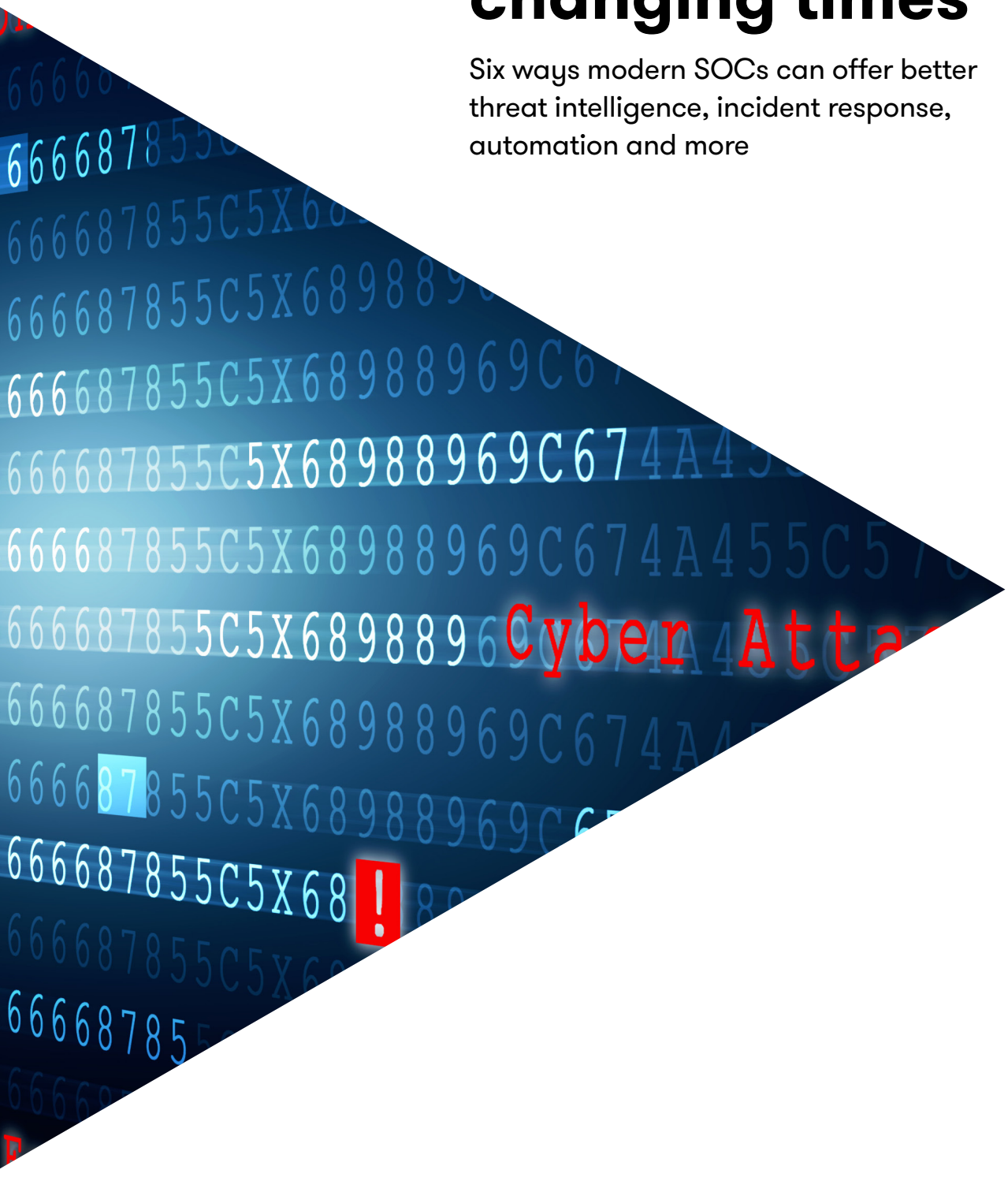
DXC.technology

White Paper

How to keep security operations centers relevant through changing times

Six ways modern SOCs can offer better threat intelligence, incident response, automation and more



Benefits of modern SOCs

- Strengthen and retain customer confidence
- Protect revenue and brand reputation
- Avoid penalties and liability
- Prevent business disruption
- Optimize productivity
- Minimize or avoid recovery costs

Security operations centers (SOCs) and their staff account for a significant amount of security spending, but these often-siloed facilities are notoriously slow at detecting breaches and responding to incidents. Breaches typically go undetected for nearly 2 months, and more than half of breaches are discovered by an external source — not the SOC.[1]

With many organizations still operating in crisis mode with an unprecedented number of remote workers, cybercriminals are intensifying their attacks. A single breach or ransomware attack can cripple a business and further erode confidence in security operations.

Other parts of the business are modernizing applications, adopting cloud and hybrid infrastructures, and embracing new mobile, internet of things (IoT) and operational technologies (OT). However, all too often, security organizations are falling behind. SOCs are still labor-intensive. They lack the ability to rapidly orchestrate and automate processes, and they struggle to deliver clear metrics on risk and compliance to justify growing costs. Finding and keeping skilled security professionals are major challenges.

All together, these factors make it increasingly challenging for SOCs to stay relevant in modern enterprises. Security programs are seen as a necessary cost of doing business, not an enabler of business change.

To effectively mitigate risk, SOCs must evolve at the same pace as the rest of the business, applying the latest security techniques, real-time threat intelligence and response, artificial intelligence (AI) tools and automation to move from reactive to proactive security operations.

[1] "M-Trends 2020," FireEye Mandiant, February 2020, https://www.fireeye.com/blog/threat-research/2020/02/mtrends-2020-insights-from-the-front-lines.html

Creating modern SOCs

Today, for a business to succeed, data must be viewed as a competitive differentiator. Analytics become an enterprise enabler, and shareholders, clients and customers benefit. SOCs must be included in this change to realize their full value and enable organizations to make intelligent business decisions using quality data points across the security value chain. The ability to deliver real-time and predictive insights from technical to societal trends data is a pivotal differentiator.

Threat intelligence combined with real-time analytics, AI and process orchestration should be the norm to support growth initiatives, resilient operations, continuous compliance and predictive risk management. As threats and vulnerabilities increase, modern SOCs must address a growing number of risks (**Figure 1**).

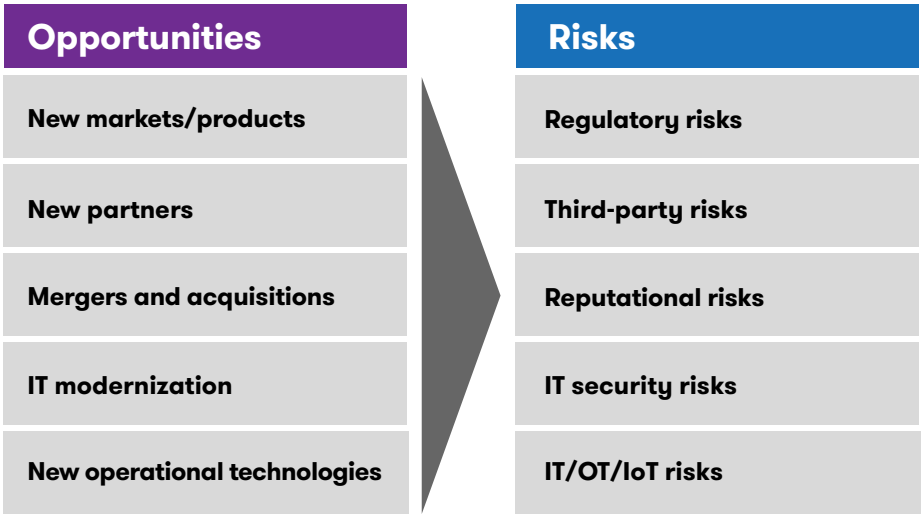


Figure 1. Growth opportunities and modernization drive increased risks

In this context, the SOC function must evolve to encompass the business dimension of the organization. It must be fully integrated with the enterprise risk management function and security operations. It must support early detection and response, effectively manage threats and vulnerabilities, and provide visibility into the enterprise security posture.

Today, SOCs must be more than the sum of their parts, and we examine this by taking a step back to look at the definition of risk (**Figure 2**). SOCs must understand and address these three dimensions of risks to be able to have full situational awareness.

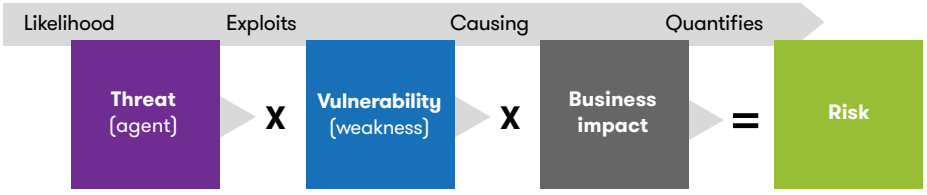


Figure 2. Risk is defined as a combination of threats, vulnerabilities and potential business impact

Many organizations are just beginning their modernization journeys. There are six key strategies for operating modern SOCs that, when designed, developed and implemented correctly, help keep security aligned with the business (**Figure 3**).

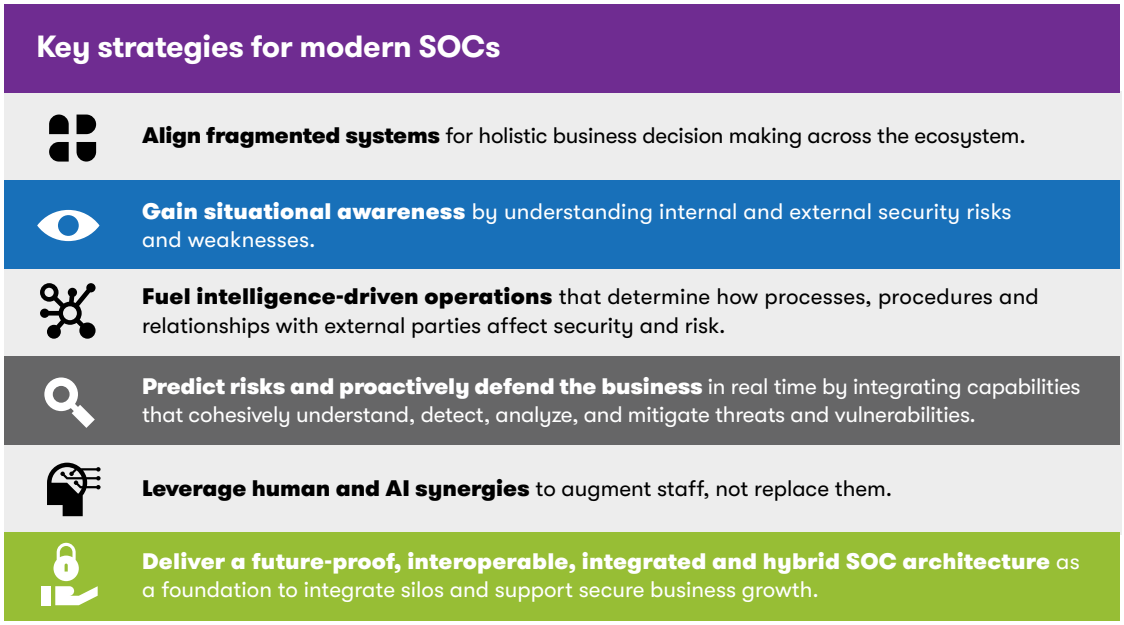


Figure 3. Key strategies impact people, systems, tools and ways of working

Align fragmented systems

Effective cybersecurity management aligns fragmented systems for comprehensive visibility of an organization's security posture. This allows enterprises to make holistic decisions that lead to better business outcomes. For this to occur, however, it is critical that organizations understand their security environments and how their teams access data.

Teams typically work in silos, disconnecting them from business operations that often contain weak procedures, structural inefficiencies or incorrect configurations. These vulnerabilities decrease security effectiveness and make it difficult for teams to access the right data or large enough volumes of data for analysis.

Organizations can minimize risk by effectively identifying, analyzing, and prioritizing threats and vulnerabilities. Many security programs follow National Institute of Standards and Technology (NIST) guidance, which requires information classification; select controls adapted to security classification, implementation and assessment; system and common control authorizations; and continuous monitoring.[2]

Organizations prioritize risks by highest impact and greatest probability of occurrence. While this approach is widely recognized, modeling threats and understanding adversaries are not. Teams working on governance, risk and compliance (GRC) rely on manual modeling, which exposes businesses to human bias and errors. To accurately and quickly identify the right information from masses of data, organizations must automate their GRC processes.

[2] "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," National Institute of Standards and Technology, December 2018, Ronald S. Ross, https://www.nist.gov/publications/risk-management-framework-information-systems-and-organizations-system-life-cycle

Businesses cannot adequately protect their assets if they do not know what they have, where they are located and what classifications of data reside within them.

To automate processes, organizations must first understand their threat landscape, business data, operations, risk management and security controls. With this knowledge, they can effectively and efficiently map relationships and build predictive models that will proactively identify threats and anticipate potential risks. Automation frees employees to focus on value-added tasks and projects; however, humans still need to interpret the data and associate it with risk events and scenarios.

When done correctly, alignment of fragmented systems and processes gives businesses the visibility they need to:

- Prioritize activities at operational levels
- Produce executive reports with business-relevant SOC metrics
- Demonstrate the impact on business objectives
- Understand how risk posture impacts businesses and annual trends
- Predict possible future outcomes
- Make better business decisions
- Support tactical and strategic initiatives for managing risk

Gain situational awareness

Situational awareness is key to successful security management. Businesses cannot adequately protect their assets if they do not know what they have, where they are located and what classifications of data reside within them. They must also assess their risks and determine the technologies in use. This requires a deep dive into internal and external systems, especially where they touch public networks, such as those of a supplier.

A comprehensive and well-maintained asset library mapped to business processes and operations improves the prioritization of assets, determines protection levels and locations, and is essential for a robust patch management and monitoring strategy. Combined with threat intelligence information tailored to the technology and organizational threat profile, it further allows tailored defense strategies and decision making.

Environmental complexities challenge businesses to achieve this level of protection. For example, security programs typically focus on process or technical aspects, risks relating to the latest vulnerabilities and patches, or security awareness training. However, security incidents can be attributed to weaknesses higher up in the organization. Therefore, it is crucial for businesses to understand where culture, security awareness and decision-making vulnerabilities exist, while also considering the effects of external forces such as regulators, government initiatives and market trends.

Organizations must manage complex sociotechnical systems that impact all areas of the business. The keys to successfully managing this complexity are highly efficient communication between cross-departmental teams and consideration of external forces (**Figure 4**).

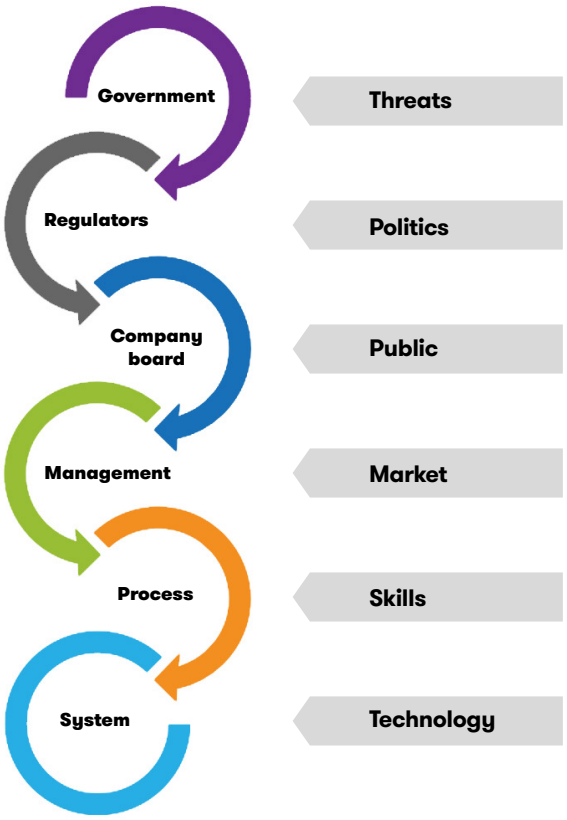


Figure 4. Organizations as complex sociotechnical systems

In these sociotechnical layers, vulnerabilities can occur at any level. For example, a regulator in one region could allow weak password policies that could lead to audit penalties in another region. Or a decision by the board of directors could unwittingly trigger a hacktivist group to launch a social media campaign to launch a distributed-denial-of-service attack against the company. Poorly communicated policies by management could lead to insider threats and the release of sensitive data.

