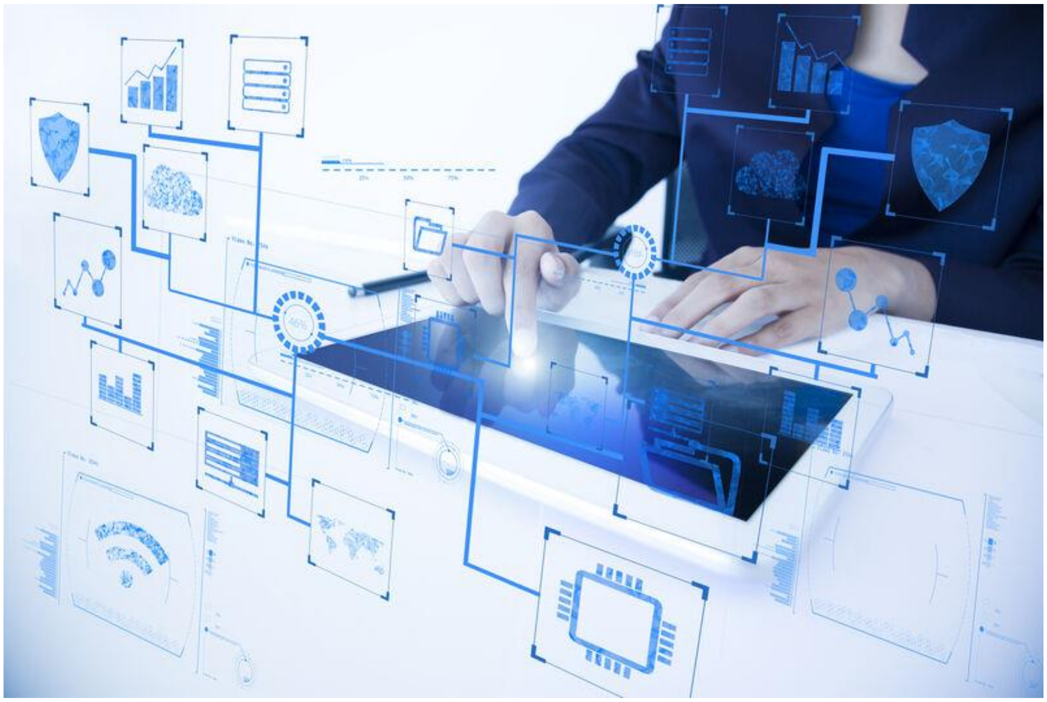
Electrosoft

TECHNOLOGY REPORT:

SECURITY OPERATIONS CENTER (SOC)



Prepared July 12, 2022

INTRODUCTION

A Security Operations Center (SOC) is a highly specialized operation staffed by IT specialists with an information security background. These professionals employ sophisticated knowledge and tools to perform a variety of cybersecurity functions including

- Threat detection, analysis and forensics related to activities occurring on a network and the systems that are part of the IT environment
- Endpoint protection of the laptops, workstations and servers comprising the network
- Compliance and vulnerability management to assure system and endpoint configurations and settings are secure and comply with applicable regulations
- Data loss prevention to protect against unauthorized data exfiltration
- Security architecture reviews and special projects to enhance cybersecurity posture

As discussed previously in Operating SOCs in a Time of War, Electrosoft is leading the way in redefining what a SOC is. We believe that today's SOC is not so much a place (physical locale) but rather a functional team (experienced professionals) providing a service (cybersecurity) that can be delivered from any locale. Cloud-based tools and applications enable our SOC staffs to operate remotely from any locale. This approach, which proved invaluable during the Covid-19 pandemic, is opening minds to a number of advantages that come with a geographically dispersed staff. These include enhanced recruitment opportunities and continuity of operations should a power or internet failure occur in a region.

