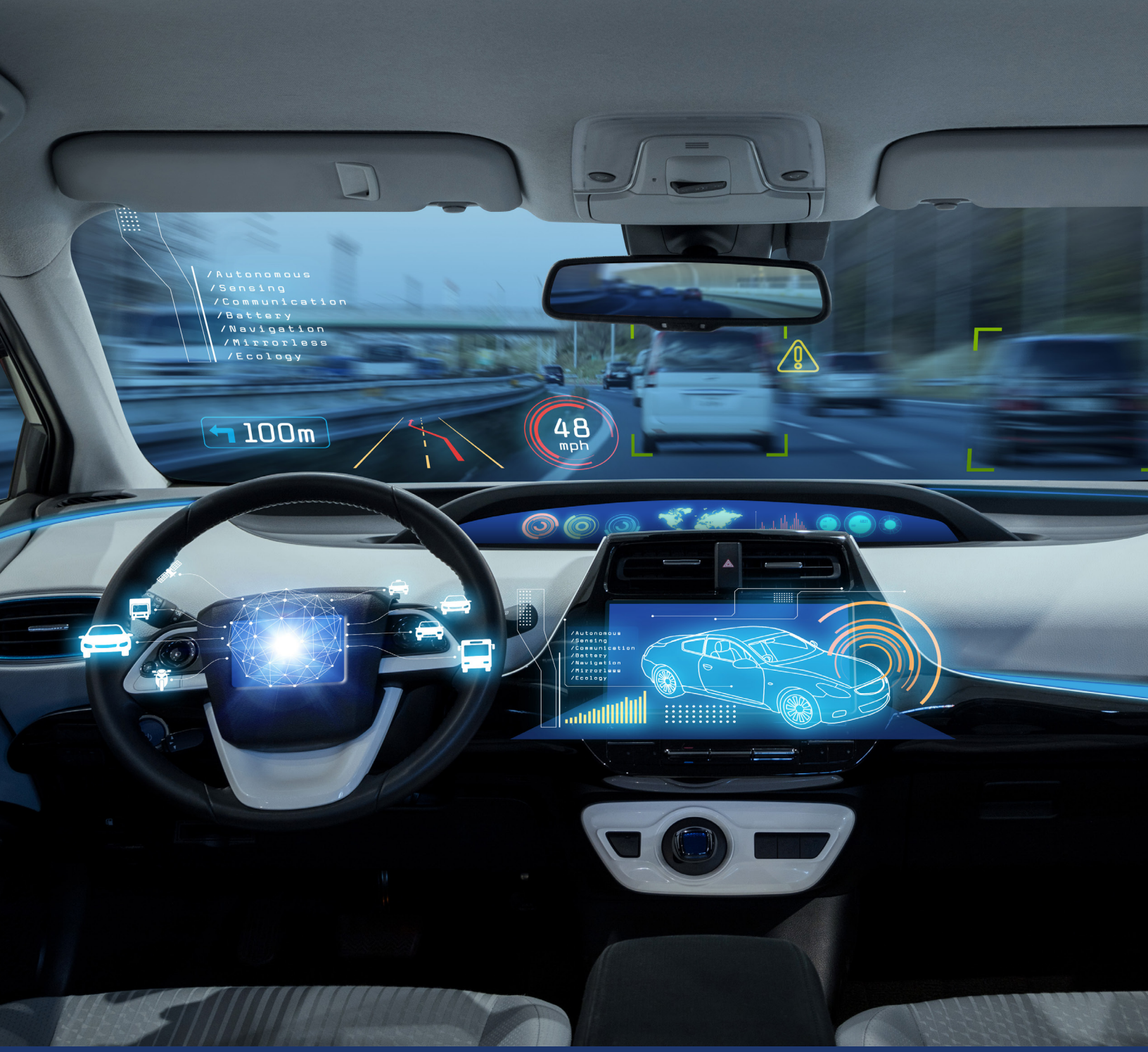


FROM ZERO TO SOC

Attaining a Security Operations Center without Breaking the Bank

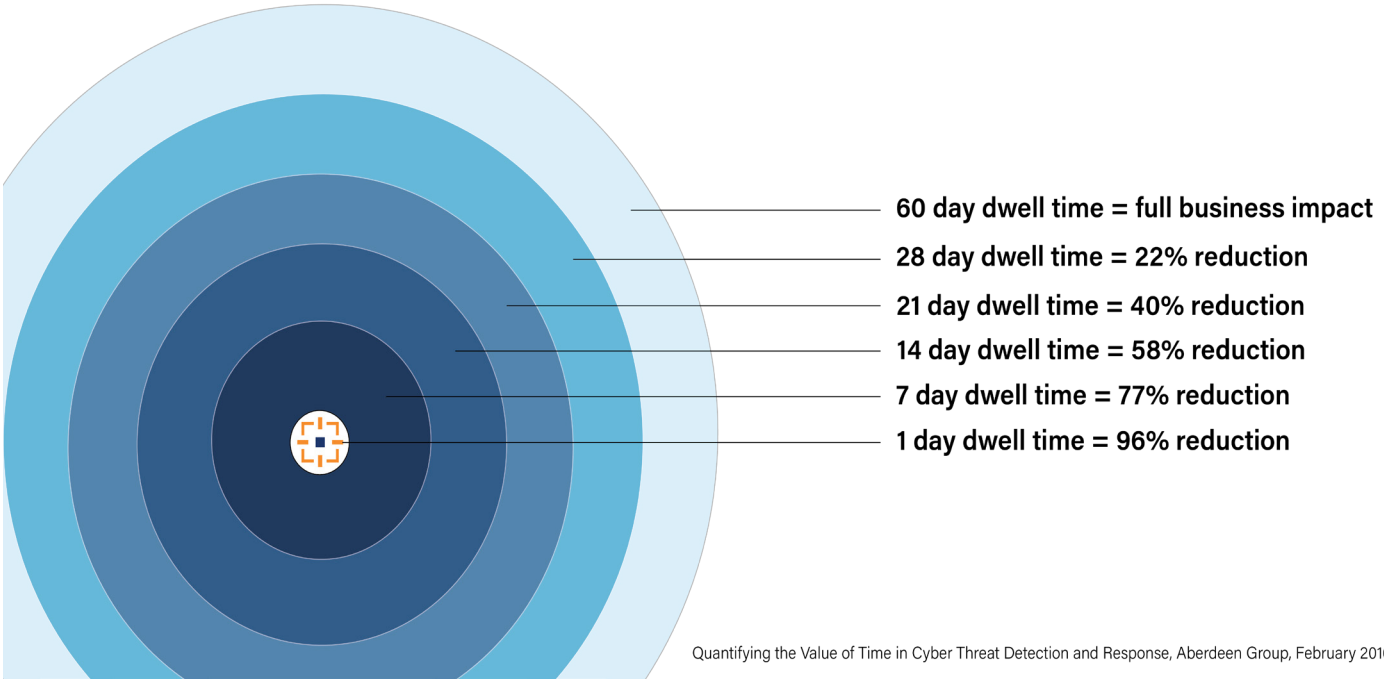
Netsurion™ | EventTracker

Every business–no matter its size–is a bullseye for cyber criminals. Data breaches cost an average of $3.6 million globally, according to Ponemon. Many people think the best way to bolster an organization's proactive protections is to build a security operations center (SOC) to monitor, detect, investigate, and respond to cyber threats 24/7. But there are many drawbacks: the cost of hardware and software is expensive; even more expensive is the challenge of attracting, training, and retaining skilled security experts in a world of high demand and low talent supply. This whitepaper lays out the real requirements for a SOC, and proposes a practical, affordable way to get the targeted, tailored protection your specific business needs without breaking the bank.

The issue: how to achieve continuous monitoring, immediate detection and rapid remediation

Security incidents happen all the time, and unfortunately organizations are usually unaware of them. They all too often find out too late, when data has already been exfiltrated, reputation damaged, customers put at risk, and revenues hit. What's needed is a way to find and deal with long-term threats as well as immediate attacks. If the organization could just do continuous monitoring and analysis of data activity, it could greatly increase the chances of detecting incidents. If you could look across your entire organization's network, including servers, workstations, applications, and databases continually–24/7/365–you would be able to reduce dwell time, the time between when attackers compromise a network (minutes), and when you discover them (currently months, according to the Verizon Data Breach Investigation Report 2018.) The average dwell time for a business is six months.

Reducing Dwell Time Reduces Business Impact



Quantifying the Value of Time in Cyber Threat Detection and Response, Aberdeen Group, February 2016

A good SOC must have three key interrelated components: platform, people, and processes.

SOC seems to be the answer

You want to be able to monitor all security-related events holistically, from a centralized location, and be able to quickly separate true problems from false positives and noise. That's the classic definition of a SOC–a centralized headquarters for monitoring, detecting, and responding to security issues and incidents. The team–whether a real physical group of people working together or a virtual organization-tracks security alerts, investigates, and validates them around the clock, ensuring timely response. In short, the SOC has overall responsibility for defending against cyberattacks. The concept of a SOC is increasingly common in business discussions: as customers and shareholders learn about security, they see a SOC as a key element in building trust.

Components of a good SOC

A good SOC must have three key interrelated components: platform, people, and processes. It takes all three, working in concert, to achieve the goal of cybersecurity defense. It's worth looking at each of these and understanding how they are intertwined.

Platform component

It takes a number of tools and technologies to build the infrastructure for a comprehensive SOC. First and foremost is the security information and event management (SIEM) system. A complete, tuned SIEM provides the visibility foundation for the platform. Additional elements include firewalls, IPS/IDS, vulnerability assessments, and threat intelligence feeds, so the SOC staff can correlate and analyze activity. Additionally, endpoint monitoring technologies that scan for vulnerabilities, protecting sensitive data, and ensuring compliance with industry and government regulations, feed into the platform. Other vital components of a SOC platform are internal and external threat intelligence from global sources, threat intelligence that is local to your organization (normal and abnormal patterns of behavior) and that is contextual (those threats that are applicable to your industry, your organization, and infrastructure). As with information on known vulnerabilities, this must be continuously kept up-to-date. But no platform can ensure optimal detection unless machine learning is applied to the massive amounts of data that flow through it, and it is fine-tuned by human experts: the people component.

People component

A SOC calls for a dedicated team of highly skilled security analysts, with the bandwidth to monitor 24/7. To be able to configure security monitoring tools, do triage, perform root cause analysis, and conduct in-depth threat hunting, they need sysadmin skills, expertise in a variety of programming languages, in-depth security knowledge, and relevant certifications such as CISSP, GCIA, GCFA, and the like. In today's market, the shortage of security experts is well known: industry group (ISC)² predicts there will be a global shortage of almost two million cybersecurity professionals by 2022. In fact, in a 2018 study by industry analysts at ESG and ISSA, 70% of cybersecurity professional say the skills shortage has had an impact on their organization: it increases their workload, makes them resort to on-the-job training of lower-skilled individuals, and forces

There are three basic ways to reach the goal of finding and mitigating threats: build your own SOC, use a SIEM-as-a-Service offering (sometimes called SOC-as-a-Service), or take a co-managed approach.

the security staff to spend most of its time on emergency issues rather than being proactive or strategic. Those organizations that can find and hire security experts must work constantly to ensure their most valuable team members are not hired away by the competition. Being an effective member of a SOC team calls for skills, discipline, and a clear understanding of all the necessary activities that must be carried out, which leads us to the process component.

Process component

Processes related to a SOC are based on a clear definition of the strategy that incorporates business-specific goals and the organization's specific risk tolerance. Documentation of the strategy, goals, and risk posture forms the basis for process documentation: each stage of an investigation is spelled out in detail. Incident handlers will usually follow a detailed playbook-a multi-page document (often running 20-30 pages) that spells out exactly what to do in the event of specific types of incidents, such as ransomware, unauthorized admin access, malware infection, website defacement, multiple simultaneous logins, etc. The playbook includes sample report and notification templates and details processes and procedures such as incident classification levels, evidence-gathering, internal and external notifications, investigation techniques, how to deal with false positives, and how and when to escalate. SOC processes call for continuous monitoring, since attackers don't take breaks during off-hours. To ensure the highest quality SOC, an organization may want to pursue ISO certification to demonstrate that proper information security controls are in place.

SOC on a budget? Three realistic approaches

Obviously, it takes a sophisticated combination of people, processes, and platform to run a SOC. It's hard to see how an organization can assemble a seasoned security team with the requisite level of expertise, put in place all the necessary processes, and ensure 24/7 monitoring based on a comprehensive technology platform without spending a lot of money. Even if the platform can be implemented, most companies fall short when it comes to processes and people with the expertise to carry them out.

There are three basic ways to reach the goal of finding and mitigating threats: build your own SOC, use a SIEM-as-a-Service offering (sometimes called SOC-as-a-Service), or take a co-managed approach. It's important to understand the costs and benefits of each and see what your organization would be signing up for.

Approach 1: Build your own SOC

An in-house SOC requires all the above components: platform, people, and processes. On the plus side, it gives you full control over the SOC: you determine your organization's risk tolerance level, you decide which threats fall outside that level, and you can implement your own specific investigation, detection, analysis, and remediation processes. On the minus side, the costs are significant and implementation complex.

People: You will need to staff up with a dedicated team that has the expertise and skills to monitor round

the clock. They must be security experts, with skills and regularly-updated knowledge if they are to do the monitoring, investigation, triage, and detection. They will need to be experts in correlating the many, often obscure, indicators of compromise, and not succumbing to alert fatigue (the tendency to become desensitized to an overwhelming number of alerts, leading to longer response times or missing an important alarm altogether). And they must be able to take swift, effective action once a threat is detected. Such a team does not come cheap, and once built, it will be a constant effort to fend off competitors trying to hire them away.

Process: You will need to define and rigorously adhere to all the relevant processes to support the skilled security team, equipping them with documented playbooks for detecting, analyzing, and remediating threats. Their procedures must include details on how to collect and correlate data, and when and how to escalate issues. To ensure you are following industry best practices, and satisfy customer and shareholder inquiries, it's worthwhile to obtain ISO certification. It will take a significant budget commitment to ensure that the processes are in place for an in-house SOC.

Platform: The technology component is perhaps the easiest of the three, although not necessarily the least expensive. You will need a variety of software solutions and the hardware and infrastructure to support them. The cornerstone is a SIEM—choose one with a proven track record and that is easy to use. An intrusion detection system (IDS) must be integrated with it, along with User and Entity Behavioral Analysis (UEBA) tools. An Endpoint Detection and Response (EDR) solution should be integrated with the other components, and continually updated with the latest threat intelligence. Each of these technologies, in turn, requires a level of expertise to implement, configure, tune, and maintain, not to mention the skills required to analyze and correlate any alerts that are presented.

Look at this as if you needed to get from point A to point B. In the "build your own SOC" approach, you would buy a car. Then you would be responsible for its operation, maintenance, troubleshooting, as well as driving. You have total control of every detail. But it's an expensive proposition.

Approach 2: Use a SIEM-as-a-Service offering

This approach allows you to use a SIEM that is owned and maintained by a third party. You do not need to purchase hardware and software or maintain your own SIEM. Your cloud access lets you run the SIEM as if it were on-premises, meaning that many of the platform components become much more manageable. You no longer have to worry about the perpetual software license, updates, introduction of timely threat intelligence, etc. You retain the ability to determine which threats fall within your risk tolerance, how they are prioritized and analyzed, and how they are remediated.

However, the people issues, and the process issues mentioned above, remain. You will still be responsible for finding, hiring, training, and retaining skilled security experts, and making sure they do not become less effective over time due to threat fatigue-the result of a constant barrage of alerts coming from multiple technologies. You will also need to make sure your processes for detecting, analyzing, prioritizing, and remediating threats are comprehensive, documented and, if possible certified.

To continue our car analogy, in this case you would rent a car to get from point A to point B. You have saved yourself the purchase price of the car, and eliminated the maintenance and upkeep, but you are still responsible for any ancillary expenses related to the use of the car (gas, parking fees, tolls, etc.) The people and process issues remain. It's still an expensive proposition, but a little less expensive than the "build your own SOC" approach.

Approach 3: Choose a Co-managed SOC approach

The innovative co-managed SOC (also called co-managed SIEM) approach combines your internal staff, and your organization-specific goals and tolerances, with an outsourced SOC team that brings all the essential security monitoring technologies—including SIEM—on a single platform. This is not simply a managed SIEM with a one-size-fits all, preconfigured set of security controls. It's a SOC that is managed jointly by you and the outsourced team. Your role is vitally important, since you know the nuances of your own network—you are the subject matter expert on "what's normal"—and you have deep knowledge of your business. By communicating that knowledge, you accelerate the outsourced SOC team's ability to understand your business and environment. As a result, you get the best of both worlds: the highest level of tailored protection, at the lowest total cost. In this scenario, you are in control of the risk tolerance of your organization, you can specify which threats are important to you, and you can dictate how issues should be escalated and prioritized. Meanwhile, the costs and complexity of the people, process, and platform issues decrease dramatically as you pass those off to the outsourced team of security specialists.

You don't have to worry about how to find skilled security experts in today's tight job market, pay for ongoing training, or worry about them leaving for a better job somewhere else. With a co-managed SOC, your team doesn't worry about detection, investigation, analysis or escalation. Their focus is solely on remediation. When it comes to process, you need only define your strategy and make sure you have the processes in place for incident remediation. Your co-management tasks are to educate the SOC team about specific risk tolerance, train them on what represents a threat to your organization and what does not, and then to remediate any threats that are escalated to your in-house team. All the rest—documentation, discipline, continuous monitoring, incident playbooks for detection and analysis of various threats, and ISO certification—is the responsibility of the SOC that you co-manage (rather than owning or renting it.)

To continue with our car analogy, you would get from point A to point B via a ride-sharing service (e.g. Uber or Lyft). You are still in control of the destination, and you get the results you want, but the cost and complexity are dramatically reduced.

Conclusion

The question is whether you can achieve an effective SOC on a budget. If you choose to buy or rent a SOC, the answer is yes…but it's going to have to be a pretty big budget! There is no way to sidestep the time, effort, and costs of building and retaining your own in-house SOC team to monitor and analyze 24/7. There is no way to avoid the costs of creating all the processes, documenting them, testing them, and training your team on how to implement them. And there is no way to circumvent the need to be experts in all aspects of cybersecurity. If the goal is to ensure constant cybersecurity protection in a way that is tailored to your organization's specific needs, clearly the most cost-effective path is through a co-managed SOC.

A co-managed SOC, on the other hand, provides all the benefits of an in-house SOC with almost none of the disadvantages. Clearly the TCO will be lower, because you avoid a wide variety of costs. (For a thorough review of the cost savings, see our online TCO calculator.) CapEx costs associated with hardware and infrastructure are not going to be a factor. The costs and the challenges associated with finding, hiring, training, and retaining a full in-house team of security experts, and setting up all the needed processes, can be avoided; ongoing OpEx costs are dramatically reduced, since the bulk of the work will be done by the outsourced co-management team.

As important as budget is for all organizations, keep in mind that the goal of a SOC is to protect your specific

organization. For that reason, it is vitally important to ensure that the SOC team understands and can tailor its activities to your environment, your risk tolerance, your definition of abnormal behavior, and your business-critical assets and data. Your co-managed SOC team can monitor, detect, and escalate security issues and incidents in a way that makes sense to your organization, leaving the all-important task of remediation to your own in-house team. A co-managed SOC provides the muscle and expertise to track and validate security events around the clock, while letting you retain control over your own environment. Surely this is the best of both worlds.

Netsurion has been providing co-managed security capabilities based on our own EventTracker SIEM to companies of all sizes for years. For more information, visit www.netsurion.com/SIEMphonic.

About Netsurion

Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion's SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion's SD-WAN edge appliance.Netsurion's Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.