Organizations do not suffer cybersecurity breaches because of a single act or one-off gap; rather, they accumulate contributing elements across all levels over time. This accumulation of risk can lead to high-profile breaches with disastrous consequences. To have true situational awareness, organizations must think holistically, communicate clearly, collect feedback across all layers and take account of change.

Fuel intelligence-driven operations

Cyberthreat intelligence is increasingly important in developing well-rounded cyberdefense strategies. However, threat intelligence programs traditionally focus on technical indicators of compromise (IOCs). IOCs by themselves are contextless and atomic in nature, similar to antivirus signatures. This one-sided view perpetuates reactive responses. To become proactive, organizations must combine security data with data from multiple sources and distill it into actionable intelligence. This puts threats into context and demonstrates relevance to industry verticals, operating regions and technology stacks.

There are primarily four types of threat intelligence, each with a different focus and relevance to various parts of the organization (**Figure 5**).

Threats	Focus	Primary defender
Strategic	• Threats tied to the organization • Risk-based view • Informs business decisions	• Board of directors • C-suite
Operational	• Current adversary campaigns • Links attacks to real-world events	• Threat intelligence analysts • Incident responders
Tactical	• Adversary techniques and procedures • Adversary capability and intent • Informs policy changes	• System architects • System administrators
Technical	• Indicators of compromise • Device logs and monitoring	• SOC staff • Incident responders

Figure 5. Major types of threats relate to multiple areas of the business

If businesses focus on certain threat types and ignore others, they receive incomplete views of the threat landscape. To see the full picture, organizations must process threat intelligence on a threat intelligence platform that supports collection, validation and storage of threat intelligence using flexible scripting and programming options that automate:

- Enrichment and triage using community and proprietary sources
- IOC processes using analysis tools such as decoders, unpackers, hashers and connection graphs
- Mature curation of signatures, use cases and scripting for deployment on endpoint incident response tools

Understanding potential attackers, their purpose and plans is critical for effective, efficient defenses that enrich, accelerate and automate security processes for:

- **Security alerting.** Automate the processing of relevant IOC data to remove repetitive, manual tasks, free up resources and improve detection rates.
- **Incident triage and analysis.** Ensure that suspected incidents and alerts are enriched with relevant information before triaging to SOC staff for investigation.
- **Threat hunting and investigation.** Proactively hunt for threats — an ongoing process in which artifacts and indicators with high severity are contained and affected systems are quarantined until investigations are complete.
- **Intelligence sharing.** Share threat intelligence across trusted groups both internally and externally to enrich the understanding of the threat landscape. As more organizations participate in intelligence sharing, the longevity of new malware techniques will shorten, which slows attack rates and minimizes their spread and effectiveness.

By employing additional intelligence elements, businesses gain a holistic view of threats, which enables threat modeling process automation.

By employing additional intelligence elements, businesses gain a holistic view of threats, which enables threat modeling process automation. This allows automatic calculation of the organizational risk posture, which leads into the predictive dimension of risk management.

Predict risks and proactively defend the business

When executives understand and anticipate threats using actionable intelligence, they make more informed risk management decisions, optimize returns on their security investments, and incorporate security and privacy into applications and infrastructures.

Active defense, borrowed from military terminology, is essential to predictive risk management because it proactively outmaneuvers adversaries, guards against attacks and helps set priorities for security management systems. NIST defines active defense as the anticipated synchronized, real-time capability to discover, detect, analyze and mitigate threats and vulnerabilities.

Active defense allows new strategies to be developed to defend valuable assets. Increased awareness provides a greater level of understanding of the “who” and “why” of an attack. It significantly changes the traditional reactive approach of security management to a proactive one. It is a top priority for security management systems, and it requires “continuous testing,” “continuous improvement” and “continuous learning” through activities such as blue and red teaming. It also incorporates security and privacy into the system development life cycle.

Combined with the other key steps covered in this paper, near-real-time risk management sets the conditions for ongoing information system and common control authorization through the implementation of continuous risk-monitoring processes. This provides for efficient, cost-effective and informed risk management decisions about the systems that support mission and business functions.

Integrating GRC, SOC and security operational processes across data, applications, IT, OT and IoT ecosystems will play an increasing role as ecosystems become more complicated. This complexity is driving the need for automation and orchestration across configuration, management and coordination of systems, applications and services. The business is then more efficient, with clearly defined automated playbooks and runbooks to mitigate incidents and improve security management across the enterprise. This reduces human intervention, while using an orchestrator to conduct the activity reduces costs and accelerates outcomes.

Leverage human and AI synergies

Modern SOCs can no longer focus solely on IT monitoring, analysis and response activities. An exponential increase in monitoring and better analytical capabilities are now required for:

- Mobile devices
- Wearable technology
- Applications
- Platforms
- Cloud and IT infrastructure
- Cyber physical systems
- IoT devices

The goal of AI is to optimize efficiencies in environments where large-scale gains are needed for organizations to survive the growing onslaught of malicious actors.

Adoption of cognitive computing and AI solutions will reduce workloads for risk management and SOC staff handling security events and will ultimately improve outcomes.

To increase productivity, multiple teams must work as one and not as siloed individuals or groups. This translates into multiskilled employees working agilely on goals that everyone understands. AI advances this model by enhancing skills and freeing resources for value-added activities. This approach is met with less resistance because it is not a short-term, cost-cutting activity that displaces individuals. The goal of AI is to optimize efficiencies in environments where large-scale gains are needed for organizations to survive the growing onslaught of malicious actors.

Some attempts to automate discovery and triage have actually led to deskilling of Level 1 staff. This can create workplace alienation, drive down quality and increase attrition. Organizations can fall into a damaging cycle as more automation or further workforce shifts continue.

When AI is introduced to support the team rather than replace it, the staff benefits from augmented security analysis and decision support, particularly at the entry level. Organizations can then create more efficient and effective SOC teams.

A modern data-led SOC analysis function with an integrated human–AI collaborative workforce can handle vastly greater amounts of information and significantly increase its value to the organization.

In this model, the roles of levels 1 – 3 change.

- **Level 1.** Trains the AI system in anomaly detection to work in partnership with humans to flag unknowns and close calls for further analysis
- **Level 2.** Builds the ability to respond automatically to incidents, while partnering with AI for joint responses
- **Level 3.** Creates and trains expert systems that aid in decision making and the diagnosis of complex issues through simulation and testing

All three roles are complementary and encourage team members from each group to collaborate. They also generate demands for higher skills in each area, leading to rewarding career paths for security analysts. To achieve this, organizations must embrace multiple perspectives for understanding and incorporating AI. This moves away from treating AI as a black box and makes it a team contributor whose strengths and weaknesses are understood and appreciated.

A modern data-led SOC analysis function with an integrated human–AI collaborative workforce can handle vastly greater amounts of information and significantly increase its value to the organization.

Deliver a future-proof, interoperable, integrated and hybrid SOC architecture

Whether building modern SOCs or transforming existing ones, organizations must adopt the same principles used to digitally transform their businesses. The process is challenging and time-intensive but required to reach acceptable levels of SOC maturity. The key principles are:

- **Future-proof.** Adopt a modular SOC architecture using open standards and Agile approaches for the ongoing evolution of security management and processes.
- **Interoperate with everything.** When designing a SOC, businesses must follow sound architecture disciplines, remain vendor-agnostic and use APIs for foundational integration and orchestration that allow future evolution and integration of new capabilities over time without rebuilding the foundations.
- **Integrate everything.** All SOC capabilities and processes must integrate with one another and with GRC, security operations, IT, OT and IoT management, business application and data management processes.
- **NoOps by design and automate the known.** Businesses must automate all known operational processes, including those for detection, analysis, validation, prioritization and response, to reduce human interactions and minimize mistakes.
- **Facilitate standardization and consistency.** Develop reusable patterns, blueprints and play/run books to ensure the above principles are embedded and adhered to for standard, consistent SOC functions across geographies and teams.
- **Everything as code.** When designing and implementing systems using the above principles, organizations should perform all functions on serverless platforms in support of portability and reversibility, accelerated service instantiation and scale on demand.
- **Hybrid operating model.** Ensure that different providers can deliver SOC functions based on the above principles.

Conclusion

SOCs by design focus on the organization's current state, what might happen next and how to predict the future. Modern SOCs must plan for breaches that have a high probability of occurring as well as those that may never materialize — and breaches that have already happened but have not been detected.

Change is a constant in business and within SOCs. To stay relevant, SOCs must continuously evolve to be ready to understand and manage both the threat and the vulnerability landscape.

Organizations must consider all valuable, relevant data that's available from the business, society, geopolitics, people, technology and processes. This is then set against the evolving threat and vulnerability landscape to assess what is likely to happen and justify decisions and prioritize actions. The SOC can no longer be considered a silo of the business and must be linked to all business lines. This means security, operational and business teams must adopt an end-to-end, integrated approach to protect and enable the business — leveraging real-time AI and remediation capabilities.

Change is a constant in business and within SOCs. To stay relevant, SOCs must continuously evolve to be ready to understand and manage both the threat and the vulnerability landscape (**Figure 6**).

Figure 6. Key capabilities of modern SOCs

The journey to modernize SOCs is evolutionary, beginning with a comprehensive understanding of enterprise risk factors, a 360-degree view of the threat and vulnerability landscape, and the right cultural behaviors to promote security. Organizations must embrace active security, turn data into meaningful intelligence, and drive increased enterprise resilience and compliance. SOCs can achieve this future state through tight, cross-enterprise integration, orchestration and automation and skilled people, leveraging machine intelligence and AI. Only then can SOCs stay relevant in the modern enterprise.

About DXC in Security

Recognized as a leader in security services, DXC Technology helps customers prevent potential attack pathways, reduce cyber risk, and improve threat detection and incident response. Our expert advisory services and 24×7 managed security services are backed by 3,000 experts and a global network of security operations centers. DXC provides solutions tailored to our customers' diverse security needs, with areas of specialization in Cyber Defense, Digital Identity, Secured Infrastructure and Data Protection.

Learn how DXC can help protect your enterprise in the midst of large-scale digital change.

Authors

Christophe Menant
Global Strategy Lead for Cyber Defense and OT Security

Christophe has 27 years of experience in IT and cybersecurity, particularly in international and global environments. He has helped customers develop security strategies and transformation programs, manage major breaches and remediation programs, and develop reference security architectures and offerings. Christophe joined HPE in 2013 and DXC in 2017. Prior to that, he worked for 15 years at IBM as executive security architect, leading the creation of standard security architectures and methodologies, and as chief security architect for cloud security offerings.

Scott Keen
Security Risk Management (SRM) Practice Lead

Scott leads the Security Advisory Services team for DXC in the Americas and is the Global Cyber Defense Situational Awareness (CDSA) offering lead. He is an accomplished leader with over 28 years of experience in IT, helping governments and customers with complex international environments develop security strategies and transformation programs.

Richard McEvoy
Senior Risk Advisor

Richard has 25 years of experience in information security risk analysis and management, primarily in government but also in sectors such as energy and transportation. As a practitioner, Richard is also an active researcher in security matters, with over 18 peer-reviewed publications in the area covering anomaly detection, adversary capability modeling, human and organizational factors, and risk analysis.

Gary Roberts
Security Enablement

Gary's career spans megadeal solutioning and governance, product management, sales enablement and marketing. His passion for cybersecurity started with mainframe computers and data center management before shifting to security consultancy, where he collaboratively wrote and implemented the UK Government IT Cybersecurity Standards. His focus is customer satisfaction, increased sales, speed to market and increased wallet share, while reducing runoff and lowering costs through a differentiated and pragmatic approach to secure growth.

Jim Hardisty
Global Lead for Strategic Threat Intelligence

Jim is global lead for Strategic Cyber Threat Intelligence at DXC. With nearly 20 years of experience in cybersecurity, he leads DXC's Global Strategic Threat Intelligence program and serves as editor of the DXC Security Threat Intelligence Report.

Learn more at www.dxc.technology/security

▶ Get the latest news on threats, breaches and vulnerabilities. www.dxc.technology/threats

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. With decades of driving innovation, the world's largest companies trust DXC to deploy our enterprise technology stack to deliver new levels of performance, competitiveness and customer experiences. Learn more about the DXC story and our focus on people, customers and operational execution at **www.dxc.technology**.

LO_3621a-21. October 2020