What are SOAR Tools?

The IT security and threat mitigation niche is known for the tens of acronyms professionals use to speak about the diverse security tools used within the industry. SOAR is one such acronym and for the many coming across it for the first time, SOAR means security orchestration, automation and response. SOAR Tools are the technologies used to orchestrate responses to security incidents and assign responsibilities between various tools and individuals within a security team or enterprise. SOAR technology automates the orchestration process through "playbooks" which simplifies the task of responding to complex security issues.

The working principles of a best-in-class SOAR technology simplify and improves IT security operations in diverse ways including:

- Through a combination of security orchestration, and automation solutions which automates incident response and threat investigation processes.
- The provision of an interactive centralized dashboard to simplify the security management process for security teams and non-technical staff.
- Simplifying case management and efficient response to security incidents through the use of a priority ticketing system.

SOAR Use Cases for Enterprises

Enterprises who rely on SOAR technology to secure enterprise networks do so for a variety of reasons and apply SOAR solutions for diverse use cases. These use cases generally differ according to the experience levels of the security team working within an organization. The major use cases for deploying SOAR include:

Managing Security Operations – As a security operations manager, SOAR technologies handle multiple tasks such as vulnerability management, security certificate management, endpoint diagnostics, and reporting activities. The broad range of management services SOAR offers means enterprises with varying security capacities can deploy SOAR for security management operations.

For example, an enterprise with a dedicated, experienced security team can rely on SOAR to send timely reminders on expiring security certificates so the appropriate individual can handle that

task. While for enterprises with limited security operating centers, SOAR can serve as a comprehensive tool for managing vulnerabilities and dealing with security incidents through automation. In both scenarios or use cases, SOAR is applied in a limited capacity in the first example and as a comprehensive security system in the latter.

Threat Hunting and Incident Response – The process of threat hunting has been elevated from simply discovering threats to gaining insight into threat complexities using machine learning and other pattern recognition solutions. SOAR provides the tools for automating the threat hunting, analysis, and response processes for enterprises regardless of the experience levels of their security teams.

Use cases for experienced security teams revolve around gaining contextual insight into indicators of compromise captured across diverse threat hunting technologies. Security teams also rely on SOAR technology to analyze big data sets from expansive enterprise infrastructures as they can extract and analyze data from both cloud-based and on-premise IT assets.

Use cases for enterprises with limited security capacity focus on taking advantage of the orchestration and automation capabilities of a SOAR technology or solution. Enterprises under this category rely on automation to discover threats and to determine the response required to mitigate discovered threats. These enterprises also rely heavily on comprehensive dashboards and playbooks to understand the nature of threats, their targets, and the severity of a security incident.

Automating Enterprise Security – Automation and the option to rely on superior analytical powers SOAR provides is a major reason why enterprises choose to make use of a SOAR solution. Due to the always-changing nature of IT security and the threats cyber criminals deploy, relying on the automated support SOAR provides to discover new threats are reasons why security teams deploy SOAR technology.

The Benefits of Having SOAR and why Your Organizations Should Use It

The working principles and use cases highlighted here all speak about the benefits of integrating SOAR technologies within your organization's IT infrastructure but other important factors also exist. These benefits include:

- **Automating Repetitive Tasks** – According to Gartner, human error in the workplace is responsible for 95% of security incidents in cloud environments. This high failure rate is

due to repetitive manual tasks which provide various avenues for negligence. The automation SOAR provides ensures threat investigations and responses are performed at a much faster rate and in a scalable way across complex or expansive IT infrastructure.

- **AI Enables New Security Initiatives to Protect Digital Infrastructure –** The integration of machine learning in SOAR solutions enables the technology to dive deep into threats, analyze them, and gain contextual knowledge of their capabilities. The insight SOAR provides serves as the foundation for fine-tuning incident response strategies to improve overall IT security.
- **Orchestrate Security Incidents to Capable Hands –** SOAR technology automates the orchestration process and routes security incidents to the analyst or expert within a team with the best credentials to handle a particular incident. Thus, flooding security teams with large data sets is eliminated as SOAR ensures teams get only the essential information needed to take action.

Interested in Protecting Your IT Infrastructure with SOAR?

If you're reading this, your security operations center is either overwhelmed with thousands of alerts or inadequate to deal with today's complex security landscape. You can learn more about how SOAR can help with securing your businesses peculiar IT infrastructure by speaking with an expert security analyst from DataShield today.