VECTRA®

WHITE PAPER

Creating Your Custom SOC Upgrade

Table of Contents

Introduction....3
Section 1. The Problem and Why It's Time for an Upgrade....3
Limitations of Legacy Tools....3
Section 2. Choosing Your Approach: Four Paths to Upgrading Your SOC....4
AI-driven SOC Upgrade....4
The Power of AI-Driven Threat Detection....4
Machine Learning Algorithms in SOC Operations....4
Using Big Data and Advanced Analytics for Comprehensive Threat Analysis....4
Benefits of AI-driven Detection in Comparison to Traditional Methods....4
Automated Response and Integrated Signal: The Future of Cybersecurity....5
Incident Response Automation Using AI and Machine Learning....5
Hybrid SOC Upgrade....5
Setting up a Successful Hybrid/Co-Managed SOC....5
4 keys to choosing the right MDR upgrade....6
How Integrated Signal Helps SOC Teams....7
Human-first SOC Upgrade....7
Challenges and Considerations for Deploying Automated Response in SOC....8
Ensuring Accuracy and Reliability in Automated Response Mechanisms....8
Section 3. Completing a SOC Upgrade....9
Understanding XDR....9
XDR's Role in Upgraded Cybersecurity....9
1. Leveraging AI in XDR to Reduce Your Team's Workload....9
2. MDR for Shared Workload....9
3. Identity-Centric Workflow Shifts....9
4. Optimized Analyst Experience for Maximum Talent Utilization....9
Benefits of Using XDR in SOC Operations....9
Enhancing Security Information and Event Management (SIEM) through AI....10
AI-driven Security Orchestration, Automation, and Response Platforms....10
Scalability and Flexibility of AI-Optimized SIEM/SOAR Systems....10
Upgrading With a SIEM-less SOC....10
What to Expect Post-Upgrade....11
Say Goodbye to Silos....11
AI's Role Facilitates Information Sharing and Communication....11
Improving Efficiency Through Integrated Signal....11
Utilizing Integrated Signal for Proactive Threat Hunting....11
Total Talent Optimization and Improved Analyst Experience....11
Upskilling the Workforce and Augmenting Human Capabilities with AI....11
Section 4: Key Takeaways:....12

About Vectra AI

As the leader in hybrid attack detection, investigation, and response, Vectra AI arms your SOC team to quickly discover and respond to would-be attackers — before they act.

The Vectra AI Platform rapidly identifies malicious attacker behavior and activity across your hybrid cloud environment. Vectra AI's Attack Signal Intelligence™ will find it, flag it, prioritize it and alert security personnel so they can investigate and respond immediately.

Vectra AI finds attacks others can't using artificial intelligence to improve threat detection, investigation, and response (TDIR) over time, and eliminating false positives so your team can focus on real threats.

Introduction

Security Operations Centers (SOCs) are the front-line defenders against cyberattacks. However, many SOCs are forced to rely on legacy approaches and technology that are no longer efficient, nor effective at detecting and responding to modern hybrid attacks. Before we dive into the details, let's first reflect on how we got here:

- Digital transformation is driving the need for threat detection coverage across an expanding hybrid attack* surface.
- The need for detection coverage is driving siloed detection tool and rule sprawl for security architects and engineers.
- Detection tool and rule sprawl is driving unmanageable alert volume for SOC leaders and their team
- Unmanageable alert volume is resulting in excessive workload, burnout, and turnover for SOC analysts
- All the above is enabling modern hybrid attackers to move laterally and progress their attacks undetected.

While organizations are using new data sources like behavior analytics and IoT data to improve their security posture, it doesn't change the fact that it adds to an already overwhelming list of tasks, contributing to security analyst burnout and exhaustion. So how can we support the defenders without adding complexity or confusion to their roles? *Enter SOC Modernization.*

But don't worry, it's not as intense as cybersecurity companies would you have believe. In fact, the path to "modernizing your SOC" should be less about cranking up the intensity on your team, and more about upgrading the strategies and tools that can help them enjoy their job again. From here on out, we'll be ditching the term SOC modernization and opting for *SOC upgrade*. Because after all, you don't *modernize* your phone, TV, home, or anything else worth improving—**you upgrade**.

Section 1. The Problem and Why It's Time for an Upgrade

Limitations of legacy tools

Cyberattacks are becoming more sophisticated and complex all the time, and with the increasing volume and velocity of data: SOCs are collecting more data than ever before. This data needs to be analyzed and correlated in real-time to quickly identify threats. Unfortunately, legacy SOC tools and processes aren't equipped to handle this volume and velocity of data.

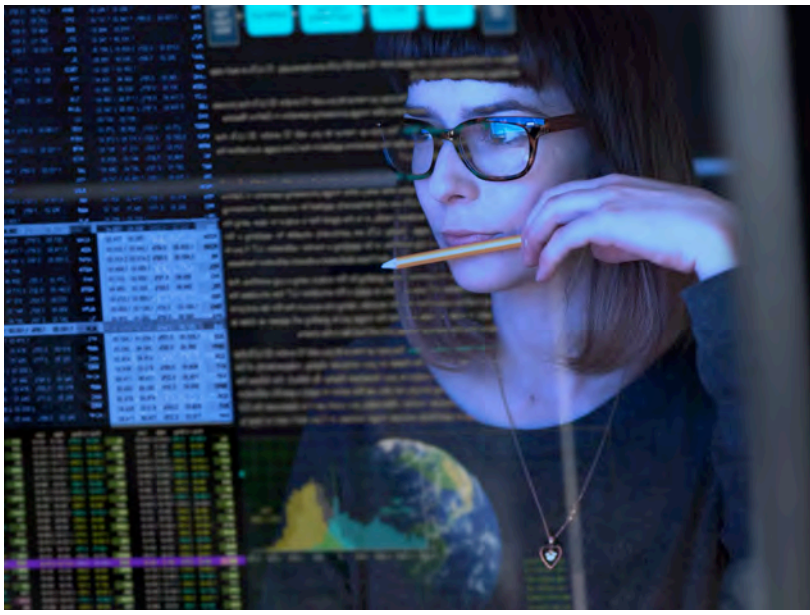
Traditionally Security Operation Centers (SOCs) have relied on a patchwork of legacy tools, including Packet Capture (PCAP) and Intrusion Detection Systems (IDS). These tools are siloed and fragmented, making it difficult for analysts to get a holistic view of their full security posture. Additionally, domain-specific tools like Endpoint Detection and Response (EDR), can be helpful, but they are simply not enough to protect organizations against the ever-evolving threat landscape.

According to a 2022 report by Enterprise Strategy Group, 80% of organizations use more than 10 data sources as part of security operations. This number has been increasing steadily in recent years, as organizations have become more aware of the importance of using a variety of data sources to detect and respond to threats.

The most common data sources used for security operations include:

- Endpoint data
- Network data
- Cloud data
- Threat intelligence feeds
- Security logs

Teams are desperate to rapidly correlate data from multiple sources, in the hopes of gaining a more complete view of their security posture and identify threats that would be difficult or impossible to detect using a single data source. However, managing and analyzing multiple data sources only magnifies the challenge of outdated tooling.



Section 2. Choosing Your Approach: Four Paths to Upgrading Your SOC

1. AI-driven SOC upgrade
2. Hybrid SOC upgrade
3. Identity-centric SOC upgrade
4. Human-first SOC upgrade

AI-driven SOC upgrade

IArtificial intelligence (AI) is playing an increasingly key role in SOC upgrades. AI-powered tools can help analysts automate tasks, reduce noise, and identify threats more quickly and accurately than traditional methods. For example, AI can be used to:

- Analyze large volumes of data from multiple sources to identify patterns and anomalies that may indicate an attack.
- Prioritize alerts and incidents to help analysts focus on the most critical issues.
- Automate tasks such as triage, investigation, and remediation.
- Transition from legacy tools to AI-based hybrid solutions.

While AI is a powerful tool, it is not a complete cure-all. Legacy tools still have a role to play in SOCs, especially for organizations with complex environments. The best approach is to transition to a hybrid strategy combining legacy tools with AI-powered tools.

The power of AI-driven threat detection

Artificial intelligence (AI) has fundamentally transformed the threat detection landscape. By leveraging AI, security teams can analyze vast amounts of data rapidly and accurately, finding patterns and inconsistencies that would be impossible for humans to spot. AI-driven threat detection systems can autonomously sift through huge datasets, making it possible to identify threats in real time or even predict them before they occur.

Machine learning algorithms in SOC operations

Machine learning algorithms are a type of AI that can learn from data over time and improve their performance without being explicitly programmed. They enable the system to learn from historical data and adapt to new threats. In SOC operations, machine learning can identify unusual behaviors, detect emerging threats, and categorize them based on their severity.

Machine learning algorithms can be used in a variety of SOC operations, including:

- **Threat intelligence analysis:** Machine learning algorithms can be used to analyze threat intelligence data from a variety of sources to identify new and emerging threats.
- **Log analysis:** Machine learning algorithms can be used to analyze log data from security devices and systems to identify suspicious activity.
- **Network traffic analysis:** Machine learning algorithms can be used to analyze network traffic to identify malicious activity, such as intrusions and denial-of-service attacks.

These algorithms continually refine their models, improving the accuracy of threat detection over time.

Using big data and advanced analytics for comprehensive threat analysis

Big data and advanced analytics are also integral components of AI-driven detection. The sheer volume and diversity of data sources make it challenging to identify threats using traditional methods. AI-driven systems excel at handling big data, correlating information from various sources, and providing a comprehensive view of the security landscape. This integrated approach helps security teams to identify complex attack patterns and respond swiftly.

Benefits of AI-driven detection in comparison to traditional methods

While effective against familiar threats, traditional threat detection struggles when faced with rapidly evolving cyber threats, especially those using sophisticated tactics.

In contrast, AI-powered signature-based detection represents a huge shift in cybersecurity. Leveraging the prowess of artificial intelligence and machine learning, signature-based detection goes beyond the limitations of predefined signatures. It operates dynamically, analyzing vast datasets to identify subtle anomalies and patterns indicative of potential threats. By employing behavioral analysis and anomaly detection, platforms like Vectra AI adapt to the unique nuances of an organization's network, detecting both known and unknown threats with heightened accuracy.

AI-driven detection has several advantages over traditional methods, including:

Accuracy: AI-powered tools can be more accurate than traditional methods at identifying threats. This is because AI tools can learn from data over time and improve their performance without being explicitly programmed.

Speed: AI-powered tools can analyze large volumes of data very quickly. This allows SOC analysts to identify threats more quickly than traditional methods.

Scalability: AI-powered tools can be scaled to meet the needs of organizations of all sizes. This makes them a good option for organizations of all sizes.

Automated response and integrated signal: the future of cybersecurity

Integrated signal analysis is a critical component that empowers SOC teams to make informed decisions. By employing integrated signal and automated response technology, SOC teams can effectively identify and respond to security incidents with actions like blocking suspicious network traffic, quarantining compromised devices, or escalating incidents for human intervention. The goal is to reduce response times, minimize damage, and alleviate the burden on human analysts.

Incident response automation using AI and machine learning

AI and machine learning are the driving forces behind incident response automation. These technologies enable security systems to recognize patterns, anomalies, and deviations from the norm. By analyzing vast amounts of data in real-time, AI can identify potential threats, assess their severity, and respond accordingly. Machine learning models continuously improve their accuracy over time, making automated response mechanisms more reliable.

Hybrid SOC upgrade

Setting up a successful hybrid/co-managed SOC

Once your team is excited about upgrading their threat detection with the power of AI and integrated signal, it's time to consider the hybrid SOC model. The hybrid SOC model is built on the principle of collaboration. It combines the strengths of an in-house security team with the specialized knowledge and resources of external security experts. This partnership provides a comprehensive approach to cybersecurity, allowing businesses to benefit from both internal knowledge of their environment and external insights into emerging threats and best practices.

Co-managed security services: advantages and potential risks

Co-managed security services are a key component of the hybrid SOC model. They have numerous advantages, including:

24/7 monitoring: Co-managed services provide around-the-clock monitoring of an organization's security landscape, helping to identify and respond to threats promptly.

Specialized expertise: External security providers bring specialized skills and knowledge that may not be available in-house, enhancing an organization's security posture.

Scalability: Co-managed services can adapt to an organization's changing security needs, making it a cost-effective solution.

However, potential risks include the constant need for clear communication and collaboration between the internal and external teams, as well as the challenge of finding the right external partner with the right expertise.

Collaborative incident handling

Collaboration is at the core of the Hybrid SOC model. When a security incident occurs, both internal and external teams need to work in concert to address threats. This collaborative approach ensures a swift and effective response, minimizing the impact of the incident. Effective communication and clearly defined roles and responsibilities are crucial for successful collaboration.

Best practices for setting up a successful hybrid/co-managed SOC

Setting up a successful hybrid or co-managed SOC requires careful planning and execution. Here are some best practices for your team:

Clearly defined roles: Define the roles and responsibilities of both internal and external teams, ensuring that each party knows its specific tasks in incident handling.

Regular training and knowledge sharing: Foster a culture of continuous learning and knowledge sharing between in-house and external teams to keep everyone updated on the latest threats and best practices.

Integration of tools: Ensure that the tools and technologies used by both teams are integrated, allowing for seamless information sharing and collaborative response.

Communication protocol: Establish a clear and efficient communication protocol for incident reporting and response coordination.

Regular evaluation and improvement: Periodically evaluate the performance of the hybrid or co-managed SOC and make necessary improvements to continue improving efficiency and effectiveness.

Understanding hybrid managed detection and response

The constructive collaboration of in-house expertise and external security services in a hybrid SOC offers heightened awareness and response capabilities. As you discover the advantages of this collaborative model, it's important to consider the transformative power of Managed Detection and Response (MDR). While a hybrid SOC lays the foundation for comprehensive defense, MDR injects a dynamic layer of vigilance, introducing proactive threat detection, swift response mechanisms, and the ability to glean insights from a wealth of external threat intelligence.

MDR is a popular hybrid solution because it provides organizations access to a team of security experts who use AI-powered tools to monitor and protect their networks. MDR providers can help organizations:

- Implement and manage AI-powered tools.
- Augment their in-house security team to address analyst shortages.
- Improve their security posture and reduce risk.

4 keys to choosing the right MDR upgrade

1. **Assess your current environment.**

   Start by conducting a comprehensive assessment of your current security environment. Identify the strengths and weaknesses of your existing tools and processes. This evaluation will serve as the foundation for your transition strategy.

2. **Define your objectives and requirements.**

   Be sure to clearly define your security objectives and requirements. What are your specific threat detection and response needs? This will guide you in selecting the right MDR provider and technology stack.

3. **Choose the right MDR provider.**

   Selecting a reputable MDR provider is a critical decision. SOC leaders should look for providers with a track record of success, a strong focus on AI and machine learning, and the ability to understand your organization's unique needs.

4. **Prioritize training and workforce development.**

   Invest in training your team to effectively work with AI-based MDR solutions. This will empower your workforce to leverage the technology to its full potential.

While transitioning to a Hybrid SOC model with an MDR solution offers numerous benefits, it's not without its challenges. Teams should be aware of the following considerations:

1. **Total cost**

   Implementing MDR services, particularly with AI-driven capabilities, can be a substantial financial investment. It's essential to weigh the cost against the potential risks and losses associated with security breaches.

2. **Integration complexity**

   Integrating AI-based MDR solutions with legacy tools can be complex. Compatibility issues, data migration, and ensuring a seamless transition can pose significant challenges.

3. **Potential skills gap**

   Leveraging AI in security operations requires a workforce with a strong understanding of AI and its applications in cybersecurity. Bridging the skills gap within your team is essential.

4. **Data privacy and compliance**

   AI-driven MDR solutions often deal with sensitive data. Ensuring data privacy and compliance with regulations like GDPR and HIPAA is a significant concern throughout the transition.

Co-managed security services bring specialized skills and resources to the table, while collaboration between internal and external teams ensures a well-rounded approach to incident handling and response. By maintaining clear communication, organizations can set up a successful hybrid or co-managed SOC, reducing the stress on internal teams and improving total threat visibility.

Identity-centric SOC Upgrade

Identity-based attacks are becoming increasingly common. In fact, a recent report by One Identity found that 89% of organizations were affected by an identity-based attack in 2022, and more than half of the organizations involved lost more than 10,000 identities. In these attacks, attackers target user credentials to gain access to sensitive data and systems. Some of the most common types of identity-based attacks include:

Phishing: Attackers send fraudulent emails or text messages that trick users into revealing their credentials.

Password spraying: Attackers try to guess common passwords or use brute force attacks to crack weak passwords.

Pass-the-hash: Attackers steal user credentials and use them to gain access to other systems on the network.

Man-in-the-middle (MITM): Attackers intercept communication between two parties and impersonate one of the parties. MITM attacks can be used to steal sensitive information, such as usernames, passwords, and credit card numbers.

Today attackers are also using new and more sophisticated tools to carry out these identity-based attacks, including:

Generating personalized phishing emails: AI can be used to generate personalized phishing emails that are more likely to trick users into revealing their credentials. For example, AI can be used to generate emails that appear to be from a legitimate source, such as the user's bank or employer. AI can also be used to generate emails that are tailored to the user's interests, making them more likely to click on malicious links or attachments.

Automating password-guessing attacks: AI can be used to automate password guessing attacks, making them more efficient and effective. For example, AI can be used to generate lists of potential passwords based on common patterns or to use brute force attacks to try every possible password.

Detecting and exploiting vulnerabilities in authentication protocols: AI can be used to detect and exploit vulnerabilities in authentication protocols, such as Kerberos. For example, AI can be used to identify weak Kerberos tickets or to create malicious Kerberos tickets that can be used to gain access to user accounts and systems.

Identifying and targeting high-value targets: AI can be used to identify and target high-value targets, such as executives or employees with access to sensitive data. For example, AI can be used to analyze social media data or employee records to identify potential targets.

How integrated signal helps SOC teams

AI, with its ability to decipher patterns, anomalies, and potential threats within vast datasets, logically integrates with signal analysis to provide a unified, real-time view of an organization's security posture. This union not only enhances the efficiency and accuracy of threat detection but also empowers SOC teams to navigate the ever-changing threat landscape with agility and precision.

Integrated signal analysis is vital for ensuring the efficacy of automated response mechanisms. By providing SOC teams with a unified view of security alerts and data, integrated signal analysis helps analysts make informed decisions, quickly. It quickly and easily combines information from various sources, resulting in a comprehensive threat intelligence picture that enables highly effective incident response.

Human-first SOC upgrade

SOC analysts are under a lot of pressure. They are expected to monitor and protect complex networks from a wide range of threats (an average of 4,484 alerts per day according to our State of Threat Detection report), and any missed alert or minor mistake has a massive impact. The same report found that more than half (55%) of analysts claim they're so busy they feel like they're doing the work of multiple people. Analysts mentioned spending too much time sifting through poor-quality alerts (39%), working long hours, and feeling "mind-numbingly" bored in the role (32%). More than one-third of respondents also cited constant workplace stress (35%), burnout (34%), and the role's impact on their mental health (32%) as ongoing stressors.

As threats continue to evolve and attackers continue to advance their tactics, analysts are responding to most threats tired, uninspired, and overworked. This sentiment was echoed in Tines Voice of the SOC report, where 63% of practitioners stated they experienced some level of burnout, with more than 80% saying their workloads have increased in the past year. It's clear that the problem is only getting worse, and upgrading is the key to providing SOC teams with the support they need to keep up, without burning out. But how?

AI and tech upgrades can help to dramatically reduce analyst burnout by automating tasks and reducing noise. This allows analysts to focus on the most critical issues and to make more informed decisions when it matters most. By transitioning to a hybrid solution that combines legacy tools with AI-powered tools, organizations can improve their security posture, reduce risk, and reduce overall analyst exhaustion simultaneously.

Challenges and considerations for deploying automated response in SOC

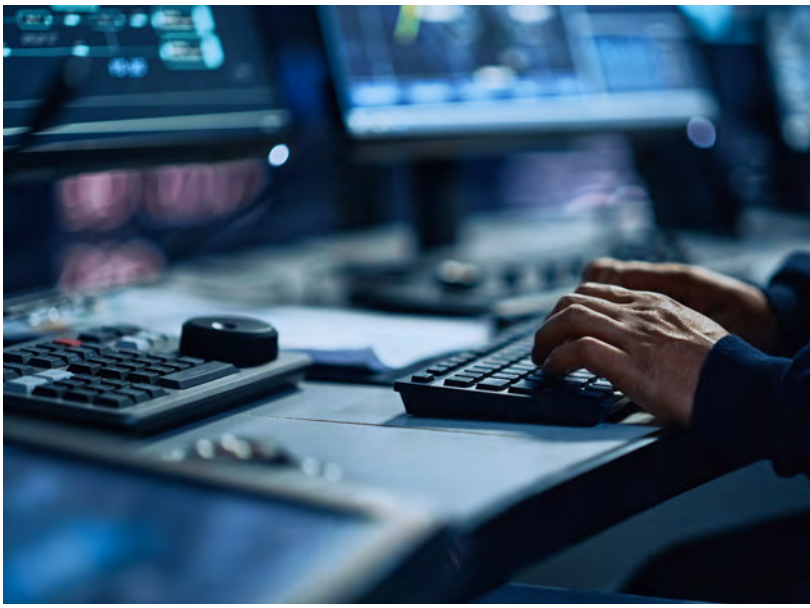
While deploying automated response mechanisms will reduce the burden on your SOC team, it has its own challenges to keep in mind for the analysts monitoring it:

False positives: Striking the right balance between security and operational efficiency to minimize false positives is a continual challenge for SOC teams. It's important to know which alerts to prioritize, so your team can determine which alerts can be safely off-loaded through automated response.

Regulatory compliance: Ensuring that automated responses comply with industry and regional regulations is crucial. Organizations seeking SOC2 compliance pay special attention to which business operations items can and cannot be automated.

Human oversight: Automated responses should be designed to include human intervention when needed, especially in complex situations. Even the most fine-tuned algorithm is merely following instructions. Teams should be prepared to set parameters for escalating important items back into human hands and keyboards.

Evolving threats: The automated system must adapt to evolving threats to remain effective.



Ensuring accuracy and reliability in automated response mechanisms

Accuracy and reliability are paramount in automated response mechanisms. False positives can disrupt legitimate operations, while false negatives can allow threats to go undetected. To address these concerns, automated response systems must be finely tuned and regularly updated. They should also incorporate human oversight to ensure that critical decisions are not made solely by algorithms.

You can see an example of how AI can work seamlessly alongside SOC teams to prioritize threats in this hybrid cloud attack simulation. Vectra AI's Attack Signal Intelligence™ detected and prioritized:

- HTTPS Hidden Tunnel
- HTTPS Tunnel, Port Scan, Port Sweep, Suspicious LDAP, RPC Recon
- Suspicious Remote Execution
- Privilege Anomaly: Unusual Account on Host
- Azure AD Suspicious Sign-on
- M365 Suspicious Email Rule
- Azure AD Risky OAuth Application
- AWS sign-in
- AWS Organization Discovery
- AWS User Permission Enumeration

With an accurate timestamp of the incident and clear threat detections, the analyst was able to catch up to the attacker in real-time, quickly disable the infected account, and lock down the host.

This is just one example where AI offers hope by not only alleviating the burden on SOC professionals but also revolutionizing the efficiency and efficacy of threat detection and response processes. Together, AI-driven threat detection and SOC teams can move toward a fully upgraded and resilient SOC.

Section 3. Completing a SOC Upgrade

Understanding XDR

XDR, or Extended Detection and Response, is a security solution that integrates data from multiple security layers, such as networks, endpoints, and cloud environments, to provide a holistic view of the threat landscape. XDR uses AI and machine learning to correlate data and identify threats that would be difficult or impossible to detect with traditional security solutions.

XDR's role in upgraded cybersecurity

With the help of machine learning algorithms, XDR can consolidate and correlate data from diverse security layers in real time. XDR goes beyond the limitations of traditional security tools to integrate and unify data from various security products, providing a clearer view of the overall security picture. XDR can also help organizations reduce the number of security tools they need to manage, which can lead to significant cost savings year over year.

1. Leveraging AI in XDR to reduce your team's workload

AI and machine learning are essential components of XDR. AI is used to consolidate and correlate data from multiple security layers and identify patterns and disturbances that may indicate an attack. XDR also uses AI to automate tasks such as threat hunting and incident response. AI-driven XDR is unique as it continuously refines its models, improving detection accuracy and reducing false positives and negatives.

2. MDR for shared workload

MDR plays a crucial role in distributing and managing the workload effectively. MDR services enable organizations to collaborate with external security experts, sharing the responsibility of threat detection and response. This collaborative approach ensures that the SOC has access to a broader pool of expertise, enhancing its overall capabilities in handling diverse and evolving cyber threats.

3. Identity-centric workflow shifts

XDR goes beyond traditional threat detection by incorporating an identity-centric approach. Shifting the workflow to focus on identity enables organizations to detect and respond to threats that are often invisible to conventional methods. By monitoring user behaviors, access patterns, and authentication activities, XDR with an identity-centric approach provides a holistic view of potential threats, including those arising from compromised credentials and insider threats.

4. Optimized analyst experience for maximum talent utilization

The human element remains irreplaceable in cybersecurity, and an XDR solution should be designed to maximize the talent of SOC analysts. A streamlined and user-friendly interface, coupled with advanced visualization tools, enhances the analyst experience. This optimization not only improves the efficiency of the analysis process but also contributes to better decision-making in the face of cyber incidents.

XDR is a comprehensive strategy that goes beyond traditional threat detection methods. By incorporating AI, MDR, an identity-centric approach, and an optimized analyst experience, organizations can effectively upgrade their SOC to face the barrage of emerging attacks. As cyber threats continue to evolve, the implementation of XDR is not just a choice; it is an imperative strategy for fortifying cybersecurity defenses.

Benefits of using XDR in SOC operations

XDR has numerous benefits for SOC teams, including:

- Improved visibility of the threat landscape
- Reduced alert fatigue
- Faster and more effective threat detection and response
- Reduced costs

XDR not only streamlines security processes but also empowers analysts to stay ahead of evolving threats. As the cyber threat landscape continues to evolve, XDR offers a vital evolution in the arsenal of cybersecurity, providing organizations with a proactive and resilient defense against digital threats.

Enhancing security information and event management (SIEM) through AI

Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms are at the forefront of the defender's battle. By harnessing the power of Artificial Intelligence (AI), these tools are not only enhancing security measures but also revolutionizing threat detection and response. AI can be used to enhance current SIEM solutions for SOC teams. For example, AI can be used to:

- Correlate data from multiple sources more effectively
- Automate tasks such as log analysis and incident triage
- Identify and prioritize threats more accurately
- And more

When used strategically, AI can help your team optimize their workload, and offload time-consuming tasks as determined by your team's unique skills and priorities.

AI-driven security orchestration, automation, and response (SOAR) platforms

AI-driven SOAR platforms can help your team automate a number of security tasks, including incident response, threat hunting, and remediation. SOAR platforms are designed to streamline and automate incident response processes. AI-driven SOAR platforms enhance these capabilities by introducing automation, orchestration, and response mechanisms that adapt to evolving threats. Machine learning algorithms enable these platforms to identify and categorize threats more effectively, ensuring a rapid and coordinated response to security incidents. Integrating AI-powered analysis with SIEM/SOAR systems can help organizations drastically upgrade their threat-hunting capabilities.

Scalability and flexibility of AI-optimized SIEM/SOAR systems

AI-optimized SIEM/SOAR systems are designed to be scalable and flexible. These systems can adapt to the needs of organizations of all sizes, from small businesses to large enterprises. Their ability to process and analyze vast datasets makes them highly effective in many different environments, and they can be tailored to the specific requirements of each organization. This flexibility ensures that AI-enhanced SIEM and SOAR systems can grow and evolve as needed.

Upgrading with a SIEM-less SOC

A SIEM-less SOC is a security operations center that does not rely on a traditional SIEM solution. Instead, SIEM-less SOCs use a variety of other security tools, like EDR and XDR, to collect and analyze data.

Some advantages of using a SIEM-less SOC include:

- Reduced costs
- Increased flexibility
- Improved performance

However, it is important to note that SIEM-less SOCs require a high level of expertise and experience.

Other challenges to consider include:

Integration complexity: Implementing a SIEM-less SOC can be technically complex, as it often involves integrating various security tools and solutions to ensure comprehensive coverage.

Data overload: Without the structured data management capabilities of a SIEM, SIEM-less SOC models may struggle to effectively handle and analyze large volumes of security data.

Team skills gap: A SIEM-less approach may require a distinct set of skills and expertise, which can be a challenge for organizations that need to adapt their workforce accordingly.

While traditional SIEM solutions still have their place in certain contexts, SIEM-less offers increased adaptability and cost-efficiency. However, successfully implementing a SIEM-less SOC requires careful planning, integration, and ensuring your team has the relevant skills to navigate the potential challenges effectively.

What to expect post-upgrade

Once you've outfitted your team with the right tools, techniques, and training to complete a full SOC upgrade, you can look forward to a slew of benefits.

