JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

SOAR Education Modules Briefing to the Centers of Excellence

February 5, 2020

Michael Vermilye
IACD Engagement Lead
JHUAPL

Topics

- What is SOAR?
- Why is it a crucial part of cybersecurity related education?
- Module A – From a Business Perspective
- Module B – Making use of SOAR – a Technical Perspective
- Lab Module – Getting your hands dirty
- Discussion

SOAR

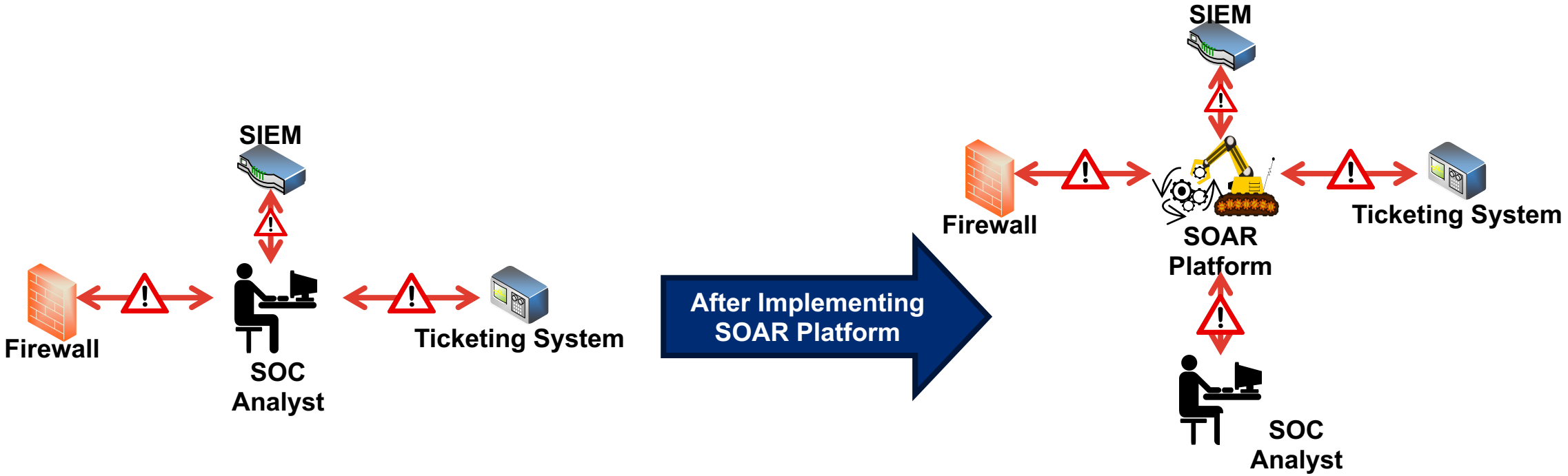
SOAR is a combination of the capabilities that exist currently in your enterprise cybersecurity defense and an *orchestrator*

The orchestrator capability allows you to automate, to the degree you are comfortable, detection, response, and recovery operations. This is done through the use of *playbooks* and *workflows*.

Playbooks are the human readable representations of the series of actions that result in the desired outcome.

Workflows are the machine execution level representation of the playbook activities.

How SOAR Platforms Work in an Environment



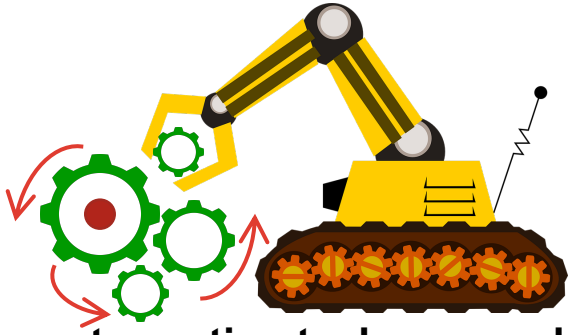
In traditional network and IT environments, a SOC analyst is responsible for the majority of actions and activities that must be carried out in response to a trigger (e.g. alerts, pre-defined time intervals, etc.).

SOAR platforms provide connectivity to, and orchestrates activities between, enterprise security tools and other network devices.

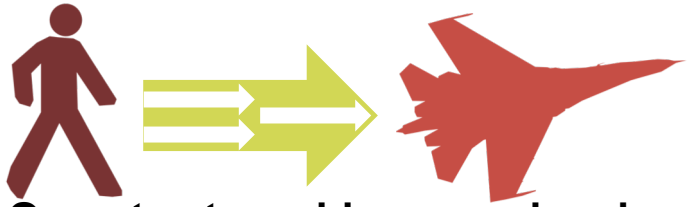
By initially automating tasks that are well defined and require minimal actual analysis, the SOC analyst is no longer the center of every activity. The SOAR tool will help SOC analysts focus on high value tasks and situations that are not ready for automation.

The Benefits of SOAR

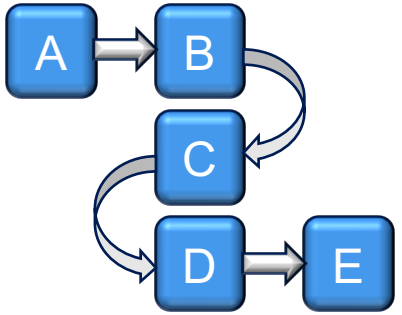
- Security orchestration, automation, and response (SOAR) can address critical shortcomings of today's cyber defense landscape.



Automate routine tasks so analysts can focus on hard technical analysis and value-add activities



Operate at machine-speed and cyber relevant time



Consistent application of organizational policies and procedures

- **What SOAR Is NOT…**

A quick turn-around solution

A whole replacement for human involvement

A one-way road towards complete automation

Why is this topic a crucial part of cybersecurity related education?

- Both business management and computer science communities need familiarization with SOAR technologies and its impact on the enterprise
- SOAR technologies are a major part of changing the defensive landscape to match the speed, scale, and sophistication of the malicious actor.
- The use of SOAR technologies allow organizations to better utilize their limited human cybersecurity resources and leverage their existing enterprise investments.
- Increasing the speed that alerts can be remediated as well as enable consistent application of organization policies and procedures when responding to said alerts.

SOAR is part of the current and evolving cybersecurity landscape and awareness of the benefits, capabilities, and implementation issues are foundational for the students of today.

Use Case A – SOAR from a business perspective

- Use Case A uses a business case describing the breach of “RSR Bank”.
- The breach and its impact are described and the students do an analysis of the enterprise network architecture to determine how the weaknesses are exploited.
- Mitigations for those weaknesses are determined as an exercise.
- How SOAR technologies can be used to mitigate the weaknesses and respond to the breach are described and discussed.

Use Case B – Implementing SOAR

- Use Case B continues the “RSR Bank” narrative after the C-Suite has decided to deploy a SOAR capability in the enterprise.
- The steps needed to deploy SOAR and the decisions that need to be made are described and discussed.
- The development of the needed playbooks and workflows are a part of the module.

Module B Lab Module – Rubber meets the road

- The lab module is an optional part of module B.
- Use of the module would require the institution to have an environment where the students would exercise the developed workflows.
- There are a number of vendors who have agreed to make their products available to academic institutions at special pricing.

How do I get this material?

Currently exploring making the modules available as a download on the https://www.clark.center/home website.

Hoping that this brief will help accelerate that process.

In the interim send an email to: ICD-Educate@jhuapl.edu to request a Box invite to download the modules.

NOTE: Response might be slow if there is high demand for the modules

NOTE: We request that only the student materials be available on a public site to prevent compromise of the instructor materials.

Discussion

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY