paloalto NETWORKS | CORTEX

The SOC Analyst Career Guide

What's Going to Be the Human's Job?

Powered by ConversationalGeek

The Changing Landscape of Security Operations Centers

In the era of digital transformation, security operations centers (SOCs) stand at the forefront of an organization's cyber defense. As technology rapidly evolves, so too does the role of the SOC and its analysts. This guide explores a pivotal shift in the cybersecurity landscape: the integration of artificial intelligence (AI) into SOC operations, offering insights from industry thought leaders on the future of AI-driven SOCs.

Traditionally, SOCs have been the nerve centers of cybersecurity efforts, employing skilled analysts to monitor, detect, and respond to threats. These analysts have relied on a combination of technology, expertise, and intuition to protect their organizations from an ever-growing array of cyberthreats. However, the increasing sophistication and frequency of attacks are pushing traditional SOC models to their limits.

> *"The increase in cyberattack sophistication necessitates a proactive approach from SOCs to integrate AI for better defense mechanisms."*
>
> —Chris Scott, Managing Partner, Palo Alto Networks

This observation above encapsulates the central theme of our guide - the transformation of SOCs through AI integration. The advent of AI in cybersecurity is not just an incremental change; it represents a paradigm shift in how we approach threat detection, analysis, and response. AI has the potential to enhance the capabilities of SOC analysts, streamline processes, and provide insights at a scale and speed previously unattainable. Yet, this technological leap also raises important questions about the future role of human analysts in AI-augmented SOCs.

In this guide, we will explore:

- ✔ How AI is reshaping the SOC environment
- ✔ The evolving roles of SOC analysts at different tiers
- ✔ The new skills and competencies required in an AI-driven SOC
- ✔ The challenges and opportunities presented by AI integration
- ✔ Practical steps for SOC professionals to prepare for this AI-driven future

By understanding these changes, current and aspiring SOC professionals can position themselves at the forefront of this exciting transformation in cybersecurity. As we delve into the details of AI's impact on SOCs, remember that while technology is rapidly advancing, the human element remains crucial. The future of SOCs lies not in replacing human analysts, but in creating a powerful synergy between human expertise and AI capabilities.

How AI Will Impact the SOC

The inclusion of AI into the SOC has the potential to radically change the way a SOC functions. Consider the three pillars on which SOCs are built: *people*, *process*, and *technology*. All three will be impacted by the inclusion of AI.

People

People are the main asset in a SOC; great technology and processes are useless without skilled and experienced staff. AI will greatly enhance the capabilities of tier one analysts, allowing them to perform at higher levels more quickly by using AI as a copilot. AI can help non-native English speakers produce high-quality deliverables and access vast knowledge instantly, saving time and improving productivity. Lower tier analysts can leverage AI to address unfamiliar incidents more efficiently by providing enriched information quickly. The result may also positively impact higher tier analysts, allowing them to focus on more complex and critical incidents.

AI also will enrich data more effectively and offer more timely and accurate alerts, allowing analysts to focus more on remediation. However, AI's methodical nature suits SOC tasks that involve data analysis and anomaly detection but will likely fall short in creative problem-solving scenarios. Therefore, human analysts will remain essential in the SOC.

> *"AI will empower SOC analysts by automating routine tasks, allowing them to focus on more complex and strategic aspects of cybersecurity."*
>
> —Oded Awaskar, Senior MDR Analyst, Unit 42

Process

AI will likely improve response times by filtering vast amounts of data to highlight significant alerts for human review, enhancing efficiency, and providing faster access to relevant information and insights. SOCs will benefit from AI's ability to triage and categorize alerts, reducing the burden on human analysts and allowing them to focus on response to eminent threats.

AI's deeper insight into data can benefit SOCs by recommending better ways to visualize data, enhancing report quality and understanding. Additionally, AI will help create and evolve playbooks based on past investigations – likely in an ongoing automated fashion with human review and approval. AI-driven playbooks will ensure consistency across analysts and can adapt based on new steps added by analysts, improving SOC efficiency without constant manual updates.

"AI-driven automation in SOCs will reduce manual efforts and errors, leading to faster and more accurate threat detection and incident response."

—Niall Browne, SVP & CISO, Palo Alto Networks

Technology

While true AI in the SOC is a new addition, many SOC systems leverage ML to improve threat detection accuracy and response times.. Advanced machine learning algorithms analyze patterns and anomalies in real-time, providing early warnings and actionable insights. This integration can lead to the development of more sophisticated and adaptive security protocols.

But AI has the potential to go far beyond just pattern analysis and improve many ways technology is used in the SOC. Here are a few examples:

AI will enhance the use of "copilot" functionality, assisting analysts by providing deeper context and understanding of the activity represented by the complex mix of data sources. AI-driven automation will streamline repetitive tasks, such as log analysis and incident categorization, allowing human analysts to focus on more complex issues.

AI also has the potential to transform the way SOCs handle threat intelligence. By leveraging AI, SOCs can aggregate and analyze vast amounts of threat data from multiple sources, including dark web forums, threat databases, and social media. This comprehensive analysis can help in predicting potential threats and vulnerabilities, allowing SOCs to take preemptive measures.

AI can aid in developing advanced forensic capabilities. AI-powered tools can assist in incident investigation by correlating data from different events and identifying the root cause of security breaches more quickly and accurately. This can significantly reduce the time required for incident response and recovery, minimizing the impact of cyberattacks.

AI will lead to the creation of more intuitive and user-friendly interfaces. These interfaces can simplify complex data visualization, making it easier for analysts to interpret and act on the information. AI can also facilitate natural language processing (NLP) to allow analysts to interact with systems through voice or text commands, enhancing operational efficiency.

Overall, the impact of AI on SOC technology will be profound, leading to more efficient operations, faster threat detection and response, and an improved overall security posture.

Now that you have a fundamental understanding of how AI will impact a SOC's people, process, and technology, let's dive a little deeper into the human element within an AI-driven SOC and look at how specific roles within the SOC will be impacted.

Roles That Will Be Impacted by AI in the SOC

AI presents an opportunity for SOC analysts to engage more in the AI process, possibly by contributing to coding and evolving AI tools. AI can help SOC analysts broaden their skill sets and career paths, moving towards data science roles. The role of SOC analysts will shift to more tactical functions, focusing on leveraging AI for better detection and response.

> *"AI-driven automation will enable real-time threat mitigation, transforming the role of SOC analysts from hands-on responders to strategic overseers who ensure the AI operates effectively and accurately."*
>
> —George Finney, CISO, The University of Texas System

Let's look at the specific roles that will be impacted.

Tier 1 SOC Analysts

AI will enhance tier 1 analysts by acting as a knowledge base and training tool. For example, AI can provide real-time suggestions and insights based on historical data and current threat intelligence, helping tier 1 analysts to understand and respond to incidents more effectively. This can accelerate their learning curve, allowing them to perform at higher levels, closer to those of tier 2 analysts, more quickly.

Furthermore, as AI handles more of the mundane tasks, tier 1 analysts will have more opportunities to engage in strategic activities, such as threat hunting and proactive security measures. This shift will not only make their roles more challenging and rewarding but also help in retaining talent by reducing burnout associated with monotonous work.

In a few years' time, tier 1 roles may be largely handled by AI, pushing the need for higher-level analysts. The entry point for SOC analysts will evolve as AI takes over more routine tasks.

Tier 2 and 3 SOC Analysts

AI will bring significant enhancements to the roles of tier 2 and tier 3 SOC analysts, primarily by augmenting their capabilities and enabling more strategic and in-depth analysis. These higher-tier analysts, who are already skilled in handling complex security incidents and deep investigations, will find their roles evolving in several key ways.

Tier 2 SOC Analysts

Tier 2 analysts are responsible for more in-depth investigations, incident response, and fine-tuning of security systems. AI will provide these analysts with advanced tools to expedite their tasks and improve accuracy. For instance, AI will assist in identifying intricate attack patterns that might be missed by human analysis alone. By processing and correlating vast amounts of data, AI can uncover subtle indicators of compromise (IOCs) and provide actionable insights faster than traditional methods.

AI will also help tier 2 analysts develop coding and scripting skills. Many AI tools require customization and integration with existing SOC workflows. As analysts interact with these tools, they will naturally gain proficiency in scripting languages and automation frameworks, enhancing their technical skill set. This capability will be particularly valuable for automating repetitive tasks, such as log parsing and threat hunting, allowing analysts to focus on more strategic activities.

Moreover, AI can streamline incident response by suggesting optimal response actions based on historical data and learned patterns. This can significantly reduce the time needed to contain and mitigate threats. AI-driven playbooks will ensure that tier 2 analysts follow best practices consistently, while also allowing them to adapt and improve these playbooks based on new threat intelligence.

> *"Tier two analysts will see their roles evolve as AI handles more routine tasks, allowing them to focus on deeper analysis and incident response. Their expertise will be essential in fine-tuning AI systems and addressing complex security challenges."*
>
> —George Finney, CISO, The University of Texas System

Tier 3 SOC Analysts

Tier 3 analysts are the experts who handle the most challenging and sophisticated security incidents. They possess a deep understanding of the organization's environment and are responsible for strategic oversight and long-term security improvements. AI will enhance their role by providing deeper analytical capabilities and facilitating more proactive security measures.

AI tools can assist tier 3 analysts by offering predictive analytics, which can forecast potential threats based on current trends and historical data. This predictive capability allows analysts to anticipate and prepare for attacks before they occur, shifting the SOC's posture from reactive to proactive. AI can also help in creating and managing advanced threat models, enabling tier 3 analysts to design more effective defense mechanisms.

Furthermore, AI will aid tier 3 analysts in optimizing security infrastructure. By continuously monitoring and analyzing system performance and security events, AI can identify areas for improvement and recommend adjustments to security policies and configurations. This continuous optimization ensures that the SOC remains resilient against evolving threats.

AI will also support tier 3 analysts in advanced forensic investigations. By correlating data from multiple sources and automating the tedious aspects of data analysis, AI allows these analysts to focus on interpreting findings and making strategic decisions. This can lead to quicker resolution of incidents and a deeper understanding of the threat landscape.

SOC Managers

The role of SOC managers will also undergo significant changes with the integration of AI. As leaders responsible for overseeing security operations and ensuring the effectiveness of their teams, SOC managers will need to adapt to a more AI-centric environment. One of the primary impacts will be on decision-making processes. With AI providing enhanced data analysis and insights, predicting trends, and recommending action plans for today, six months, and a year ahead, SOC managers will be able to make more informed strategic decisions. AI can help identify trends, predict potential threats, and evaluate the effectiveness of security measures, allowing managers to allocate resources more efficiently and prioritize actions based on real-time data.

Additionally, SOC managers will need to develop a deeper understanding of AI technologies to effectively lead their teams. This includes knowledge of how AI tools function, their limitations, and how to interpret AI-generated insights. Managers will be responsible for ensuring that AI tools are properly integrated into SOC workflows and that their teams are adequately trained to use these tools. They will also need to monitor the performance of AI systems, addressing any issues that arise and continuously optimizing AI applications to align with evolving security needs.

Furthermore, SOC managers will play a crucial role in fostering a collaborative environment, where human analysts and AI tools work seamlessly together. This involves promoting a culture of continuous learning and adaptation, encouraging analysts to embrace AI as a valuable asset rather than a threat to their roles. Managers will need to balance the strengths of AI with the unique capabilities of human analysts, ensuring that both are utilized to their full potential. By effectively integrating AI into the SOC, managers can enhance their team's efficiency, reduce response times, and improve overall security outcomes.

> *"SOC Managers will need to bridge the gap between AI-generated insights and business decisions, effectively communicating risks and actions to the C-suite while ensuring their team leverages AI tools optimally."*
>
> —Donnie Hasseltine, VP of Security, Second Front

How Will AI Impact the SOC Team Overall?

There are also some specific ways the insertion of AI into the SOC will impact the entire SOC team, establishing an ability to leverage people with diverse skill sets and experience to craft the next generation of SOC personnel.

Lower Barrier to Entry

AI has the potential to revolutionize the training and onboarding processes in cybersecurity, making it easier for new talent to enter the field and take on a role within a SOC. Traditionally, becoming proficient in cybersecurity – something usually desired for even the lower analyst tiers – required extensive technical knowledge and hands-on experience, which could be a barrier for many aspiring professionals. However, AI-based learning tools can provide interactive and adaptive training experiences, providing instant feedback and personalized learning paths, accelerating the development of essential skills and reducing the time and resources needed for training.

In addition to improving training, AI can democratize access to cybersecurity roles by lowering the technical barriers to entry. AI-driven SOC platforms will guide individuals through complex tasks, such as configuring security systems or analyzing threat data, without requiring analysts to have deep prior knowledge. For example, AI can assist users in understanding and implementing best practices for network security or interpreting the results of vulnerability scans.

This capability opens doors for individuals from diverse backgrounds, including those without traditional IT or computer science degrees – as well as professionals from related fields (such as IT support or software development) – to transition effectively into cybersecurity roles within the SOC. As a result, the industry can tap into a broader talent pool, fostering diversity and inclusion within SOCs.

By making cybersecurity more accessible and less intimidating, AI will ensure that organizations can build robust, versatile SOC teams capable of defending against a wide range of threats.

The Number of Analysts

The number of analysts needed may decrease as AI automates more of the work accomplished today by humans. AI will be used to replicate and improve the investigation process, allowing SOC managers to focus on monitoring AI outputs and trends. Analysts will need to oversee AI operations, ensuring the accuracy of AI decisions and catching anomalies.

A Potential New Role: SOC Prompt Engineers

In the short run, the SOC may need prompt engineers who can effectively interact with AI tools to generate desired outputs. Expertise in crafting precise prompts is becoming valuable, especially in generating relevant and accurate results from AI models. As AI platforms learn from prompts and adjust automatically to provide better responses, this may become less necessary over time.

Emphasizing the Need for Humans

Despite AI's impressive capabilities in automating tasks and enhancing data analysis, it's important to note that human interaction will remain crucial within SOCs, especially when handling exceptions and nuanced scenarios. While AI excels in processing large volumes of data quickly, identifying patterns, and flagging anomalies, it lacks the intuitive understanding and contextual knowledge that human analysts bring to the table.

Humans excel in interpreting complex situations, making judgment calls, understanding the broader implications of security incidents, and ensuring user satisfaction. For instance, while AI can detect an unusual login pattern, a human analyst can correlate this with recent organizational changes or industry-specific threats, providing a more comprehensive and accurate response. The nuanced understanding and experience that human analysts offer are irreplaceable, particularly when dealing with sophisticated or novel cyberthreats that fall outside the scope of AI's programmed knowledge, as well as incidents that require human interpretation, such as a user making a mistake like emailing a customer list to an outside email address that looks like a threat action, but was actually an accident.

Moreover, human oversight is essential to mitigate the risks associated with AI use in cybersecurity. Advanced AI systems are not immune to errors, biases, or manipulations, such as data poisoning by attackers. These vulnerabilities necessitate vigilant human supervision to ensure AI decisions are accurate and reliable. For example, if AI incorrectly flags a legitimate software update as malicious due to a data anomaly, human analysts must step in to correct the false positive and prevent unnecessary disruptions.

> *"The human touch will remain crucial for interpreting AI-driven insights and ensuring the accuracy of responses."*
>
> —Niall Browne, SVP & CISO, Palo Alto Networks

Additionally, human analysts play a critical role in maintaining ethical standards and accountability in cybersecurity operations. They ensure that AI-driven actions align with organizational policies and legal requirements, protecting both the organization's assets and its reputation. Therefore, while AI significantly enhances the efficiency and effectiveness of SOCs, the strategic and critical thinking capabilities of human analysts remain indispensable in achieving a balanced and robust cybersecurity defense.

With every aspect of the SOC potentially being impacted by the use of AI, it's imperative that those impacted begin to take immediate steps to prepare themselves for how the SOC will change... and their role within it.

What Should SOC Leaders Do to Prepare Today?

As AI becomes an integral part of security operations centers, SOC leaders will play a critical role in ensuring that their teams are equipped to leverage AI effectively and that the transition enhances overall security posture. So, SOC leadership must be proactive in preparing for these technological advancements.

Below are some of the practical areas SOC leadership should take focus on today to prepare for an AI-driven future.

Understand AI: SOC leaders need to gain a deeper understanding of AI, how it can help, how it will be specifically used, and how it will impact decision-making. Leaders must ensure that AI tools are used correctly and that human analysts can adjust AI's operations. They must understand the strategic implications of AI recommendations and make informed decisions.

Ensure Analyst Competence: SOC managers should ensure analysts are well-versed in AI tools and processes, encouraging continuous learning, skill development, certification, and adaptation. Managers should expect candidates to use generative AI tools during assessments, ensuring they understand and interpret AI-generated data correctly.

Champion AI Integration: SOC leadership should focus on communicating AI-derived insights clearly to executive teams, ensuring informed decision-making. Organizations should foster a culture of continuous learning, keeping pace with AI advancements and integrating them into SOC practices.

What Should Those with Impacted Roles Do Today?

As AI continues to integrate into security operations centers, it is crucial for individuals currently in SOC roles, as well as those planning to enter the field, to prepare for these changes. The advent of AI will transform various SOC roles, enhancing efficiency and altering the scope of responsibilities. By taking proactive steps today, SOC professionals can position themselves to collaborate effectively with AI technologies and maintain their relevance in an evolving landscape. This section provides practical recommendations for different SOC roles, highlighting the skills and knowledge that will be essential for thriving in an AI-enhanced SOC environment.

Tier 1 SOC Analysts

In the next few years, the entry point for SOC analysts will evolve. The role of tier 1 analysts will become more sophisticated, requiring a solid understanding of AI tools and processes. While AI may take over many routine tasks, human analysts will still be essential for handling exceptions, providing oversight, and making nuanced decisions that AI cannot.

Tier 1 analysts will need to handle exceptions and interact with customers, maintaining human relationships and managing unique cases. Because of this, tier 1 analysts should develop a foundational understanding of AI processes and data inputs, enabling them to interact effectively with AI tools using the following practical recommendations.

Develop foundational AI knowledge: Gain a basic understanding of how AI tools work and how they can assist in cybersecurity tasks.

Embrace continuous learning: Stay updated with the latest AI advancements and their applications in cybersecurity.

Leverage AI for efficiency: Use AI tools to automate routine tasks and focus on higher-priority incidents.

Improve reporting skills: Utilize AI-driven NLP tools to enhance the clarity and precision of reports and incident summaries.

Collaborate with AI: Learn to work alongside AI tools, using them to provide enriched data and insights for more informed decision-making.

Practice with AI tools: Engage with AI-based training and simulation tools to build confidence and proficiency in using AI in daily tasks.

Higher Tier Analysts

Higher-tier analysts will need to become experts on the AI tools they use and the mechanisms behind them. They must grasp how data is processed, how rules are written, and how AI reaches its conclusions to ensure accurate and reliable outcomes by using the following practical recommendations.

Master AI tools: Gain in-depth knowledge of AI systems and understand their functionalities to effectively utilize them in advanced cybersecurity tasks.

Develop programming skills: Enhance your coding abilities, particularly in scripting and automation, to customize AI tools and integrate them into SOC workflows.

Understand data processing: Learn how AI processes data and the algorithms it uses to identify patterns and anomalies, ensuring accurate interpretation of AI-generated insights.

Optimize AI integration: Continuously refine and adapt AI tools to align with evolving security needs, ensuring they remain effective and reliable.

Focus on strategic analysis: Use AI to conduct deeper and more comprehensive threat analysis, leveraging AI's capabilities to uncover sophisticated attack patterns.

Lead AI-driven initiatives: Take an active role in developing and implementing AI strategies within the SOC, guiding the team in adopting and optimizing AI tools for enhanced security operations.

Conclusion

The integration of AI into security operations centers is set to bring transformative changes to the people, process, and technology within traditional SOCs. AI will enhance the capabilities of SOC personnel, streamline processes, and introduce advanced technological tools that will significantly improve efficacy and effectiveness in threat detection and response. Every role within the SOC will be impacted in some way, from tier 1 analysts to SOC managers. Understanding and embracing these changes is essential for maintaining a robust cybersecurity posture.

Those having or desiring roles within the SOC will need to adapt to new responsibilities and learn to collaborate with AI-driven tools. Processes will become more efficient, with AI handling repetitive tasks and enabling faster, more accurate decision-making. Technology will advance, incorporating AI to enhance data analysis, threat intelligence, and incident response capabilities. These advancements will collectively elevate the SOC's ability to protect organizational assets against sophisticated cyberthreats.

For those currently in SOC roles or those planning to enter the field, it's necessary to follow the practical steps outlined in this guide today to prepare for the AI-driven changes to the SOC. By proactively preparing for these changes, SOC professionals can remain at the forefront of daily cybersecurity efforts, effectively leveraging AI to create a more resilient and responsive SOC.

paloalto® NETWORKS | CORTEX®