White Paper: Amplify Visibility and Unlock Your SOC

ANOMALI

Introduction

Security Operations Centers (SOC) are the nerve center of cybersecurity defense. The results of both tactical and strategic security initiatives are manifested, tracked, and managed at the operational level, and the visualization of that level is the SOC. In spite of the critical role they play, SOCs and the people who work there are under tremendous pressure; potential security events are growing exponentially, separating signal from noise is an increasing challenge, analysts are asked to do more with less and are tasked with taking on adversaries who are not constrained by rules of engagement.

While SOCs are at an inflection point, their supporting technology infrastructure is also evolving at a rapid pace to support automation, integration, correlation, and streamlining. Automating and providing better visibility into a Security Operations Center is absolutely mission-critical for effective cyber security.

SECURITY ANALYTICS

With Anomali you can run real-time queries against a significantly larger (historical) data set - scan petabytes of data in seconds - to build more sophisticated and actionable threat models across your entire security telemetry, mapped to your external threat environment. This correlation creates significantly faster threat detection, more proactive threat hunting, and improved incident response and mitigation capabilities.

Enhanced Threat Detection

AI-driven security analytics leverages machine learning algorithms and anomaly detection techniques to quickly identify sophisticated threats that may go unnoticed by traditional security controls. By analyzing vast amounts of internal security data, including logs, network traffic, network security events, and endpoint behavior against external threat intelligence in real time, Anomali Security Analytics can identify patterns, correlations, and IOCs that point to malicious activity. This enhances the SOC's ability to detect known and unknown threats in real time, reducing dwell time and improving overall threat detection capabilities, mitigating risks and preventing further damage. We're talking minutes, not days or weeks.

Automated Incident Response

Through the use of Anomali Security Analytics, SOC staff can enable automated incident response, significantly reducing errors associated with manual effort. By defining playbooks and response workflows, Anomali can automate routine tasks such as containment, isolation, and remediation of security incidents. By working with real-time insights into attack vectors, compromised systems, and attacker behavior, SOC teams are enabled to implement appropriate actions, isolate affected systems, and mitigate further damage. The use of real-time data also minimizes the risk of data loss or tampering, ensuring the accuracy and integrity of investigative findings. This not only accelerates incident response and analysis, it also frees up analysts' time to focus on more complex investigations and strategic activities.

Continuous Monitoring, Analysis, and Compliance

Anomali provides continuous monitoring capabilities, allowing SOC teams to capture and analyze security events in real time. By correlating to historical data, Anomali can quickly uncover the potential scope and impact of security incidents, giving SOC analysts a real-time understanding of emerging threats and enabling the implementation of measures to prevent similar incidents in the future. By aggregating and analyzing network telemetry data over time, SOC teams can detect patterns in the attack chain, identify changes in network behavior, and uncover potential security weaknesses. In addition, real-time monitoring supports the ongoing management of security controls and compliance requirements. SOC teams can ensure that security policies, configurations, and access controls are consistently enforced and meet regulatory obligations. Continuous, real-time visibility helps identify compliance gaps and potential policy violations and enables them to be addressed promptly.

PROACTIVE THREAT HUNTING

Security analytics accelerates proactive threat-hunting within the SOC. Leveraging AI-driven analysis, SOC analysts can search for hidden or emerging threats by quickly identifying unusual behaviors, and uncovering attack patterns that may not be apparent through standard monitoring. Proactive threat hunting helps identify and mitigate potential threats before they cause significant damage, strengthening the organization's security posture.

Threat Intelligence Integrations

Anomali integrates with public (OSINT) and curated threat intelligence feeds to enhance threat detection and prioritize responses. By correlating internal security telemetry with external threat intelligence such as known malware signatures, malicious IP addresses, or IOCs, Anomali enables operations teams to identify and prioritize evolving threats based on TTPs (tactics, techniques, and procedures), relevance, and severity, to hunt for threats that align against specific profiles or indicators associated with known threat actors. This integration also strengthens the SOC's ability to immediately implement effective countermeasures and ensure a proactive defense posture, with the final output providing valuable insights for risk management and strategic planning.

Forensic Analysis and Investigation

Improved SOC performance includes a robust post-incident analysis process to identify the root causes, lessons learned, and areas for improvement. Through post-incident root cause analysis, the SOC team can reconstruct the sequence of events, trace the source of the attack, and understand the TTPs employed by threat actors to uncover hidden threats, persistent attack patterns, or attack vectors that were not initially detected. The knowledge gained from incident analysis loops back into the threat-hunting process, allowing analysts to quickly and efficiently search for similar attack patterns or indicators across the environment.

WORKFLOW AUTOMATION

Automate intelligence workflows to ingest, enrich, score, share and distribute intel, automating routine analyst tasks and reducing human errors and its associated stress. Workflow automation can streamline processes, enhance analyst efficiency and drive a faster response to security incidents, including:

Ticketing and Case Management

Workflow automation tools integrate with ticketing and case management systems to facilitate seamless incident tracking and collaboration. Automated ticket generation ensures that every incident is properly documented, assigned, and tracked through its lifecycle. This enables efficient communication and collaboration among SOC analysts, allowing them to work together on resolving incidents and sharing relevant information.

Playbook Execution

Automation enables the execution of predefined playbooks or response workflows for common security incidents. Playbooks outline step-by-step procedures for incident response, including containment, investigation, and remediation activities. By automating playbook execution, SOC analysts can eliminate manual and repetitive tasks, ensuring consistent and timely incident response.

Reporting and Metrics Generation

Workflow automation simplifies the generation of reports and metrics related to SOC performance. By automating data collection and analysis, SOC teams can generate accurate and timely reports on incident trends, response times, resolution rates, and other key metrics. These reports provide valuable insights for management, compliance, and continuous improvement of SOC operations.

Compliance and Audit Trail

Automation tools help maintain a comprehensive audit trail of SOC activities, ensuring compliance with regulatory requirements and providing evidence for internal or external audits. Automated workflows document actions taken, decisions made, and changes implemented during incident response, ensuring transparency and accountability.

COLLABORATION AND KNOWLEDGE SHARING

Automate intelligence workflows to ingest, enrich, score, share and distribute intel, automating routine analyst tasks and reducing human errors and its associated stress. Workflow automation can streamline processes, enhance analyst efficiency and drive a faster response to security incidents, including:

Collective Expertise

Collaboration brings together the collective expertise and diverse perspectives of SOC analysts. By encouraging collaboration, teams can leverage the knowledge, skills, and expertise of individual analysts to solve complex problems, investigate incidents, and make informed decisions. This collective expertise enhances the overall effectiveness of the SOC and enables analysts to tackle challenges more efficiently. This is particularly the case with collaboration across communities via entities such as ISACs (information sharing and analysis centers).

Cross-Functional Collaboration

Collaboration promotes cross-functional integration within the SOC and with other teams in the organization. By working closely with other departments such as IT, network operations, or application development teams, SOC analysts can gain a broader understanding of the organization's systems, infrastructure, requirements, and vulnerabilities. This cross-functional collaboration enables better threat identification, proactive risk mitigation, and more effective incident response.

Knowledge-Sharing Platforms

Establishing knowledge-sharing platforms, such as wikis, internal forums, or chat channels, encourages the sharing of information, best practices, and lessons learned within the SOC. Analysts can document incident analysis techniques, emerging threats, or effective response strategies, making this knowledge readily available to the entire team. These platforms serve as a centralized knowledge repository, fostering continuous learning and enabling analysts to quickly access relevant information.

Continuous Learning and Skill Development

Collaboration and knowledge sharing support continuous learning and skill development within the SOC. By sharing knowledge techniques and resources, analysts can expand their skill sets, stay abreast of the latest security trends, and develop new capabilities. This continuous learning culture strengthens the SOC's capabilities, fosters innovation, and empowers analysts to tackle complex security challenges more effectively.

Automation and Tooling Insights

Collaboration allows for the sharing of insights and experiences related to automation tools, security platforms, and other technologies used in the SOC. Analysts can exchange information about tool configurations, use cases, and automation scripts, enabling the optimization of SOC tools. This knowledge-sharing enhances the SOC's technical capabilities, streamlines operations, and improves overall efficiency.

Conclusion

There is a wide and evolving range of challenges facing every security operations center, both from an internal and external perspective, but the right solutions and platforms, backed by the right policies and procedures can comfortably take your security operations center to the next level. To gain a real-world perspective on how Anomali's Security Operations Platform can help you immediately gain actionable insights into your security challenges, please contact us here.

info@anomali.com | www.anomali.com

808 Winslow St., Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI