MAXIMISING SOAR IN SOC ENVIRONMENTS

CREST

Contents

Introduction

The Security Orchestration, Automation, and Response (SOAR) framework revolutionises security operations by enabling teams to seamlessly orchestrate, automate and respond to security incidents. In today's rapidly evolving threat landscape, SOAR technology also plays a pivotal role in enhancing the efficiency and effectiveness of Security Operations Centres (SOCs). This white paper delves into the significance of SOAR in SOC environments, its benefits, challenges and strategies for successful implementation. What does SOAR do?

- **Orchestrate:** This involves the integration and co-ordination of various security tools and systems to automate workflows and processes. It ensures that different security technologies work together seamlessly.
- **Automate:** Helps automate repetitive and manual security tasks such as alert triage, incident response, and threat hunting. Automation helps reduce the workload on security teams and speeds up response times. Automating the manual playbooks.
- **Respond:** This refers to the actions taken to respond to security incidents, including containment, eradication, and recovery.

For example, in a typical SOC operation, all incidents are mostly investigated manually, within the functions of the tools themselves, in most cases a SIEM or XDR or both. An example of a typical common alarm would be investigation on a malicious IP. An analyst would probably have to check with multiple reputational intelligence sources to determine if it's truly malicious and plan for the next step of action, eg. to block the IP on multiple firewalls or IPS systems and the flood of these alarms usually causes fatigue and time to investigate. With a SOAR, in this kind of incident these individual actions can be automated to reduce the time taken to investigate and respond.

SOAR in SOC:
Streamlining Security Operations

In recent years, there has been a shift towards more organisations adapting the traditional SIEM with Endpoint Detection and Response (EDR) and Network Detection and Response (NDR) to create an Extended Detection and Response (XDR) solution and cloud-based security tools[1] within cloud environments. This brings multiple data into the SOC to ingest, investigate and respond to.

As cyber security technology vendors also advance, such as EDR (Endpoint Detection and Response) providers transitioning to XDR (Extended Detection and Response) and SIEM (Security Information and Event Management) vendors incorporating NDR (Network Detection and Response) and UEBA (User and Entity Behaviour Analytics), there's an overlap of data being ingested by security analysts in the SOC. This information influx creates a surge of noise and false positives that must be addressed and fine-tuned through detection engineering to effectively investigate and prioritise incidents.

With SOAR, the SOC is supposed to ingest alerts from all these technologies within a single platform to triage and automate playbooks as much as they can - with minimal user intervention.

SOAR empowers security teams to streamline their operations by automating repetitive tasks and integrating with various security technologies. By automating mundane tasks, such as alert triaging and response, SOAR alleviates analyst fatigue and enables teams to focus on addressing critical threats.

[1] Such as the Cloud Network Access Security Platform (CNAPP) and the Cloud Workload Protection Platform (CWPP). CNAPP focuses on securing network access to cloud resources. CWPP protects workloads and applications running within those environments.

Challenges in SOAR Implementation

Despite its numerous benefits, implementing SOAR in SOC environments presents certain challenges.

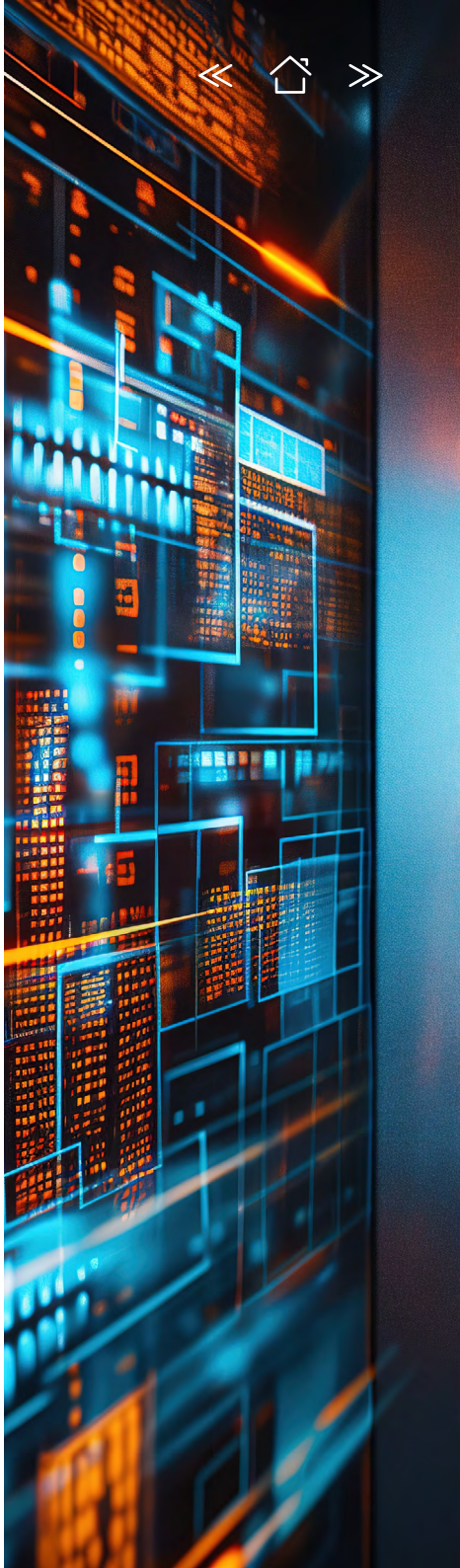
Perhaps the main issue is integrating SOAR with existing security technologies which may be complex and require the development of custom integrations or leveraging APIs. Whilst integrations are available for mainstream products, their capabilities vary between vendors and need to be reviewed to ensure more than just basic functions are included that might restrict or make automation tasks more complex.

API calls are not complete in some cases, and only have certain information sent to a SOAR platform. For example, an XDR solution may only allow certain information to be ingested to a SOAR which may not provide enough data for a playbook to give enough context to enable the creation of a response.

The shortage of skilled SOAR engineers and the need for dedicated resources to manage SOAR initiatives also poses significant challenges. Having a team of dedicated SOAR engineers to just work on SOAR may be costly.

When deploying and developing SOAR, a key consideration is value to the business. Value needs to consider: the effort saved versus the effort to develop and maintain; the risk of delay of containment to an infrequent incident; and getting the right information every time.

Aligning SOAR processes with existing SOC workflows and playbooks requires careful planning and coordination. Teams may have to change current playbooks to fit an existing process in a particular SOAR platform.



Starting the SOAR Journey: Best Practices

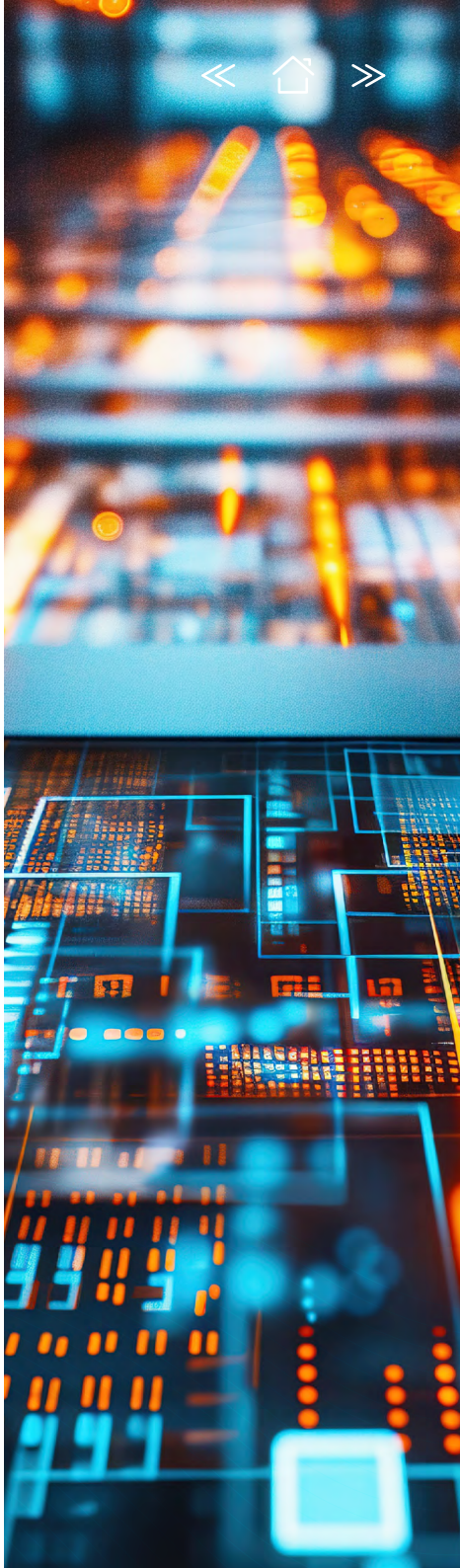
To embark on a successful SOAR journey, organisations should start with a clear understanding of their objectives and pain points.

You should:

- Already have well developed incident response plans
- Prioritise automation of repetitive tasks and streamline investigation playbooks so they can be automated, maximising efficiency
- Establish a dedicated team led by a champion to drive the automation project forward

The most suitable team to work on automation is the security engineering team. They will have to work closely with the SOC team to plan and identify what to automate first and build a roadmap for improvements.

- Collaborate closely with the SOC and security engineering teams to identify automation opportunities and develop a roadmap for continuous improvement.



Success outcomes with SOAR

The adoption of SOAR yields tangible benefits for SOC operations.

By automating repetitive tasks and level 1 activities, typically the basic triage and context enrichment for incidents, a clear benefit is that SOAR reduces analyst fatigue and enables teams to focus more on critical threats.

With automation in place, analysts can now focus only on alerts that really need attention and respond to them.

As SOC analysts focus on real investigations rather than time-consuming, repetitive activities, their development is enhanced meaning they can focus on other desired outcomes within the SOC, such as threat hunting, purple teaming and move more towards initiating an active defence approach for SOC operations.

The ability to automatically have response playbooks in place moves SOC operations to actually taking responses from a single platform instead of responding separately on separate tools, eg. investigating in a SIEM and responding to an EDR agent. With this, the Mean Time to Respond (MTTR) is greatly improved.

SOAR also enhances incident response capabilities, by enabling rapid response to security incidents from a single platform. This leads to improved MTTR – such as disabling users, blocking firewall IP's and other manual response tasks which may have been previously done by another team or completed manually – and enhanced security outcomes.

With a unified view of security operations, all tools are consolidated within a single SOAR console, whether it's an internal SOC or an MSSP supporting multiple environments. This consolidation ensures all data is ingested into one system, minimising the risk of overlooking security alerts. For MSSPs, this means they can create playbooks to execute actions across various devices and environments simultaneously. For instance, they can swiftly distribute Indicators of Compromise (IOCs) to multiple systems across different sites.

SOAR's common pitfalls

SOAR can provide enormous benefits, but often fails because a real strategy is not adopted that takes into consideration all security operations and engineering.

The common pitfalls for why SOAR projects fail include:

- Engineering-led and focus on technology, not the actual security operations;
- Focusing on End-to-End automation and not automation that delivers value (reduced response time, better contextual information, consistent information/response)
- The need for SOAR to be outcome based and not just focused on the technology capabilities because not everything within SOC operations can be automated.

Conclusion

Put simply, SOAR plays a pivotal role in enhancing the effectiveness of SOC operations.

By automating tasks, streamlining workflows and enabling rapid response to security incidents, SOAR empowers organisations to navigate the complexities of today's threat landscape more effectively. It reduces the complexity and fatigue to security analysts, improves SLA's and gives the SOC teams the ability to look for real threats and improve the outcome of security investigations and responses in a complex environment.

While challenges may arise during implementation, a strategic approach focused on collaboration, process optimisation and continuous improvement can maximise the potential of SOAR in SOC environments.
It should start simply and progress towards a level of maturity that demonstrates how automation can enhance the service outcomes of a SOC.


CREST