WHITE PAPER

HOW WILL AI-FIRST SOC CHANGE CYBER SECURITY?

Infosys®
Navigate your next

How can AI radically transform the first line of defense of enterprise security?

Under the onslaught of Artificial Intelligence (AI) powered threats and ransomwares, enterprises struggle to find the right balance between detection and effective response to threats. For enterprise scale cyber defense, it is critical to build, refine and evolve Security Operations Centers (SOC) using AI. The AI-First SOC is prioritizing organization design change, use cases and AI technology radically change their security operations.

Heather Hoff, an operator in Diabolo Canyon nuclear plan, California was horrified to see the meltdown of Fukushima nuclear reactor thousands of miles across the Pacific Ocean. The Japanese nuclear reactors were designed to withstand earthquakes, but vulnerable to large tsunamis. The great East Japan earthquake stuck the Fukushima region created an unprecedent fifteen meters high tsunami wave. The plant was designed based on the scientific knowledge collected in 1960s. It was built ten meters above sea level based on the historic data indicating a max limit of three-meter-high tsunami waves. This example explains the point of how standardized process can create baseline for defense, but still fail in dynamically changing situations such as the modern SOC.

Three out of Four security professionals agree SOC needs to evolve to manage the continuous siege of threats, avoid burn out of security team and manage over saturation of tools. To operate in a dynamic environment, the modern SOC must transform into an AI-First organization with focus on intelligence, improve the standard process and amplify the abilities of the SOC analyst.

AI's ability to process vast amounts of data at unprecedented speeds allows for the identification of patterns and anomalies that human analysts might miss. The enormous data quantities that machine learning can analyze is beyond human capacity and creates exponential scale for the SOC. This capability facilitates near real-time threat detection, significantly reducing the time between initial compromise and discovery. Further, AI systems can automatically categorize and prioritize alerts, drastically reducing the flood of false positives that often overwhelm Tier 1 analysts.

Mega trends driving AI in security operations

The modern SOC needs a solid process foundation and the right technology platform to amplify the defender potential. Enterprise SOC set up across the globe struggle with key challenges pertaining to:

Volume

Today's SOC analysts face a complex challenge that contribute to high stress levels and burnout. They are overwhelmed by the high volumes of data they process, often described as finding needles in ever-growing haystacks. This information overload and poor engineering is compounded by an abundance of false positives, with over 50% of SOCs struggling to keep up with alerts. As per a study by Ponemon Institute, 65% of SOC Teams suffer burn out. A more exhausted team with a large volume of alerts from disconnected end points can lead to inaccurate detection and response. Vasts volume of data from multiple tools result in the overwhelming number of incidents and alerts for the SOC to investigate and resolve. This negatively affects the overall security posture.

Velocity

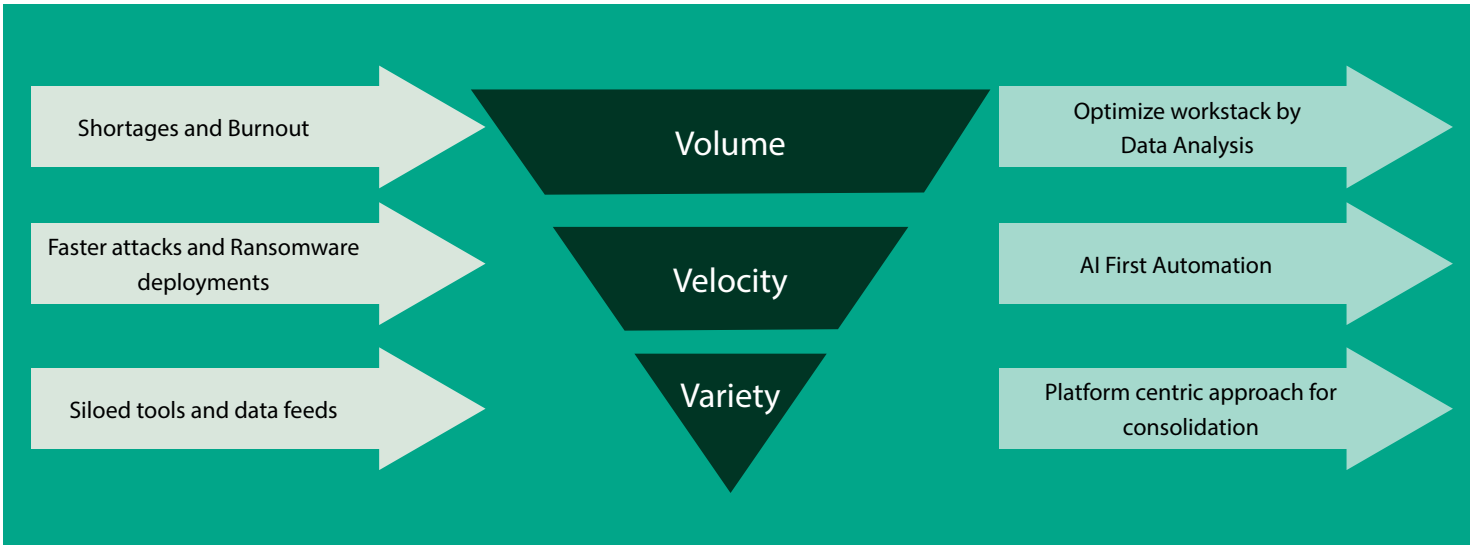
Velocity of comprehension of an attack is critical for an enterprise respond and recovery with minimal impact.

The pace of attacks is crucial and as a cascading business impact. For instance, Clorox had a cyber-attack which damaged portions of its order management application and caused orders to be processed manually. This resulted in dip in sales, brand image and eventual share price.

Cybercriminals equipped with Gen AI based weaponry are now deploying ransomware within 24 hours. which used to take more than four to five days.

Variety

Too many siloed tools and data feeds results poor threat detection outcomes and delay in incident response. Complex organization structures, such as decentralized operations and independent operations of IT and cyber security teams, further widen the gap for the SOC operations. For instance, the Log4j vulnerability created a global impact due to this. The nature of the vulnerability not only impacted the apps using the library but also any service that used these applications. Enterprises and end users alike did not realize how widespread this issue within their IT landscape. When handling alerts SOC analysis struggled with alert fatigue and manual correlation was not scalable for the high volumes experienced. Increasing complexity of the IT landscape and lack of awareness of the loop holes of the backend systems make it difficult find the root cause in time.



Key challenges faced by SOC teams

The case for AI-First SOC - Business Framework

The overemphasis on technology in cybersecurity is a persistent problem. Siloed teams with divergent objectives or conflicting priorities result from a lack of an organization-wide, top-down strategy and consistent communication.

Security professionals struggle to quantify how their security and compliance activities in the SOC delivers value. Further according to a study in LogRthym, 85% of the business face unintended security process and technology duplication. In this state, asking enterprises to invest in AI for Cyber defense and SOC modernization is a hard ask. Enterprises must align security outcomes with business priorities through an AI-First SOC.

As SOC faces pressures from regulatory, financial and organizational dynamics. The focus of the AI first SOC should be:

1. SOC Goals and benchmarks aligned with the AI investments

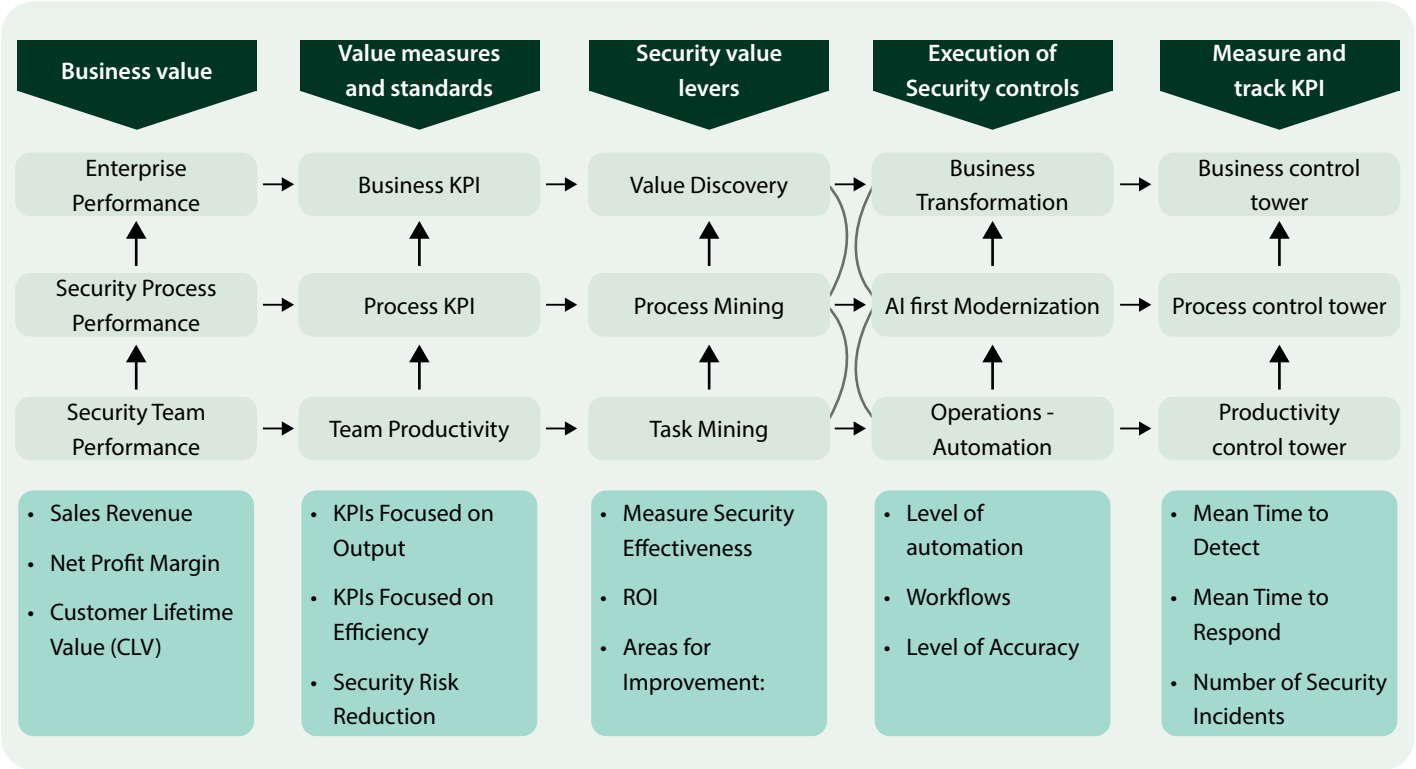
The enterprise would want to have a metric of improving security posture against external attacks. This would need constant measurement of the percentage of the systems which needs to be fully patched. AI investments should be aligned to clear SOC goals and evaluated on the resources consumed, dependencies and objective data collection process.

2. AI adoption based on Value

Intelligent Value Realization from an AI-First SOC is baseline on AI adoption in SOC to create measurable outcomes. The outcomes can be simplifying the process, building better analyst experience or improving operational metrics like Mean time to remediate (MTTR).

3. Strategic decision making

Aligning security outcomes with business goals gives insight into how the SOC's operational priorities are aligned to level of risk. Many cyber professionals struggle to explain or quantify how their SOC activities support the business and ultimately deliver value. AI-First SOC must simplify processes for reporting key performance indicators (KPIs) that relate to company goals and demonstrate alignment with the overall business strategy.



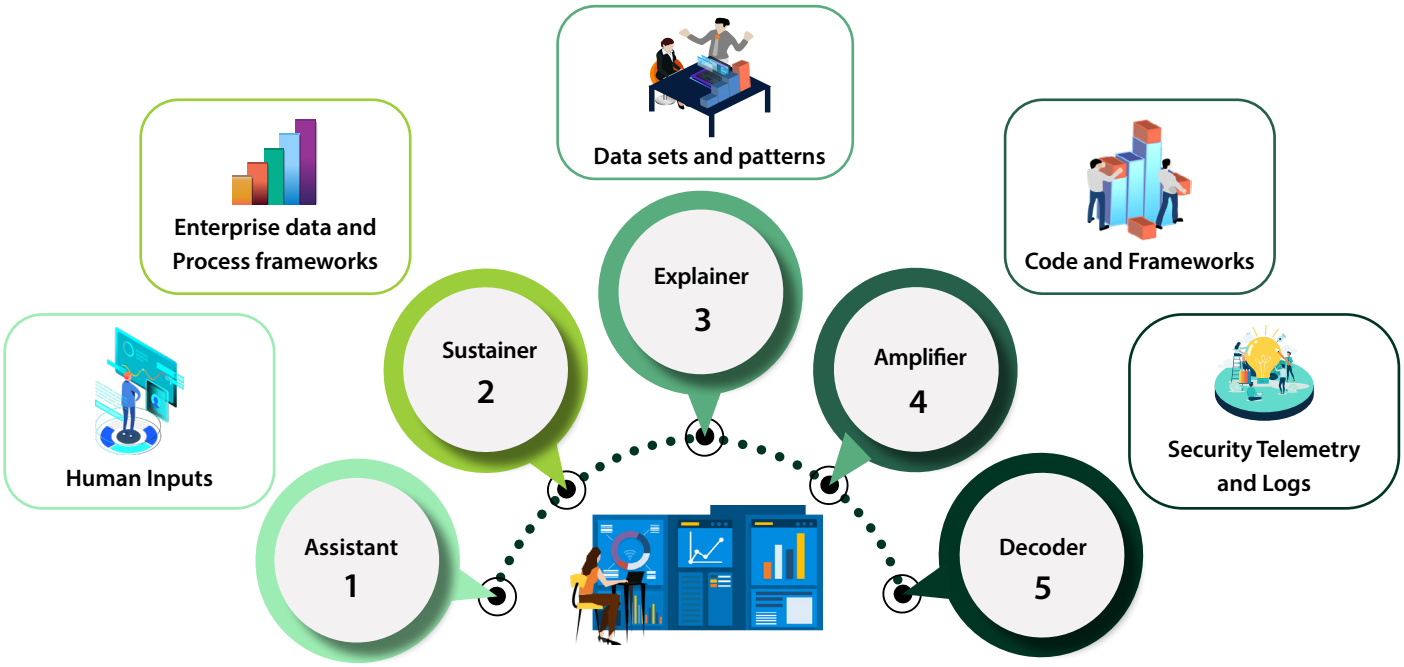
Role of AI in transforming the conventional SOC operational models

AI is critical to build cyber defense as it has proved good in reduction of false positives, scanning large data volumes to identify patterns and provide Gen-AI based assistants for personas in a SOC. While AI is here to radically alter security operations and who does it, the larger impact comes in collaborating and amplifying the defender's capabilities and not replacing them.

Through collaborative intelligence, SOC team and AI actively enhance each other's complementary strengths. What comes naturally to an analyst in SOC (calling out for help from a senior analyst) can be tricky for machines and what is straightforward for machines (analyzing large volumes of incident data for false positives) will be impossible for humans.

To make this augmentation of defender potential, enterprises should re-think the SOC processes to support the partnership. The following are five key types of interconnected Cyber AI capabilities which enables us to visualize an AI-First SOC.

Five Key Interconnected Cyber AI Capabilities for an AI-First SOC



Assist – Cyber Assistance for persona of the Security Team

Gen-AI Assistants in SOC must focus on the experience they provide in the SOC and buildt a 2-way conversation with the SOC Analyst. AI algorithms must be taught how to assist the SOC team members based on their work requirements. In this effort to build personalized assistance, the assistant should be trained with large training data sets are used to teach machine translation apps to handle security operations through ingestion log data, incident and alert data along with the reactions of SOC team members to different possible scenarios.

Consider Microsoft Security Co-pilot, the Gen-AI assistant must develop the right temperament and personality to match the high-pressure environment of the SOC: Confident, Assertive and Calm to match the mood of the SOC. This requires iterative training and testing with human inputs on responses from experts.

Gen-AI assistants to display complex and subtle human traits need human trainers to build the right personality.

Sustain – Improved operational efficiency

Making the cybersecurity analyst's work as straightforward and efficient as possible is a primary justification for updating your security processes. AI should help SOC Teams to build consistent, continuous, contextual process which can help them sustain the SOC operations across multiple shifts 24X7X365.

For instance, a security analyst can be trained to run AI based data discovery tools which can scan and find sensitive data which can be exploited by threat actors. This requires a significant training where the analyst can understand the limitations of the AI powered tool to correct and override the wrong decisions taken by Cyber AI applications. Once trained, AI can sustain repeatable process.

Most SOC teams' heavy workloads add to the pressure of effectively managing cyber-risk. Attrition rates are notoriously high in the SOC. Automation and improved efficiency enables the analyst's process followed daily and reduce their fatigue.

Explain – Nonhuman experts in Cyber defense

AI are increasingly replacing human experts in their field. SOC is not exception in AI based assistance for non-expert users.

Reverse engineering requires analysis of the semantic information from source code. This requires human experts to painstakingly analyze code to find the application boundaries, flow of data and process control. Deep learning algorithms trained on code binaries can identify patterns and anomalies that would have previously remained undetected from legacy SOC methods.

As many of the commercial software do not provide source code, AI based reverse engineering proves to be the right tool for hard to identify, uncover and predict security issues in code.

Amplify – Amplifying defender potential

AI can boost our analytics and decision-making ability by providing the right information at the right time. While AI tackles most threats in an automated process, skilled analysts can focus on the most advanced threats, creating a more fulfilling role and career path.

AI can automate threat hunting activities, proactively searching for threats that may have evaded traditional detection methods.

A Threat hunter does not have to know the queries to hunt for patterns. AI trained on internal and external intelligence sources interpreted within the guardrails of a framework such as ATT&CK can detect threats that may be missed by human analysts.

This helps to bridge the rising skill gap in the cyber security world and reduce the cost of security operations.

Decode – Demystifying the unknown-unknown threats

A modern SOC not only recognizes the need for formalizing intelligence collection using a framework, but systematically puts collected observations into action.

For example, looking at user behavior, anomalies may reveal compromised accounts and systems faster than intelligence or rule-based approaches because of how compromised accounts may stand out against a baseline of typical peer behavior.

One powerful way to do so is through the maintenance and use of Priority Intelligence Requirements (PIRs) to steer intelligence efforts. Because PIRs require consistent review to maintain alignment to the organization's goals and concerns, they naturally align with healthy habits such as proactive threat modeling and threat landscape assessment.

SOC Manager

Experience – Co-pilot and AI based reporting

SOC Operations

Explainer – Identify patterns in threat data

Tier 1 — Triage Specialist

Sustainer – AI based Automation

Security Engineer

Decoder – Anomalies and loopholes

Tier 2 — Incident Responder and Threat Analyst

Explainer – Identify patterns in threat data

Tier 3 — Threat Hunter and Intel Analyst

Amplified – NLP for Threat hunting

AI for each Persona in Enterprise Security Teams

AI-First SOC and how can we avoid the common pitfalls

Digitization and AI can spur productivity gains, but there is no crystal ball to show how a SOC will evolve in the next 10 years. Business leaders should take the right steps to build an AI powered intelligent SOC which can scale and provide productivity gains over time. There are three stages of capabilities which AI powered SOC can be equipped:

Protect the human defender through Guardrails

AI in SOC is beyond replacement of team members and cost savings. AI can help augment the capabilities of the human defender. One SOC analyst says, "I could use AI for generating threat hunting queries writing which is boring and waste of time". This is a positive view of AI, where AI helps security teams to augment their skills AI as useful helpers. AI can offload routine mundane boring tasks to build new tools which can improve communication and experience. Further, this becomes a channel to build better security products, services and business models in the SOC. AI handles more routine tasks, focusing on building the right guardrails has become even more important. Cyber AI must be fair, ethical and have high privacy standards to ensure AI augments capabilities that are compliant to regulation, can cause no physical or mental harm to users and not liable to legal risks to the enterprises.

Rethink the organization design of SOC

Enterprises cannot get the best of their AI investments using the same security team roles, job descriptions and organization structures. Leaders must access the team roles. They must be open to activities and related roles which are needed to manage AI, evolve it and keep the human in loop. A larger energy major based out of UK, has built a Gen-AI assistant which aims to make the security team more productive. To build this Gen-AI assistant effectively, there enterprise needed a non-hierarchical AI organization through which employees collaborated across business functions, organization silos and data islands. This helped the enterprise deploy the right human talent to experiment, validate and iteratively build AI to assist their security team.

Security Team members as AI Partners

Help of security team members is critical to transform SOC and strike the right balance between investing into AI and run the core security tasks. As per Infosys Survey, security team members and employees in general are eager to learn new skills and stay relevant in their field. Without the support of the current SOC team, the invest on an AI-first SOC and additional intelligence is a waste. Involvement of key team members bring the human elements for AI adoption such as creativity, empathy and problem solving. Further, building soft skills like communication, teamwork and strategic thinking is equally pressing, as these human-centric abilities become more valuable in an AI-augmented workplace.

The debate of fully autonomous AI driven SOC will continue to rage on, but enterprises should accept that AI is going to transform their security operations. Further, there is a need to use AI to build the first line of defense against emerging AI powered threats. AI-First SOC is only the first step towards what enterprises will go through to thrive in this exciting Gen-AI era.

Future of SOC

The future transformation of SOC is one of the biggest blackhole faced by enterprises today. AI, big data analytics and advance automation helps algorithms take cyber defense tasks which require a human to perform. The opinion on AI is split between AI eliminating security team members or augment intelligent threat detection capabilities. As per Accenture research, some enterprises are transforming themselves into intelligent enterprises where decisions taking place in the SOC are digitized, data driven where AI can perform both detection and prevention.

While the future capabilities of AI are unknown, one scenario might be the integration of AI in SOCs moving toward greater automation and even "self-healing" SOC which can run by intelligent AI systems. This future state could include automated remediation of more incidents without human intervention, and SOC must be an AI powered orchestration layer across IT, security and compliance functions.

Decision making algorithms are data driven tools not artificial minds. This misconception leads to unrealistic or even misleading expectations for what AI can defend. As AI handles more routine tasks, focusing on problem-solving and critical thinking becomes even more important. These skills are needed for tackling the complex security challenges that AI can't solve alone. Building soft skills like communication, teamwork and strategic thinking is equally pressing, as these human-centric abilities become more valuable in an AI-augmented workplace.

For those starting or advancing their careers in cybersecurity, preparing for an AI-integrated future is crucial. Embracing continuous learning is key, with a commitment to ongoing education in both traditional security concepts and emerging AI technologies. Developing a strong foundation in networking, operating systems and security principles remains essential, as AI will augment these skill areas rather than replace them.

References and further reading

- https://www2.deloitte.com/content/dam/Deloitte/us/Documents/about-deloitte/us-google-cloud-soc-whitepaper.pdf
- https://www.cnbc.com/2022/06/07/the-diablo-canyon-control-room-turned-this-mom-into-a-nuclear-advocate.html
- https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-daiichi-accident
- https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/cortex-xsiam
- https://www.linkedin.com/pulse/velocity-new-currency-cybersecurity-bill-thorn-cfqoe/
- https://www.usatoday.com/story/money/retail/2023/09/18/clorox-shortage-cyber-attack-2023/70892434007/
- https://www.darkreading.com/vulnerabilities-threats/5-tips-for-modernizing-your-security-operations-center-strategy
- https://www.microsoft.com/en-us/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/
- https://gallery.logrhythm.com/analyst-reviews-and-reports/logrhythm-na-the-state-of-the-security-team-research-report-2022.pdf
- 70% of the SOC experience burn out - https://www.darkreading.com/threat-intelligence/more-than-70-of-soc-analysts-experiencing-burnout
- https://www.creativebloq.com/news/uber-eats-ai-image-generation

About the Author

Karthik Nagarajan

Practice Manager and Senior Industry Principal

Karthik heads Cyber Platforms and Infosys Data Protection Practice. He has 18+ years of experience in Product design and consulting. He is an expert on AI, Data Protection and Customer Experience Strategy.

For more information, contact askus@infosys.com

Infosys®
Navigate your next