



# Security Orchestration, Automation and Response (SOAR)

As the threat landscape continues to grow in size and scale, it is important to decrease response times and better utilize resources. Automation tools that are integrated with your security stack help build a much more comprehensive and powerful solution for your organization – often requiring less headcount and offering much faster response time.

The ePlus SOAR Workshop will provide you with an introduction into the world of Security Orchestration, Automation and Response. Learn how adding a SOAR solution to your current security program can help give you better visibility into your network and security program and greatly reduce your attack surface.

## WHAT IS SOAR?

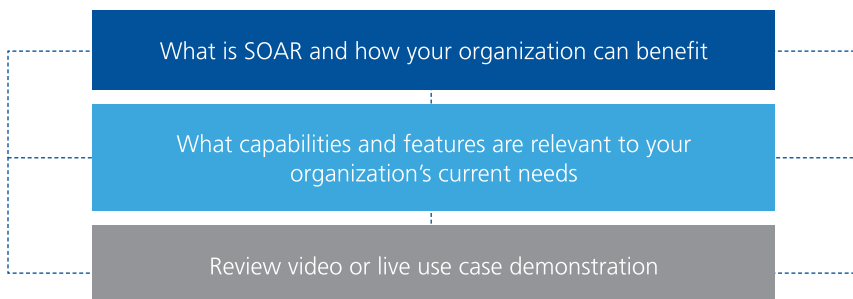
SOAR stands for Security Orchestration, Automation and Response. A SOAR solution integrates your organization's technology, people and processes and automates workflows into one centralized platform. This provides a faster, more effective approach to incident response and threat management.

## WHAT ARE SOAR CAPABILITIES?

- + Can support on-premise, hybrid and cloud-based infrastructures
- + Ability to take automated or prompted actions against infected systems (threat response)
- + Comprehensive event information correlation and forensics
- + SIEM, analytics and device integration
- + Ticketing system integration
- + Machine learning/AI capabilities

## WHAT DOES THE SOAR WORKSHOP LOOK LIKE?

The workshop can be delivered as an onsite or WebEx session with your key internal stakeholders. During the session, we will cover:



Transition into a deeper, consultative and more personalized discussion to address your specific business needs and desired outcomes.

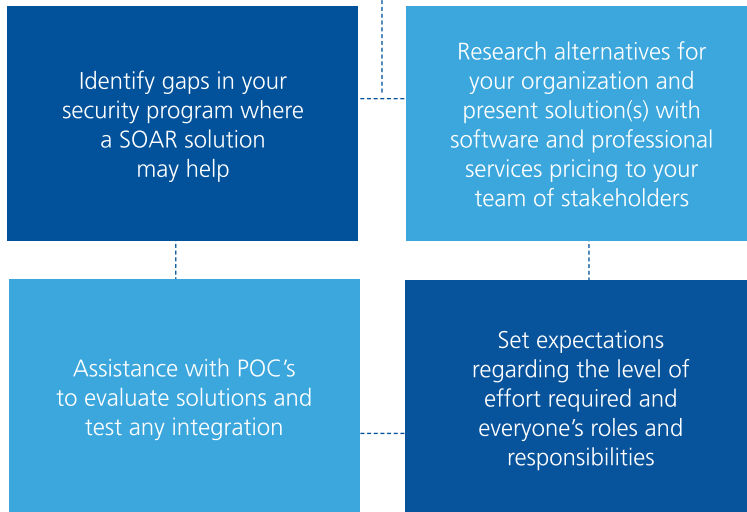
## Benefits of a SOAR Solution

- 1 Minimizes the MTTD (mean time to detect) and MTTR (mean time to respond)
- 2 Reduces the complexity of security solution management
- 3 Addresses the shortage of qualified security engineers/staff
- 4 Faster threat containment and remediation
- 5 Reduction in security-related operational costs

“By year-end 2020, **15% OF ORGANIZATIONS** with a security team larger than 5 people will leverage SOAR tools for orchestration and automation reasons, up from less than 1% today.”

– GARTNER

## What are the expected outcomes of the Workshop, and what will ePlus deliver?



## HOW CAN A SOAR SOLUTION HELP YOU OPTIMIZE YOUR DEFENSES?

The future of cyber security is about humans and machines working together to balance time and context. Your security staff needs access to accurate intelligence rapidly, but they also need enough information to decide on how to act. When automated defenses are enabled through orchestration capabilities and advanced behavioral analytics, your organization can take advantage of expedited and accelerated incident remediation. This improves security operations, enabling more value from existing tools and staff through greater emphasis on simplicity and efficiency. Also, automating low-value, repetitive manual tasks can enable scarce, and over-burdened, staff to focus on high-value activities.

- + Utilize tools that will lower overall IT costs, free up engineering time and improve delivery
- + Gather predictive and advanced behavioral analytics through integrated Machine Learning
- + Automate manual and repetitive processes to improve security operations efficiency

## Schedule a Workshop Today!

Contact your local ePlus Account Executive today to schedule your SOAR Workshop, or email [eplus-security@eplus.com](mailto:eplus-security@eplus.com)

For more information, visit [www.eplus.com/securityworkshops](http://www.eplus.com/securityworkshops)

©2019 ePlus inc. All rights reserved. ePlus, the ePlus logo, and all referenced product names are trademarks or registered trademarks of ePlus inc. All other company names, product images and products mentioned herein are trademarks or registered trademarks of their respective companies.

## What can a SOAR Workshop do for you?

### ORCHESTRATION

Making different products integrate with each other and automating tasks through workflows

### AUTOMATION

Combining technology, people and processes

### THREAT INTELLIGENCE

Using evidence-based knowledge to inform decisions regarding response to cyber threats

### INCIDENT RESPONSE

Identify, manage, record and analyze threats or incidents in real-time and with rapid response