The need for SOCs is growing as evidenced by the increasing incidence of cyberattacks. Citing multiple sources, TechTarget recently reported some sobering statistics:

- The number of attacks grew by 31 percent from 2020 to 2021.
- The FBI alone received 791,790 internet crime complaints in 2020.
- Over 90 percent of cyberattacks are launched via spear phishing emails, a technique that targets individuals based on their social media presence.
- Data breach identification and containment can take an average of 287 days.
- As of December 2021, the United States faced a security workforce gap of 377,000 jobs.
- By 2025, the estimated cost of cybercrime will be $10.5 trillion.

Many organizations are looking to operate their own SOC or outsource that function. Either way, SOC creation and operation are not without challenges. Electrosoft recently convened experts from government, industry and academia to discuss the role of SOCs as part of an effective enterprise cybersecurity program and explore the many challenges inherent in building and operating an effective SOC. This technology report summarizes the lessons learned from Electrosoft's expertise in operating SOCs on behalf of federal agencies and the expert opinions expressed during the virtual technology summit.

MANAGEMENT OPT-IN

We find – and the experts agree – that cybersecurity is no longer a fringe activity. It is an essential business process, vital to every organization regardless of size or industry sector. Yet, convincing management that the investment in a SOC is worthwhile, whether outsourcing or building it in-house, can be a challenging proposition.

The optimal time to broach the subject is before a breach occurs. Being proactive is paramount, as prevention surpasses reactive measures. However, the power of an urgent crisis to prompt executive action cannot be overlooked.

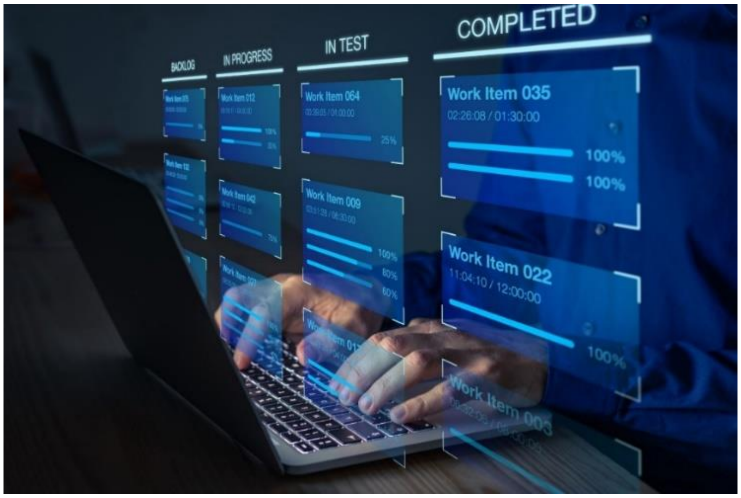
Possessing a positive relationship with the C-suite is seen as a prerequisite to success. So, too, is being frank, offering realistic observations of exactly how a breach would impact specific business functions or missions. An important theme is that a cyberattack is not an “if” propositions; it is a matter of when.

Wherever possible, it’s important to underscore the business value of investing in cybersecurity. A risk-opportunity matrix can be invaluable in this regard. The focus should be realistic breach scenarios that include estimated costs for each event envisioned. For example, a denial-of-service attack equates to an entire organization that can’t work. Computing the personnel costs and lost revenue for the downtime; the expenditures required to evict, remediate and recover; and the cost of hiring outside consultants and potentially acquiring new hardware and software helps quantify impact and makes a potent argument.

Every SOC budget proposal must include costs for remediation (catch up), cyber hygiene (heightened staff awareness) and insider threat (assure no one is being extorted) in addition to operating costs. Most important, management buy-in is essential to any cybersecurity program.

KEY SUCCESS METRICS

Technical metrics, such as vulnerability against remediation and uptime versus downtime, are straightforward, with most cybersecurity programs doing a good job of identifying and tracking them. Business-centric metrics are more challenging to formulate. How do you encapsulate SOC productivity and tie it to the overall return on investment and/or the value added to the business? How much is the SOC saving? How much is your phishing training program saving the business? What value do you attach to your customers not being able to reach you? What value captures your workers not being able to do their jobs? Brainstorming sessions are invaluable in discerning the right metrics for each organization.



Most executives grasp metrics such as data integrity, data confidentiality and data availability, as they readily align with usual business functions. It's also important to formulate basic business unit estimations such as, How long can each business unit exist without the network operational? How long will it take each unit to transition to a backup site and come online again?

Other metrics, such as the cost of an employee clicking on a bad link or opening an infected email, readily demonstrate impact for purposes of employee awareness training. They also help assure you've established the right internal training programs.

FEDERAL SOCs AND OUTSOURCING

State and local agencies like the fixed price, tools and skilled personnel available via a managed security service model. There is a place for outsourcing within the federal government, too, but data integrity and confidentiality requirements often dictate that some operations must remain internal.

A hybrid approach to SOCs, where some cybersecurity operations are outsourced and others remain within the agency, is feasible for many federal organizations. For example, threat hunting and forensic analysis are functions that should always remain within an agency. Conversely, vulnerability scanning and analysis as well as remediation activities can be outsourced.

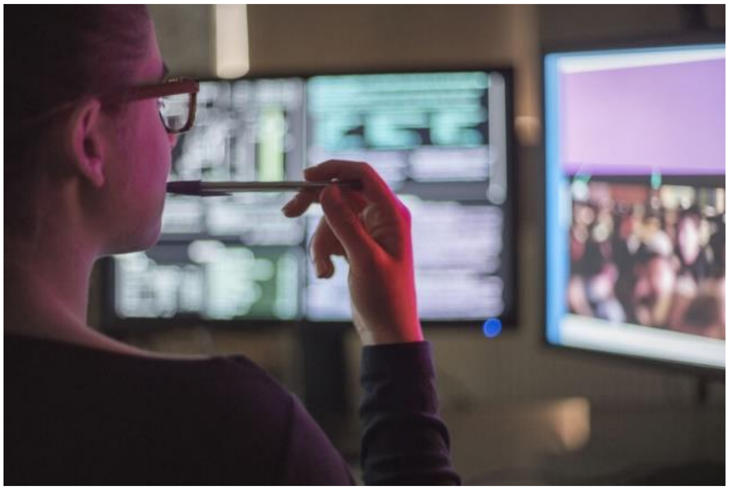
Of course, size matters, and it's not a one-size-fits-all proposition. Funding is a key factor in that regard. Small and medium-size operations won't have the resources to perform every function. Thus, it's often a necessity to construct individualized cybersecurity operations relying on service-level agreements. Yet, regardless of size, no vendor should dictate how continuity of operations will occur. The organization must describe how it will continue to operate, leaving it to the consultants to calculate the amount of time needed to get back online.

Being resource limited tends to make an organization select functions that are more mission related. In government, though, security officials must remember that they cannot transfer risk to someone else via outsourcing. They retain ultimate responsibility for their data, so they must always retain complete visibility. The risk transfer option doesn't work well in the federal model.

HIRING ANALYSTS AND SKILL CURRENCY

Hiring someone to sit at a desk and monitor a screen for 8 to 10 hours at a time is difficult. It's shift work and can be quite trying. Plus, it's no secret that cyber analysts have their choice of jobs now, and salary is a major deciding factor. Defense and federal civilian programs trying to infuse cyber talent have a hard time competing with the private sector.

One technique is to focus recruitment efforts on recent graduates who need to gain experience. It goes without saying that a degree or certification means nothing until someone has executed tasks such as system intelligence monitoring, alert management, incident response and analysis, threat hunting, intrusion detection and more.



Creating and growing a pipeline are key. An important talent source can be individuals retiring from the military services. Often, a direct appeal to their sense of patriotism can be persuasive. Likewise, conveying the job challenges inherent in protecting the nation's intellectual property can heighten job interest.

Another talent source can exist within the hiring organization. Select middle managers or program managers might be open to the career opportunities available in the cybersecurity field and be willing to transition to a new career ladder after training. Communicating with employees via internal newsletters or job boards can assist such efforts.

Retaining good analysts is a challenge. So, too, is creating meaningful training and incentive plans. Work-life balance is important, as is a path for career growth. Ongoing training in new tools and techniques is critical. Incorporating these and other factors can improve not only SOC analyst performance but also continuity within an organization.

SECURITY, COMPLIANCE AND EFFECTIVENESS

If security is only about compliance, an organization has already failed. Likewise, being compliant and being effective are two different things. Compliance has its place but being effective is more important. Prioritize effectiveness and compliance will fall in place.

At the end of the day, it's all about protecting data, i.e., getting the right data to the right user at the right time. When you provide authentication (username and password), there's compliance but not effectiveness. Moreover, a system can achieve Authorization to Operate (ATO) and be compliant with hundreds of controls. Yet, placing a list of the requirements demanded by a Zero-Trust Architecture side-by-side with the ATO controls often reveals a system that comes up short on the effectiveness scale.

Some experts believe too much money is wasted pursuing an ATO or a System Security Plan (SSP). They feel that a minimally compliant application often is preferable, as getting something completed now increases the time to add security in the next sprint. They assert that evolution via incremental change is better than revolution.

One key theme regarding effectiveness involves SOC analysts: They should not have to focus their efforts on the repetitive alerts so often generated, especially since so many involve false positives or mundane issues. Automating them frees these professionals to focus on higher-level activities deserving of their time and expertise.

Discussions on effectiveness would be incomplete without touching on the importance of holding regular security exercises involving red teams and penetration testing. Practice is the only way to assure that SOC staff will be effective in dealing with a real cyber threat when it occurs.

PROCESSES

Technology must keep up with emerging threats and real-world adversarial approaches. Tactics, techniques and procedures (TTPs) are growing every day, and advanced persistent threats (APTs) are getting smarter and harder to identify. Artificial intelligence (AI) and machine learning (ML) are key to making processes more streamlined and effective. What's more, streamlining often leads to cost savings.

When talking about processes, the need to hold regular exercises is worth repeating. Formal exercises instill the type of repetition and learning often only achieved in battle drills. They identify skill gaps within SOC staff and provide the opportunity to address these shortcomings before an actual breach occurs. Regular practice assures SOC staff know the response plan and their role in executing that plan.

CORE CAPABILITIES AND TOOLS OF MODERN SOCs

Sometimes we get enamored with tools and forget about the basics. It's not about replacing people. It's about implementing tools that enhance the SOC staff's capabilities.

Tools should be both physical and logical. They should fit a purpose. If the purpose is monitoring, for example, it's easy to acquire the best monitoring tools available in the marketplace. But, if these tools result in so many false positives that the SOC staff can't sift through them all, what logical good has the tool achieved? Here is where AI adds value.

Consider AI as *augmented* intelligence rather than *artificial* intelligence. Then, select those AI tools that augment SOC analysts rather than create more work. Free them to perform the analyses that AI can't do. Then, let AI handle the rest.

SOCs should have threat intelligence tools, compliance tools, Security Incident Event Management (SIEM) systems and Security Orchestration, Automation and Response (SOAR) technology. Relative to SOAR, the orchestration component is important as it speaks to the maturity of the SOC and how well the members function as a team.

At the heart of a modern SOC is a solid Structure Synth, a tool for creating 3D images. Likewise, modern SOCs should have EDR (endpoint detection and response) and XDR (extended detection and response) systems to enhance threat detection and speed response.

• • •

Readers interested in watching the video of the full Virtual Technology Summit panel discussion can access it on the Electrosoft website under Resources or on our YouTube channel.