Say goodbye to silos

Organizational silos in cybersecurity hinder information sharing and collaboration, limiting the ability to effectively detect and respond to threats as a team. This is especially harmful when you consider the way hybrid attackers move quickly, exploiting a segmented security posture and using it as one giant playground. Identifying and addressing silos is the first step in breaking them down. Often, silos are a result of departmental boundaries, communication gaps, or different tools and processes used by various security teams.

An upgraded SOC acts as the antidote to silos. It breaks down the barriers that prevent different security teams from working together. Integrated tools foster a comprehensive understanding of the threat landscape, allowing teams to respond more effectively to security incidents, together. For example, the network security team can collaborate with the endpoint security team to correlate data and detect threats across the entire environment. This cooperative approach helps in building a more resilient defense.

AI's role facilitates information sharing and communication

AI also plays a pivotal role in breaking down silos and facilitating information sharing. Machine learning algorithms can analyze and correlate data from various security layers and share insights across departments, enhancing situational awareness and response capabilities.

A unified ecosystem connects the various security components, tools, and technologies, allowing them to work seamlessly together. It integrates processes and data to provide a holistic view for everyone involved in security at your organization. This unified approach enhances resiliency, streamlines incident response, and minimizes business disruptions.

Improving efficiency through integrated signal

In the upgraded SOC, security professionals no longer feel overwhelmed by a deluge of signals from various security tools and data sources. With the help of signal integration, data is no longer fragmented and difficult to analyze effectively. Integration creates a unified view of the security landscape for your SOC team. And with machine learning algorithms in place, AI can correlate and analyze signals from various sources, providing comprehensive threat intelligence. This not only reduces the workload on your security analysts but also improves the overall accuracy of detection.

Utilizing integrated signal for proactive threat hunting

Integrated signals help your SOC team hunt for threats proactively. Rather than simply responding to alerts, they can actively search for signs of compromise, reducing the risk of undetected threats that could lead to data breaches or system disruptions. To magnify the

effect of integrated signals, a centralized platform for managing them is essential. One unified single source of truth provides a single pane of glass view, streamlining the monitoring and response process. This unified approach will help your team react faster and feel less overwhelmed by multiple tools and items to monitor.

Total talent optimization and improved analyst experience

The shortage of skilled cybersecurity professionals is a well-known challenge. Attracting and retaining talent is a constant struggle for organizations, and the gap is widening as the threat landscape continues to evolve. Fortunately, upgrading your SOC, in combination with AI-driven solutions, can help overcome these challenges.

Upskilling the workforce and augmenting human capabilities with AI

AI is a powerful ally in talent optimization within the SOC. It can automate routine tasks, allowing human analysts to focus on more complex and strategic activities. This automation not only enhances the efficiency of general SOC operations but also reduces the workload on human analysts, preventing burnout and attrition.

As organizations embrace AI-driven solutions, upskilling the workforce is a necessity. Training programs can help cybersecurity professionals become proficient in utilizing AI tools and technologies that will, in turn, make their jobs easier. By upskilling the workforce, organizations ensure that their teams are well-prepared to operate effectively in an upgraded, AI-driven SOC environment. In fact, Tines Voice of the SOC report found that 93% of respondents believe that more automation would improve their work-life balance.

Section 4: Key Takeaways:

In summary, embarking on a SOC upgrade is a vital evolution in ensuring organizational resilience against evolving cyber threats. By breaking down silos, integrating signals, and optimizing talent, businesses can build a more effective and efficient security infrastructure. AI is the linchpin in this transformation, facilitating communication, analysis, and optimization across all these aspects, making it your ally in the ongoing battle for cybersecurity.

Balancing the benefits of SOC modernization with the well-being of analysts is paramount. While AI-driven detection, automation, and XDR enhance efficiency, they must be deployed with a keen eye on the mental and emotional health of the defenders who safeguard our digital environments. By addressing analyst burnout as an integral part of SOC modernization, organizations can ensure the long-term effectiveness of their cybersecurity operations while maintaining a healthy and motivated workforce.

Take the next step toward upgrading your SOC

About Vectra AI

Vectra AI is the leader in hybrid attack detection, investigation and response. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Vectra AI's patented Attack Signal Intelligence empowers security teams to rapidly detect, prioritize, investigate and stop the most advanced hybrid cyber-attacks. With 35 patents in AI-driven detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai