FORBES > INNOVATION > AI

Advancing The Security Operations Center (SOC): New Technologies and Processes Can Help Mitigate Cyber Threats

Chuck Brooks Contributor ⓘ
Global Thought Leader in Cybersecurity and Emerging Tech

Follow

0

Apr 26, 2023, 02:39pm EDT

Listen to article 19 minutes

In the System Monitoring Room Two Senior Operators Work on a Big Interactive Map. Facility is Full ... [+] GETTY

We are in a state of cyber-flux with new and many asymmetrical challenges to cybersecurity. As cybersecurity gaps abound, a new urgency in both industry and government has arisen on how to better protect the cyber landscape.

The Evolving Cyber-Threat Landscape

The digital attack surface has vastly expanded from the transitions by many companies and organizations to remote work, and from more interconnectivity of PCs and smart devices coming online from around the globe. For many companies and institutions, the overall IT perimeter is now more complex and dispersed with on-premises systems, cloud, and edge computing that necessitates more visibility, and a need for better threat detection, analysis, and incident response.

The cyber ecosystem is in a precarious situation. Emerging technologies such as the Internet of Things, Machine learning & artificial intelligence, and 5G are creating operational shifts that require new and more robust cybersecurity strategies. Exacerbating the cybersecurity challenge is the global dearth of qualified cybersecurity workers and expertise available to help defend the data at risk.

Finally, but not least of concern is the fact that criminal enterprises and state actors are posing a much more sophisticated and capable threat. They are sharing resources and tactics over Dark Web forums and using advanced hacking tools that enable them to discover vulnerable targets to infiltrate malware and automate attacks.

One vital and important development to meet these numerous cyber-threat challenges is the development of enhanced capabilities in Security Operations Centers (SOCs) used by companies, government, and organizations. SOCs provide an operational risk management structure for organizations to organize, monitor and respond to cybersecurity threats.

An effective SOC can manage corporate systems, control systems, and physical security. It is designed to deliver continuous prevention, protection, detection, and mitigation of threats to systems. SOC teams also uncover vulnerabilities, respond to threats, and handle incidents that may be in progress on your networks or systems. A SOC’s success quotient depends on the rapid and accurate interpretation and response to threats by analysts and the security team. Please see my article on the key functions and operations of SOCs in Homeland Security Today at: Using SOCs and Cybersecurity Hubs to Prioritize Security Operations in a Critical Era - HS Today

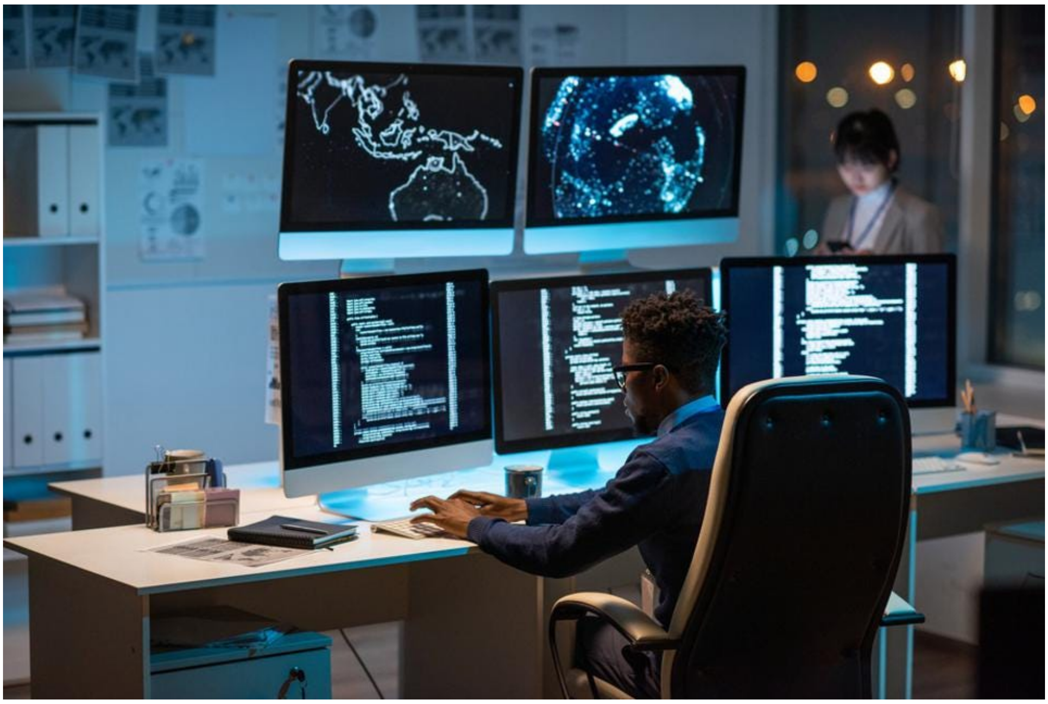
Also, security operations center benefits are well defined in an article called “Security Operations Center Trends for 2023” by Gilad David Maayan:

· **Improved Security Posture:** A SOC helps to improve an organization's security posture by continuously monitoring for security threats and vulnerabilities and taking appropriate action to address them. This can help prevent security incidents and protect the organization's assets.

· **Enhanced Visibility:** A SOC provides a centralized view of the organization's security posture, allowing security professionals to easily see what is happening across the organization's networks, systems, and applications.

- **Improved Response Time:** A SOC enables organizations to respond more quickly to security incidents and threats, as it provides a dedicated team of security professionals who are trained to handle these types of events.
- **Better Coordination:** A SOC can coordinate the organization's overall security efforts, including the implementation and maintenance of security policies and procedures, the deployment of security technologies, and the training of personnel on security best practices.
- **Improved Compliance:** A SOC can help organizations to meet regulatory and compliance requirements by providing a structured and documented approach to security management.

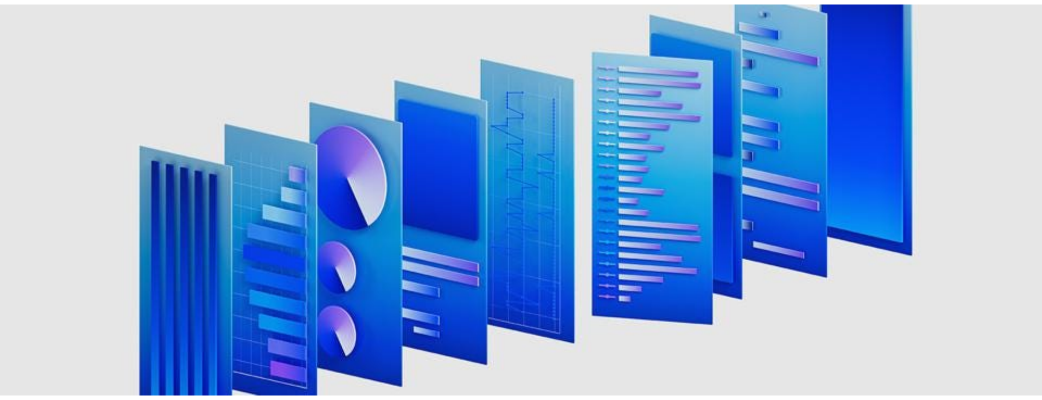
Please see: Security Operations Center Trends for 2023 - DZone



contemporary cyber security manager typing while sitting by desk in front of computer monitors GETTY

New SOC Products And Solutions To Optimize SOC Functions And Capabilities

Every year the RSA conference in San Francisco operates as a venue where many new cyber technologies are introduced for consideration to IT and security teams. SOC technologies have become a significant focus of those seeking improved cybersecurity. Other venues and conferences are also discussing the important role of SOCS for cybersecurity as the threat matrix grows. I have selected a few examples of solutions and products in different areas of SOC operations that can help advance SOCs and their operators for the years ahead.



IBM Launches New QRadar Security Suite to Speed Threat Detection and Response IBM

A New Suite of Products Assisting SOC Operators With AI, Automation, and Connected Interface

IBM, a historical leader in developing tools for SOCs, has responded to new SOC challenges with an array of AI and security solutions designed to unify and accelerate the security analyst experience across their entire process of threat detection, investigation and response The IBM QRadar Suite offers a comprehensive set of security software built around a new user interface that is embedded with AI, and connects security data and response workflows between SOC analyst toolsets. It is delivered as SaaS and is designed so businesses small, medium, and large can select and customize products from the suite that specially fit their unique situations.

Specifically for SOC operators these products include AI/automation innovations for:

· Alert triage; contextualizing threats, reducing false positives, and automatically prioritizing or closing alerts with AI trained on prior analyst response patterns,

· Threat investigation; with the system automatically conducting early investigation steps that analysts would normally do manually, such as searching across systems for other evidence related to the security incident, and compiling results into easy to digest format for analysts to review and respond.

According to IBM's press release from the RSA conference, there are three core design elements of the QRadar Suite that immediately garnered my attention that bring immediate advantages to SOC operators to help ameliorate cyber-threats:

- **Unified Analyst Experience:** Refined in collaboration with hundreds of real-world users, the suite features a common, modernized user interface across all products:

designed to dramatically increase analyst speed and efficiency across the entire attack chain. It is embedded with enterprise-grade AI and automation capabilities that have been shown to speed alert investigation and triage by 55% in the first year.

- **Cloud Delivery, Speed & Scale:** Delivered as a service on AWS, QRadar Suite products allow for simplified deployment, visibility and integration across cloud environments and data sources. The suite also includes a new, cloud-native log management capability optimized for highly efficient data ingestion, rapid search, and analytics at scale.
- **Open Foundation, Pre-Built Integrations:** The suite brings together the core technologies needed across threat detection, investigation, and response - built around an open foundation, an extensive partner ecosystem, and more than 900 pre-built integrations that provide strong interoperability between IBM and third-party toolsets.

Please see RSA Press Release:

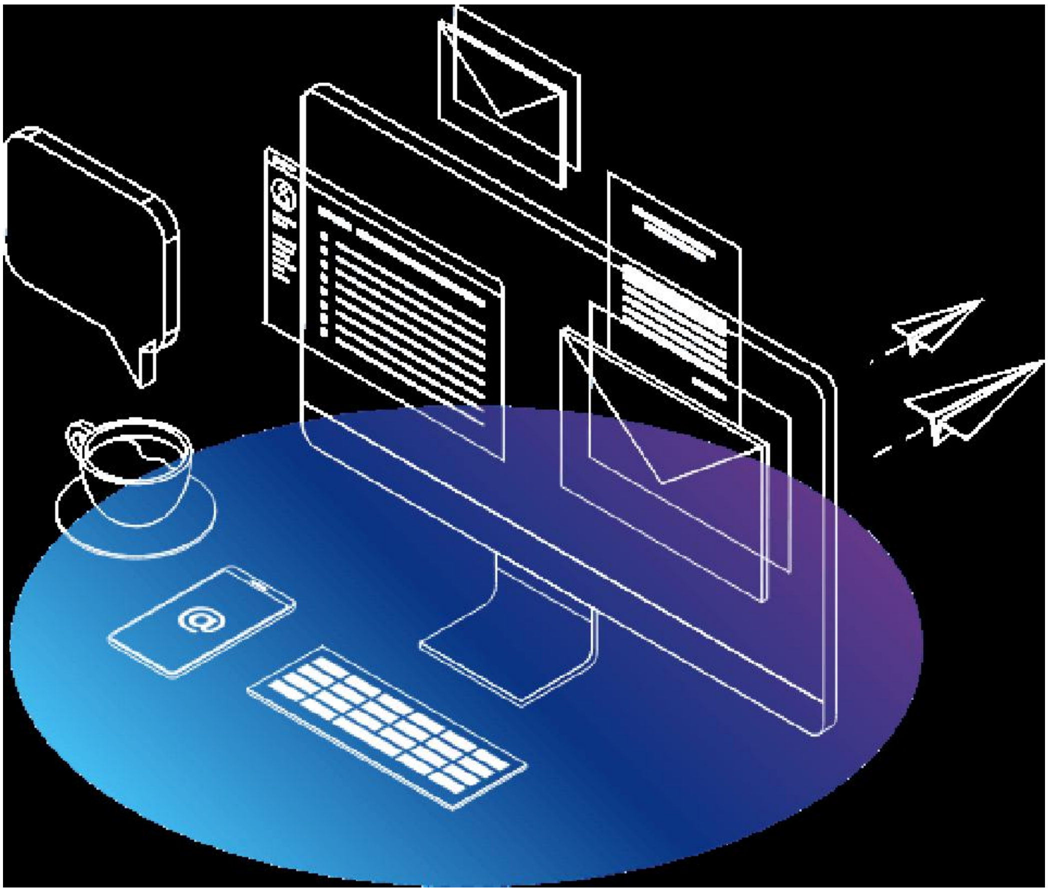
IBM NEWSROOM

IBM Launches New QRadar Security Suite to Speed Threat Detection and Response

For more information also for a deeper dive on QRadar see:

IBM

Security QRadar | IBM



Peripherals FIBERNET

Separating Multi-media Signals That Pose Threats To Devices and Networks in SOCS

An Israeli company called **Fibernet LTD**. known for their data center expertise (including for the CERN particle reactor), and has developed of a line of products for SOCs to keep secure USB, HDMI, and similar data lines. Their solutions allow companies to protect high-level secured environments, including multi-media peripherals that connect to SOCs, by separating source and data. Their new products can secure and simplify the aggregation of audio/visual data from multiple sources that may feed into a SOC. Fibernet restrings, emulates and separate signals, keeping functionality and avoiding any possibility of hacking through these lines.

Cybersecurity at the signal level is an interesting approach as physical security is based on the laws of physics– it makes it physically impossible to transfer data in the wrong direction, denying an attacker access to your system.

For more information, please see:

FIBERNET

Cybersecurity Archives - Fibernet

Business, Technology, Internet and network concept. Audit business and finance concept. GETTY

Following The Audit and Log SOC Trail

A Canadian company called Datex created a technology called DataStealth that is beneficial for SOC operators performing audits. DataStealth is deployed between 2 endpoints: User to Application or Application to a database or even an On-Premises environment to a SaaS Service. Their platform then creates an audit record for everything that passes between.

“The uniqueness of this approach is that the collection is performed at the transport layer enabling DataStealth to sit between any source and target, without any installation of collectors or agents. By collecting and reviewing audit logs, system administrators can achieve unparalleled granularity in tracking user activity, while security teams can easily and quickly investigate any security incidents to ensure full compliance with regulations, privacy laws, and governance requirements.”

Please see: DataStealth Audit and Logging Use Case

Top view of laptop, phone, glasses and pencil with card with inscription cybersecurity training. GETTY

Training of SOC Personnel Is Fundamental

While technologies are very important, there is no substitute for the human factor in cybersecurity and in especially managing the operations of a security operations center. There are a variety of organization that specialize in SOC certifications, two of them are described below.

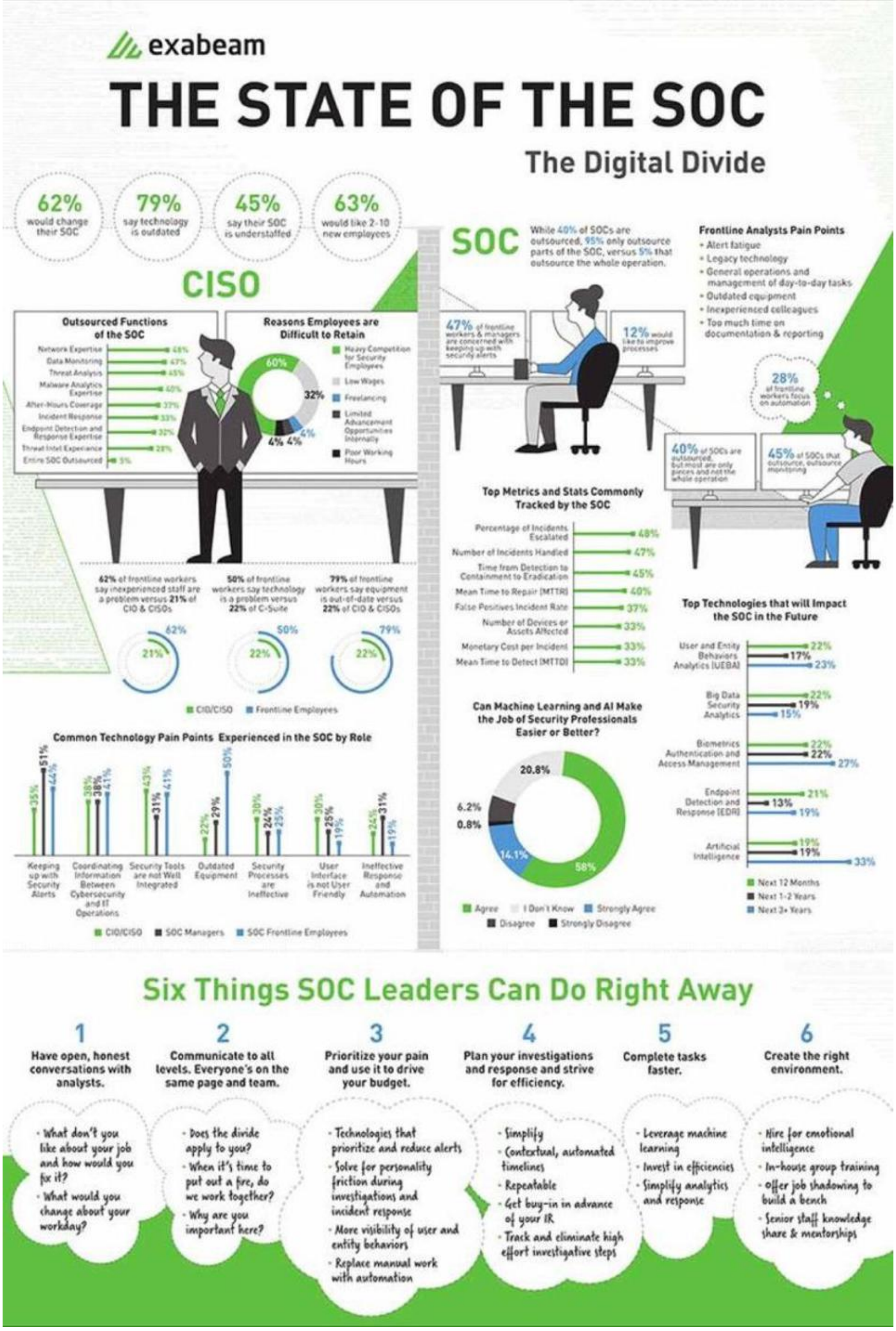
SANS Institute

The SANS Institute was launched in 1989 as a cooperative for information security thought leadership. SANS' ongoing mission to empower cyber security professionals with the practical skills and knowledge they need to make our world a safer place. SANS offers the latest SOC training certification and resources for SIEM, Elastic Stack, and modern detection techniques to help equip Blue Teamers with the right knowledge and ability that is needed to safeguard their organizations and drive security operations with actionable intelligence.

Please see: Security Operations Center | SANS Institute

CompTIA is another certification organization that offers excellent training for potential SOC analysts. “The Computing Technology Industry Association (CompTIA) is a leading voice and advocate for the $5 trillion global information technology ecosystem; and the estimated 75 million industry and tech professionals who design, implement, manage and safeguard the technology that powers the world’s economy.”

Please see: What Is a Security Operations Center | Cybersecurity | CompTIA



Six Things SOC Leaders Can Do Right Away

1 Have open, honest conversations with analysts.
- What don't you like about your job and how would you fix it?
- What would you change about your workday?

2 Communicate to all levels. Everyone's on the same page and team.
- Does the divide apply to you?
- When it's time to put out a fire, do we work together?
- Why are you important here?

3 Prioritize your pain and use it to drive your budget.
- Technologies that prioritize and reduce alerts
- Solve for personality friction during investigations and incident response
- More visibility of user and entity behaviors
- Replace manual work with automation

4 Plan your investigations and response and strive for efficiency.
- Simplify
- Contextual, automated timelines
- Repeatable
- Get buy-in in advance of your IR
- Track and eliminate high effort investigative steps

5 Complete tasks faster.
- Leverage machine learning
- Invest in efficiencies
- Simplify analytics and response

6 Create the right environment.
- Hire for emotional intelligence
- In-house group training
- Offer job shadowing to build a bench
- Senior staff knowledge share & mentorships

The State of The SOC COMPTIA

SOC Risk Management Strategies

The adage is that people, processes, and technologies are essential for holistic cybersecurity. I have discussed some interesting technology applications, but there are also newer processes that SOCs need to implement. While models can differ, below is a glimpse of the basic elements usually found in operating an SOC:

In the past, three significant risk management themes have been put forward to help ameliorate the digital risk ecosystem including: security by design, defense in depth, and zero trust. They are a triad, or three strong pillars of risk management needed for a successful cybersecurity strategy.

Security by Design is well defined in an article in United States Cybersecurity magazine, cybersecurity expert Jeff Spivey provided an excellent working definition: “Security by Design ensures that security risk governance and management are monitored, managed, and maintained on a continuous basis. The value of this “holistic” approach is that it ensures that new security risks are prioritized, ordered, and addressed in a continual manner with continuous feedback and learning.” Security by Design | United States Cybersecurity Magazine (uscybersecurity.net)

Security by Design is really the initiation point of a risk management process—especially if you are a software or hardware developer concerned with security. In fact, DHS CISA recently came out with a strategy for both the private and public sectors making security by designing a preferred course of action. Please see: Secure by Design, Secure by Default | CISA

Defense in Depth. A variety of strong definitions exist for defense in depth in the security community**.** A NIST publication defines the Defense-in-depth concept as “an important security architecture principle that has significant application to industrial control systems (ICS), cloud services, storehouses of sensitive data, and many other areas. We claim that an ideal defense-in-depth posture is 'deep', containing many layers of security, and 'narrow', the number of node independent attack paths is minimized." Measuring and Improving the Effectiveness of Defense-in-Depth Postures | NIST

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources. A zero-trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established. Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud- based assets that are not located within an enterprise-owned network boundary. Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource. This document contains an abstract definition of zero trust architecture (ZTA) and gives general deployment models and use cases where zero trust could improve an enterprise's overall information technology security posture. Zero Trust Architecture | NIST

RISK Management and icons on a virtual screen. Man tapping on the screen GETTY

Frameworks, processes, strategies, operational SOC are elements that should be prioritized in industry and government. I provided a working checklist in a recent article in Homeland Security Today on the topic that can be found at the following link: Using SOCs and Cybersecurity Hubs to Prioritize Security Operations in a Critical Era - HS Today

A useful publication to better understand the importance of the role of SOCs that was written in 2021 is "The Evolution of Security Operations and Strategies for Building an Effective SOC" by Lakshmi Narayanan Kaliyaperumal. The author noted that "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)." And that "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 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."

Please see: The Evolution of Security Operations and Strategies for Building an Effective SOC (isaca.org)

The Importance of SOCs is a global issue and the importance of the SOC role is recognized in new legislation by the European Community. The proposed EU Cyber Solidarity Act, aims to strengthen cybersecurity by creating better detection, preparedness, and response to significant or large-scale incidents. This involves creating a European Cybersecurity Shield and a Cyber Emergency Mechanism, using national and cross-border state-of-the-art Security Operations Centers (SOCs) tasked with detecting and acting on cyberthreats. The EU's Cyber Solidarity Act: Security Operations Centers to the rescue! | WeLiveSecurity

In summary, innovative technologies, (some of which I have highlighted) and which are being introduced in 2023 at RSA and other venues are focused on those capabilities and will significantly assist SOC operators with cybersecurity challenges. Being aware of the resources available and operational requirements for SOC cybersecurity is a starting point for business, government, and many organizations. The cyber threats and risks are too high not to be proactive in advancing the capabilities of security operations centers.

TOP CYBER NEWS
MAGAZINE
FEBRUARY 2022
Chuck D. BROOKS
BROOKS CONSULTING INTERNATIONAL
CHANGING the CYBERSECURITY AWARENESS
May THE Techs Be With You
Exclusive article by
June R. KLEIN
CEO at Technology & Marketing Ventures Inc.
HOW CHUCK D. BROOKS IS CHANGING CYBERSECURITY AWARENESS, REACHING THE RIGHT MIND AT THE RIGHT TIME, STEP BY STEP, RAISING UNDERSTANDING OF THREATS IN CYBER REALM

Chuck Brooks TOP CYBER NEWS MAGAZINE

Chuck Brooks is a globally recognized thought leader and subject matter expert Cybersecurity and Emerging Technologies. Chuck is also an Adjunct Faculty at Georgetown University's Graduate Cybersecurity Risk Management Program where he teaches courses on risk management, homeland security technologies, and cybersecurity. LinkedIn named Chuck as one of "The Top 5 Tech People to Follow on LinkedIn." He was named "Cybersecurity Person of the Year for 2022" by The Cyber

Express, and as one of the world's "10 Best Cyber Security and Technology Experts" by Best Rated, as a "Top 50 Global Influencer in Risk, Compliance," by Thompson Reuters, "Best of The Word in Security" by CISO Platform, and by IFSEC, and Thinkers 360 as the "#2 Global Cybersecurity Influencer." He was featured in the 2020, 2021, and 2022 Onalytica "Who's Who in Cybersecurity" He was also named one of the Top 5 Executives to Follow on Cybersecurity by Executive Mosaic, He is a GovCon Expert for Executive Mosaic/GovCon Wire, He is also a Cybersecurity Expert for "The Network" at the Washington Post, Visiting Editor at Homeland Security Today, and a Contributor to Skytop Media, and to FORBES. He has an MA in International relations from the University of Chicago, a BA in Political Science from DePauw University, and a Certificate in International Law from The Hague Academy of International Law.

FIBERNET

Cybersecurity Archives - Fibernet

IBM

Security QRadar | IBM

IBM NEWSROOM

IBM Launches New QRadar Security Suite to Speed Threat Detection and Response

Follow me on Twitter or LinkedIn. Check out my website.

Chuck Brooks

Follow

Chuck Brooks, President of Brooks Consulting International, is a globally recognized thought leader and subject matter expert... **Read More**

Editorial Standards

Reprints & Permissions