The Evolution of Security Operations and Strategies for Building an Effective SOC

Cybersecurity threats are becoming increasingly complex, sophisticated, malicious, well organized and well funded. The widespread adoption of artificial intelligence (AI)-powered tools and technologies will lead to customized, high-impact cyberattacks. Addressing the complexity and sophistication of such attacks requires an empowered security operations center (SOC).

A SOC is a facility that houses cybersecurity professionals responsible for real-time monitoring and investigating of security events to prevent, detect and respond to cyberthreats using a combination of people, processes and technologies.

SOCs are responsible for monitoring and protecting the organization's assets including intellectual property, confidential/personnel data, business systems, critical infrastructure and brand reputation from cybersecurity threats. SOCs serve as the eyes and ears of an organization, raising the alarm when suspicious or an abnormal cybersecurity events occur and enabling a quick response to reduce the impact to the organization. Due to the adverse impact of security incidents, organizations are looking for ways to improve their SOCs to reduce their exposure and keep their assets and data secure.

Understanding the evolution of and building a successful and effective SOC can greatly enhance the ability to detect and disrupt cyberattacks, protecting the organization from harm.

SOC Evolution

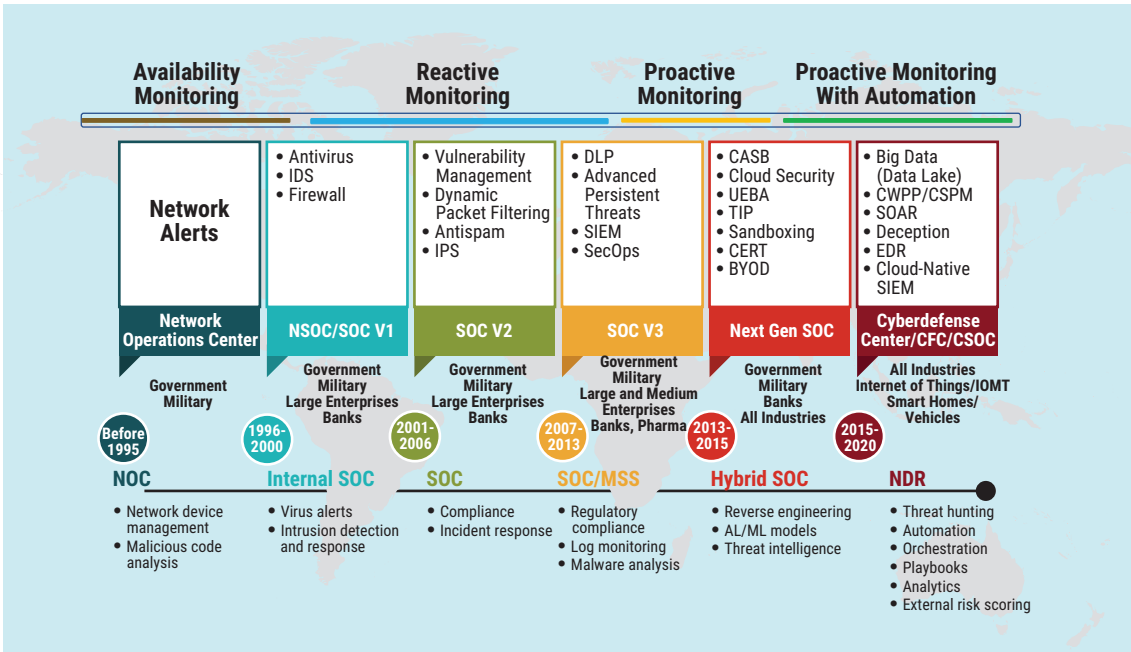
In the past, a traditional network operations center (NOC) would focus on incident detection and response with availability as the primary objective. A NOC's key responsibilities were network device management and performance monitoring.

As illustrated in **figure 1**, originally, SOCs were implemented for government and defense organizations. The major responsibilities of an early SOC included handling virus alerts, detecting intrusions and responding to incidents. After 2000, large enterprises and banks started implementing similar monitoring operations.

The Information Security Management Standard was released in 2005, and compliance was added to the SOC's objectives.[1] Dynamic packet filtering firewalls, antispam and vulnerability management,

Lakshmi Narayanan Kaliyaperumal, CISA, CISM, EnCE, GNFA
Is vice president and head of cybersecurity technology and operations at Infosys. Kaliyaperumal established and maintains an organizationwide cybersecurity program, global cybersecurity strategy, security operations, compliance, application security and effective operating model to ensure information assets and related technologies/processes are protected in the digital ecosystem hosted in the cloud or on-premises. Kaliyaperumal has more than 20 years of cybersecurity and IT experience in various leadership roles at Infosys with a focus on cybersecurity, secure engineering, risk management, security controls, enterprise security architecture and cloud transformation.

Figure 1—Evolution of the SOC



and intrusion prevention were added for monitoring and response.

The era between 2007 and 2013 was the golden age for SOC evolution. Many important security solutions that are key for security monitoring, such as data leakage prevention (DLP) and security information and event management (SIEM), entered the cybersecurity ecosystem during this time. The number of advanced persistent threats (APTs) significantly increased during this period, with an 81 percent increase from 2010 to 2011,[2] and SOCs played the major role in detecting and preventing them. Log aggregation, regulatory compliance, malware analysis and DLP were key objectives of security operations in that era.

Managed security service providers (MSSPs) also emerged for IT and security operations. As a shared model, managed security service is not exclusively dedicated to a single organization or entity. MSSPs were initially adopted by large enterprises and then eventually adopted by small and medium-sized organizations interested in employing them to meet their organizational security operation requirements.

In the evolution of the SOC, next-generation SIEM entered the security ecosystem and operations journey. SIEM is also referred to as user entity behavior analytics (UEBA) and is based on machine learning (ML), which is a subset of artificial intelligence (AI).

Organizations deployed UEBA on top of existing SIEM technology to reduce the false positives. SIEM is a rule-based technology that works based on a logic and threshold set for the rules. The threshold parameter is a major challenge for SIEM technology because it is impossible to keep the threshold open for more than a few hours. If the threshold is open for too long, then performance of SIEM will diminish significantly. Since the advent of mobile technologies, bring your own device (BYOD) and cloud adoption, identity and access are core components of security management. UEBA/user behavior analytics (UBA) technologies use identity and access to define normal and anomalous user and entity behaviors.

Security operations driven by threat intelligence, reverse engineering and AI/ML-based monitoring technologies have changed next-generation SOCs.

Hybrid SOCs—deployed and operated on a customer's premises by an MSSP—emerged during this time. Hybrid SOCs are also referred to as remote SOCs.

In 2015, threat intelligence platforms (TIPs), open-source intelligence (OSINT) and commercial threat intelligence feeds became core components of security operations.[3] Threat intelligence enriched the context of incidents and helped security analysts make the decisions. Threat intelligence also created visibility on adversaries' tactics, behaviors, tools and processes. Tactics, techniques and procedures (TTPs)-based threat hunting added more value to SOCs by enabling early detection and remediation of hidden threats.

> "THE SECURITY OPERATIONS JOURNEY STARTED WITH A REACTIVE APPROACH THEN MOVED TO A PROACTIVE APPROACH AND NOW EMPLOYS A PROACTIVE PHASE THAT INCLUDES AUTOMATION."

Cloud migrations started during this time, and cloud security solutions such as cloud access security brokers (CASBs) entered the security market to shine a light on shadow IT and shadow data in the IT and security community. The SOC's monitoring responsibilities expanded to include cloud, and sophisticated threats also increased during this time. Cloud security posture management (CSPM), cloud workload protection platform (CWPP), cloud-based endpoint detection and response, and cloud-based hunting are new capabilities added as part of modern security operations.

Cyberdefense center (CDC), cyberfusion center (CFC), cybersecurity operation center (CSOC), cybersecurity incident response team (CSIRT) and joint operations center (JOC) are new names coined for the SOC after 2015. The security operations journey started with a reactive approach then moved to a proactive approach and now employs a proactive phase that includes automation.

Soon, more than 50 percent of SOCs will be migrated to modern CDCs integrated with automated threat hunting and incident response capabilities.[4, 5] Organizations not yet on their SOC journey can start with MSSP, then move to a hybrid SOC model and finally reach their own mature SOC. A modern CDC or CFC provides the following services:

- Security event monitoring, detecting, investigating, triaging
- Malware analysis, reverse engineering, digital forensics, insider threats, cyberfraud
- Threat intelligence platform management
- Threat hunting
- Content management
- Threat and vulnerability management
- Compliance
- Reporting and notifications
- Training
- Identity and access governance

SOC Challenges

False positives are the biggest challenge for SOCs (**figure 2**); more than 50 percent of SOC analyst efforts are allocated to handle false positives.[6] Integration of log sources, out-of-the-box use cases and rules without validation are major contributors to false positives. Lack of context to incidents and threshold-based correlation rules is a challenge for security analysts. Threshold-based correlation rules have been converted into ML models since the integration of AI/ML monitoring solutions. This integration of threat intelligence solves the problem of missing context.

Over time, siloed solutions have been added into SOC monitoring, and security analysts have to toggle between multiple consoles to respond to incidents. Training people on multiple technologies in a short span of time is impossible. Documenting and updating the security incident

Figure 2—SOC Challenges

playbooks/runbooks and maintaining up-to-date knowledge bases require a lot of effort but are key for any SOC.

Multiple-point solutions increased the number of incidents for security analysts. Repetitive tasks and alert fatigue are the major reasons why security analysts leave security operations positions.

Traditional SIEM solutions and next-generation SIEM solutions do not have the capacity to calculate mean time to detection (MTTD) and mean time to response (MTTR) for incidents by default. Manual efforts are required to enable these kinds of calculations and metrics.

SOC Challenges After a Pandemic

Both the pandemic and remote work have created cybersecurity challenges as illustrated in **figure 3**.

- **Collaboration**—Typically, a security operations team comes together in a secure place with specialized systems, monitors and network to collaborate easily to respond to advanced threats in person. Since the COVID-19 pandemic started, collaboration has become a challenge, and virtual collaboration tools and war rooms are the best available solution.
- **SecOps tools**—Analysts must respond to and mitigate threats through remote access. Access to specialized SecOps tools is another major challenge, as multifactor authentication and security must be enabled.
- **Systems design**—SOC team analysts typically worked with wide-screen dual monitors and customized hardware. In the wake of the pandemic, SOC analysts are facing challenges to achieve the same productivity with their laptops.
- **Health and wellness of security operations teams**—This is crucial to any organization. Enterprise leaders must focus on their SOC teams' health and wellness to continue the fight against current and future emerging threats.
- **Separate virtual private networks (VPNs)**—Implementing alternative VPN access to critical SOC systems is the newest challenge to overcome, to allow fallback mechanisms if the infrastructure is compromised.
- **New threats**—Threats such as double extortion ransomware, phishing using artificial intelligence techniques, ransom distributed-denial-of-service (DDoS) attacks and privilege access attacks have created new challenges for SOC teams. Maintaining secure communication channels and separate VPNs for security operation technologies are the newest challenges to overcome.
- **Secure communication**—Normally, SOC analysts communicate face-to-face in the physical SOC. Communicating artifacts, evidence and screenshots have become challenging in the work-from-home model.
- **Remote SecOps**—SOCs are physical sites and cannot be replaced fully with virtual environments.

Figure 3—Challenges After a Pandemic

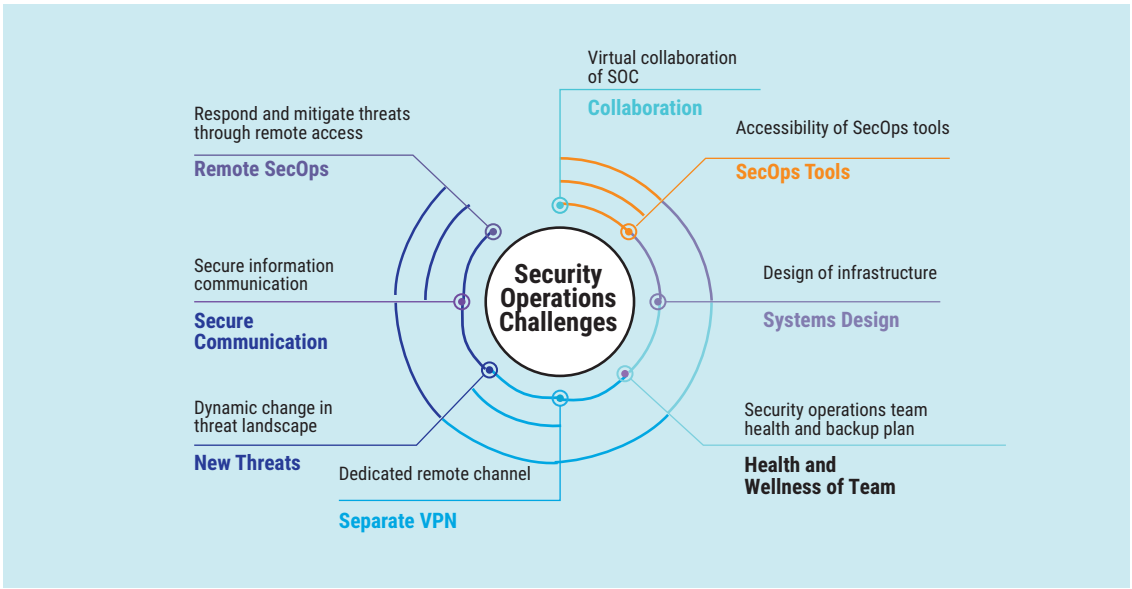
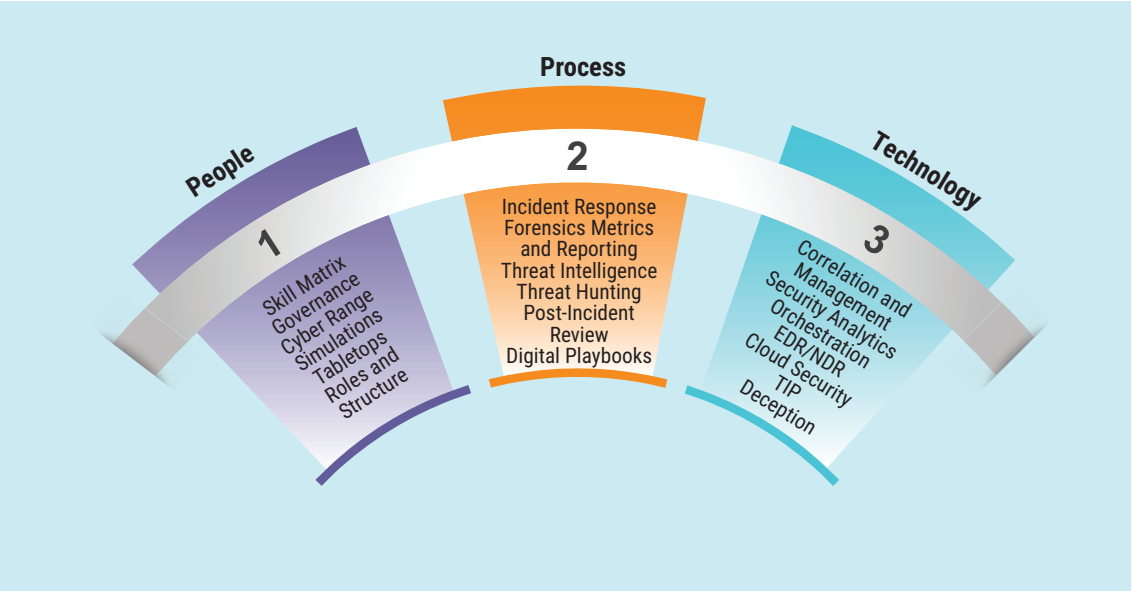


Figure 4—Critical Components of the SOC



Strategies to Building an Effective SOC

Organizations can benefit from SOCs using minimal resources and time with the help of people, process and advanced next-generation technologies (**figure 4**). Building an effective SOC requires understanding the needs of the organization as well as its limitations. The following best practices will help organizations build an effective SOC with the right tools and technologies and within the budget, once the needs and limitations of the organization are understood.

Consistent Executive Management Sponsorship
The chief information security officer (CISO) or chief information officer (CIO) should review and sign off on the scope of the SOC and continuously monitor the progress of project implementation. Executive management must review and make decisions on budget, including the selection of the

> "FALSE POSITIVES ARE A MAJOR CHALLENGE FOR ANY SOC, AND THEY CAN BE AVOIDED BY COLLECTING RELEVANT ACTIONABLE DATA AND ENRICHING THE CONTEXT BASED ON RELEVANT ACTIONABLE THREAT INTELLIGENCE."

right tools and technologies and SOC services offered. The CISO/CIO and the SOC architecture team must decide whether to implement an internally managed SOC, an MSSP or a hybrid SOC (**figure 1**) based on cost, availability of internal and external skilled resources, and regulatory and compliance requirements.

Selecting the Right People

The multiple phases of building an effective SOC include plan, design, build, operate, measure and optimize. Each phase requires a different set of capabilities and skills, including gap assessment, SOC design, infrastructure design, facilities management, electrical engineering, network engineering, SIEM engineering, incident response workflows, vulnerability management, event correlation and data analysis, playbook development and automation, technology integration, security risk management, malware analysis, intrusion detection and response, identity and access analytics, security analytics, threat intelligence, threat hunting, and forensics.

Establishing the SOC Organizational Structure, Steering Committee and Governance Team

This is typically the first step in implementing a SOC program. The steering committee reviews the progress of program implementation and provides updates to executive management. The steering committee should have leaders from IT, security engineering, incident response, risk management, data privacy, various business units and human resources. The governance team and steering committee must decide and document the services offered by the SOC and the benefits to the organization from the security risk perspective.

Integration of People, Process and Technology

SOC components must be assessed on a periodic basis to improve the services and maturity of the SOC (**figure 4**). There are various SOC maturity assessment models available, including CREST[7] and SOC-CMM,[8] and the best option can be selected based on the organization's needs. The objective of SOC components assessment is to understand how the SOC is managing the threat and risk and how SOC strategy is aligned to business strategy. The gaps identified in the assessment should be used to improve the effectiveness and maturity of the SOC components.

The security orchestration automation and response (SOAR) solution entered the realm of the SOC after 2017 and solved many of the previous challenges. Orchestration of multiple-point solutions along with threat intelligence, end-to-end automation of repetitive tasks, incident response, dynamic updating of playbooks/runbooks, context enrichment, MTTD, MTTR calculations and incident prioritization have made security analysis much easier.

Breach attack simulation and cybersecurity range (**figure 4**) are new capabilities to the modern SOC. Cybersecurity range helps SOCs train security analysts to fight sophisticated threats through simulated cybersecurity exercises. Breach attack simulation (BAS) technology helps security analysts and leaders understand the effectiveness of implemented security controls against the latest threats without disturbing production infrastructure. BAS can also help chief information security officers (CISOs) optimize and justify security investment of various security controls.

Use Case Development and Analysis Depending on Relevant Data Collection

Event logs from various log sources, network flows from network devices and network packets from deep packet inspection solution are collected, aggregated, deduplicated and analyzed for security monitoring. The SOC engineering team should get answers for the following questions from the SOC steering committee before implementation to reduce false positives:

- What devices and technologies need to be monitored?
- What log events must be generated and collected?
- What security alerts should be raised?
- How, where and at what intervals should logs be collected from various log sources based on the objectives of SOC and compliance and regulatory requirements?

False positives are a major challenge (**figure 2**) for any SOC, and they can be avoided by collecting relevant actionable data and enriching the context based on relevant actionable threat intelligence. The use case development framework must be implemented before use cases can be developed for the SOC. The following must be documented as part of the use case development (**figure 5**) for all the use cases identified for security monitoring:

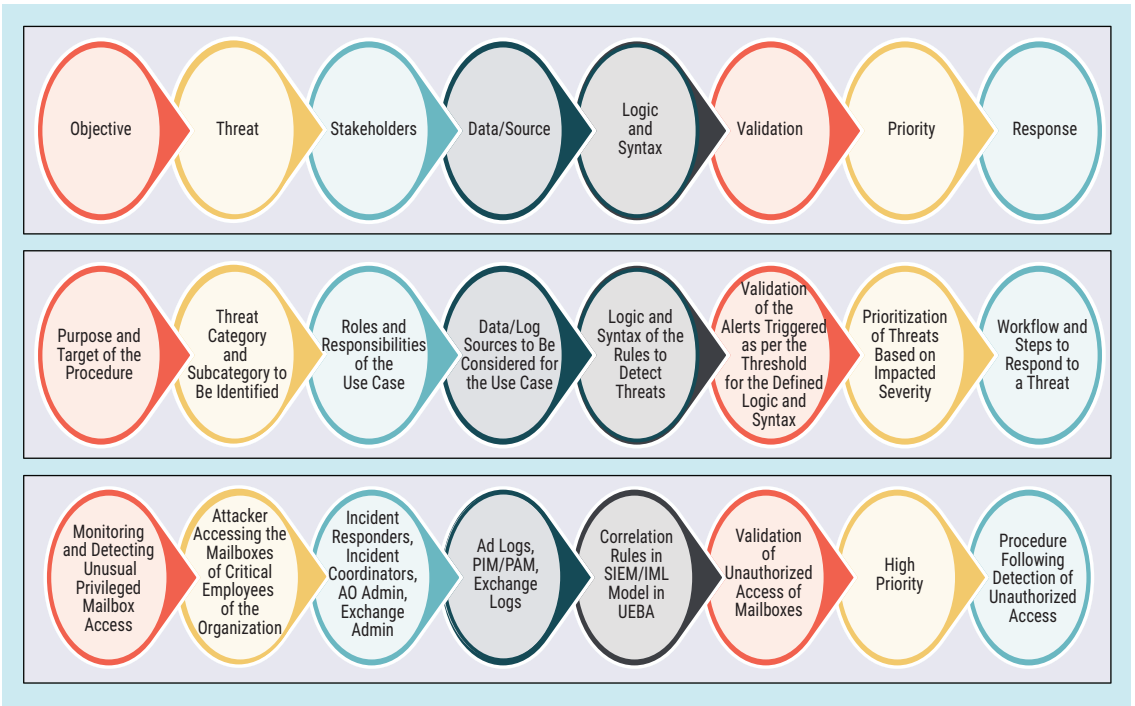
- Objectives, purpose and target of the use case
- Threats the use case will address
- Stakeholders and their roles and responsibilities in the use case and incident response workflow
- Data sources to be correlated
- Logic and syntax of the correlation rules/data models to detect the threats
- Validation/testing of the syntax and logic
- Priority of the alerts based on the risk and impact
- Response/mitigation/steps to be followed as part of incident response

> "BREACH READINESS ASSESSMENTS CAN HELP IDENTIFY THE BLIND SPOTS IN THE SECURITY ARCHITECTURE AND DEPLOY SECURITY CONTROLS."

Reactive to Proactive Approach of Security Operations

This is the key to handling the threat surface, which changes rapidly: Proactively analyzing applications, infrastructure and networks for threats based on predetermined objectives and laying out countermeasures to prevent attacks and mitigate damage. Breach readiness assessments can help identify the blind spots in the security architecture and deploy security controls. The probable attacker's profile, the most likely attack vectors and the assets most desired by an attacker are key to identifying the threats. Cyberthreat intelligence is a key security operations enabler, providing the context necessary to inform decisions and actions across the organization. Well-structured cyberthreat

Figure 5—Use Case Development



intelligence functions serve stakeholders as well. Cyberthreat intelligence integration with existing processes and infrastructure helps provide a deeper understanding of what is happening outside an organization's network, providing better visibility of the cyberthreats that bring the most risk to the organization's infrastructure.

Threat hunting is an advanced security analysis process that leverages deep knowledge of a network or organization to catch subtler, more deeply embedded attackers than an SOC finds. Threat hunting gives defenders tools to reduce the gap by actively looking for anomalous and suspicious behavior. Defenders can identify changes in TTPs before they show up in the threat feed. Threat intelligence and threat hunting functions exist to strengthen other teams in the organization. Therefore, it is critical that threat intelligence and hunting teams include people who understand the core business, operational workflows, network infrastructure, risk profiles and supply chain as well as the technical infrastructure and software.

Proactive monitoring of endpoints is crucial because endpoints are the beginning and end of most breaches. Endpoint detection and response (EDR) capabilities are useful if regularly used to capture unfiltered data and conduct continuous monitoring.

What Is Next?

Extended detection and response (XDR) and the integration of IT/operational technology (OT)/industrial control systems (ICS) are likely the next advancements in the SOC evolution. XDR is evolved from current reactive threat detection and response solutions and integrates security technologies signals to extract threat events across identity, endpoints, the cloud and the network. XDR capabilities include identity analytics, network analysis, integrated threat intelligence, AI/ML-based detection, and automated and orchestrated investigation response. XDR is going to change the way SOCs operate by helping security analysts with the following:

- Complete automated and orchestrated investigations to reduce time to detect and time to triage.
- Uncover root cause analysis and gain extraordinary situational awareness through cross-surface correlation.
- Track threats across multiple system components.
- Improve detection and response speed.
- Eliminate the efforts required to integrate and maintain log sources.
- Increase scalable storage and compute through cloud-based big data lakes.
- Improve the productivity of the SOC.

The manufacturing industry has accelerated digital transformation to automate their processes and be competitive in the market. OT is used to manage industrial operations such as those found in manufacturing. This extends to cover ICSs and the ICS management framework as well as supervisory control and data acquisition systems (SCADA).

OT and ICS networks depend on digital systems to carry out their daily operations. The increased connectivity of OT/ICS has led to an increase in cybersecurity threats against OT/ICS networks. By converging OT with IT, the previously isolated and protected systems that manufacturing organizations used are now open to the same kinds of security threats normally targeted at IT systems. The most common cyberattacks against OT/ICS networks are protocol vulnerability attacks, data leakage, remote access trojan, ransomware, bot attacks and distributed denial-of-service (DDoS) attacks.

The integration of IT SOC and OT SOC is very much required to manage sophisticated cyberthreats against IT/OT systems and networks. Organizations that have OT and ICS as part of their infrastructure will be able to enable security monitoring of OT systems. OT SOC can be integrated with IT SOC. Partnership between IT, SecOps and OT teams is critical for the successful integration of IT/OT SOC. Establishing communication and building trust between the teams are important to create a strong partnership. Integration of IT/OT SOC will protect OT systems by:

- Continuous discovery of assets and behavior analytics (type of device, network behavior, activity monitoring)
- Vulnerability life cycle management and configuration compliance
- Continuous monitoring of OT/ICS/SCADA systems to discover the cyberthreats and respond
- Responding to access anomalies
- Deep packet inspection
- OT/ICS-specific threat intelligence

Conclusion

While the threats facing cybersecurity professionals continue to evolve and proliferate, it is imperative to keep track of emerging threats and adapt new ideologies to address them, including evolving the SOC. This includes the influence of a pandemic and the techniques that must be employed to overcome it so that a physiological virus does not deplete the SOC of human interaction. As cybercriminals and nation-state-sponsored attackers launch increasingly sophisticated attacks to steal sensitive data and to disrupt business, SOCs are the dedicated frontline teams working 24/7/365 to stop them.

The SOC is critical to all types and sizes of organizations in today's digitized economy, as so much of an organization's operations and sensitive data are online and in the cloud. A modern approach to SOC operations is required to fight against cybercriminals and the key best practices are as follows:

- Establish SOC governance, metrics and reporting.
- Invest in establishing the SOC with the right people by creating a talent strategy, using relevant technologies and creating a culture of curiosity.
- Deploy AI/ML systems and comprehensive threat intelligence to automate highly repetitive and mundane tasks.
- Be aware of hardware/software/network/IOT/OT assets and consistently mitigate vulnerabilities and misconfigurations based on prioritization.
- Ensure continuous visibility across organization networks.
- Establish proactive incident detection and remediation through threat hunting, breach attack simulation.
- Consistently train SOC analysts on practical knowledge using Cyber Range and simulation solutions.
- Continuously test and update SOC detection/prevention strategies using cybersecurity assessments and SOC maturity assessments.
- Collaborate with IT and business units to align SOC strategy with business strategy.
- Continually adapt and modify cybersecurity defenses on an ongoing basis.

"THE SOC IS CRITICAL TO ALL TYPES AND SIZES OF ORGANIZATIONS IN TODAY'S DIGITIZED ECONOMY, AS SO MUCH OF AN ORGANIZATION'S OPERATIONS AND SENSITIVE DATA ARE ONLINE AND IN THE CLOUD."

Endnotes

1 International Standards Organization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2005 *Information technology—Security techniques—Information security management systems—Requirements*, Switzerland, 2005, *https://www.iso.org/standard/42103.html*
2 Olavsrud, T.; "Target Attacks Increased, Became More Diverse in 2011," *CIO*, 30 April 2012, *https://www.cio.com/article/2396583/targeted-attacks-increased—became-more-diverse-in-2011.html*
3 IBM, "IBM Opens Threat Intelligence to Combat Cyber Attacks," 16 April 2015, *https://www-03.ibm.com/press/us/en/pressrelease/46634.wss*
4 Schueler, C.; "Automation: Friend of the SOC Analyst," *DarkReading*, 5 September 2019, *https://www.darkreading.com/vulnerabilities-threats/vulnerability-management/automation-friend-of-the-soc-analyst/a/d-id/1335686*
5 Bollapragada, S.; "SOAR: Transforming the Security Operation Center," Micro Focus, 1 July 2019, *https://community.microfocus.com/t5/Security-Blog/SOAR-Transforming-the-Security-Operation-Center/ba-p/2684589*
6 Bhargave, R.; "False Positives Have Real Consequences," *DarkReading*, 22 June 2017, *https://www.darkreading.com/endpoint-security/false-positives-have-real-consequences/a/d-id/733939*
7 CREST, "Maturity Assessment Tools," *https://www.crest-approved.org/knowledge-sharing/maturity-assessment-tools/index.html*
8 SOC CMM, *https://www.soc-cmm.com/*