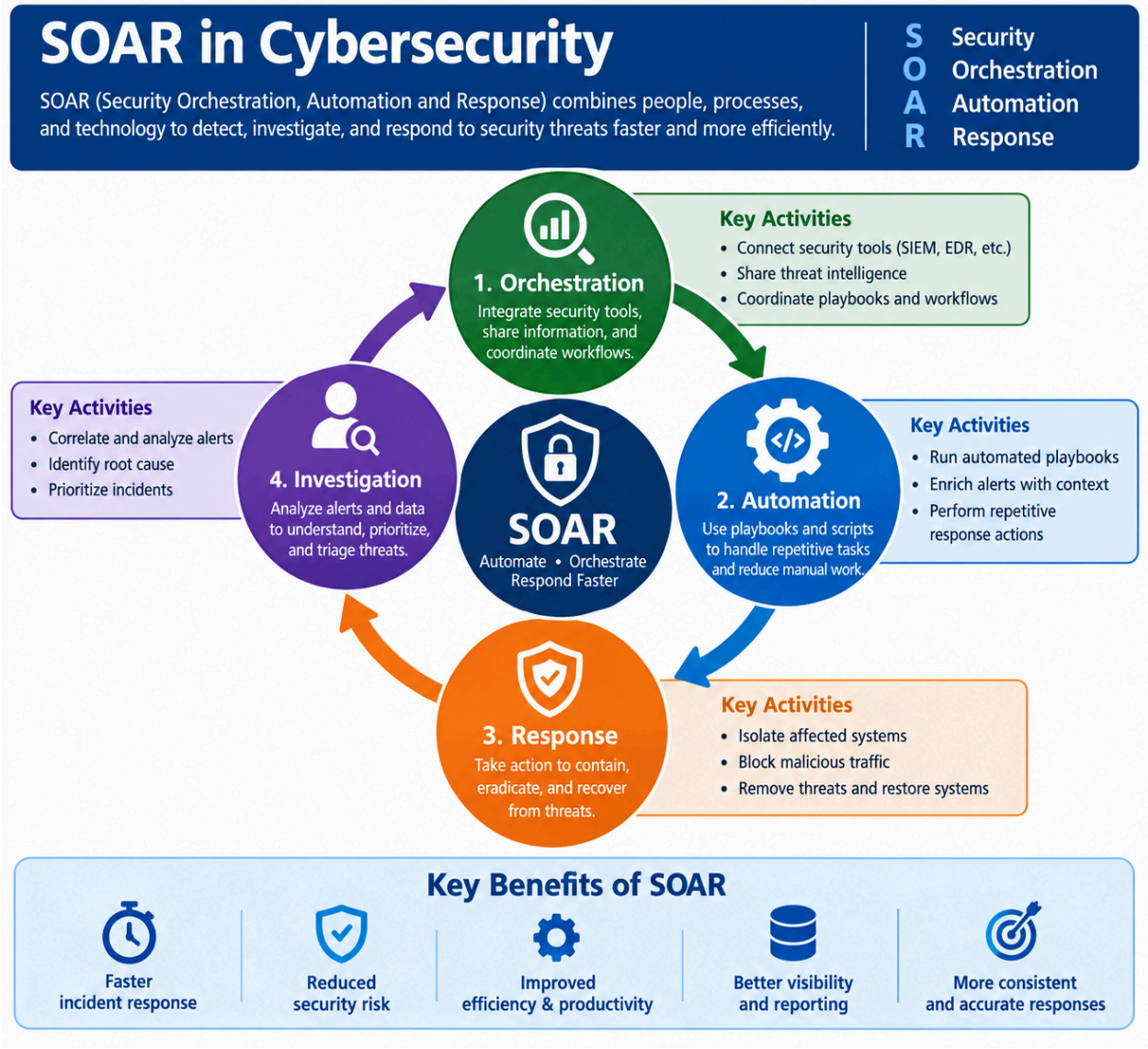
SOAR Cyber-security Framework Tutorial:

What is the SOAR Framework?

SOAR Stands for Security Orchestration, Automation, and Response. This framework is an integration of a variety of cybersecurity tools and technologies to help businesses and organizations in the management and response to security problems in a more efficient and feasible way.



SOAR achieves a feasible security framework by a combination of three areas of functionality:

Security Orchestration- Coordinates security responses and proactive steps across a variety of tools.

Automation- Streamlines repetitive security responses and proactive steps across a variety of tools.

Incident response- is a management of workflows when dealing with the protection of an information system from security threats.

According to the Splunk Security Event and Incident Management System SOAR has five essential functions, which are:

Orchestration- The direct guidance of all activities about a given security situation from the start of the incident to the end of an incident.

Automation- Methods like an execution plan that permits a security response team to implement a collection of basic reactions to a security incident in a matter of a few moments, versus hours when conducted manually.

Interoperability- Your SOAR framework should facilitate the support of including new security situations, new technologies and services, and new ways of doing things along with execution plans to implement during a cybersecurity incident.

Event and Alert Management and Prioritization- An organization's SOAR technological solution should organize, queue, and prioritize inbound security incidents and alarms or notifications.

Metrics and Reporting- It is imperative for the system professionals to comprehend the quantitative outcome and achievements along with resources that save the information technology infrastructure that automation provides, and to have real time access to this data through a dashboard within a SOAR Technological Tool.

The following are SOAR Tools on the market, some have a free community edition:

- **IBM Security QRadar SOAR**
- **Palo Alto Network Cortex XSOAR**
- **Rapid 7 InsightIDR**
- **Service Now Security Operations**
- **Crowd Strike Falcon SOAR**
- **Splunk Phantom**

IBM Security QRadar SOAR- is a SOAR platform designed to make central security responses and increase the way security operations centers (SOC's) in the management, automation, and resolution of cyber-security incidents, threats, and vulnerabilities.

Palo Alto Networks Cortex XSOAR- is an enterprise level SOAR framework. This platform is designed to assist centralized security operations center teams in consolidating security alerts and notifications, automate repetitive tasks, and increase the speed of tasks to respond to an incident. The Cortex can reduce incident response times by 90% or greater.

Rapid 7 InsightIDR- a security information and event management and extended detection and response platform that was developed to gather security telemetry data, reveal and find suspicious behavior, investigate security scenarios or incidents, and help security operation centers or teams respond to a security threat efficiently.

Functions of Rapid 7 InsightIDR:

1. Log and event collection
2. User and entity analysis of behavior on the information system.
3. Detecting suspicious network events or activities.
4. End point detection and response to security incidents.
5. Investigating and responding to a security incident.

ServiceNow Security Operations- ServiceNow Security Operations is an enterprise grade platform created to assist companies and organizations in identifying, promoting, investigating, and responding to security incidents and vulnerabilities. ServiceNow Security Operations integrates security data from cyber-security tools that are present in the ServiceNow platform and uses organized workflows, automation, and IT services from a cyber-security perspective to assist cyber-security teams in reacting to security threats in a proficient manner. A huge section of ServiceNow Security Operations is Security Incident Response (SIR) because it enables teams to import outside security notifications and incident data from outside the ServiceNow platform,

while looking into security incidents to gather more facts about it, practice security drills, and collaborate with teams or IT specialists.

CrowdStrike Falcon SOAR- CrowdStrike Falcon is a cloud-native endpoint cyber-security platform that collaborates with next generation anti-virus, endpoint detection and response, along with a round the clock 24 hour 365 day a year managed hunting service. This platform is implemented by a network professional because it uses the CloudStrike Security Cloud and artificial intelligence to present a real time detection of a cyber-attack, threat intelligence, and enriched telemetry across the whole platform. This platform uses an AI agent that consolidates multiple security abilities and gathers valuable endpoint data for detecting and responding to a network or Information Technology infrastructure threat.

Splunk Phantom- Splunk Phantom combines anomaly detection and automated incident response attributes. This platform enables automated incident management by rapidly assessing data and finding the root cause behind a security incident. In this platform, generative AI excels is AI-augmented vulnerability management.

References

Abdelmaboud, A., Salih, S., Hashim, A. H., Almohamedh, R. M., Tajelsier, H., & Motwakel, A. (2025). Are GPT-powered AI systems superior to traditional cybersecurity tools: Applications and challenges. *International Journal of Safety and Security Engineering*, *15*(9), 1885-1900.

Funskin, M., & Friedman, A. (2023). Usability of Artificial Intelligence, Machine Learning and other Emerging Technologies in Cybersecurity for Detection and Prevention of Cyber Attacks.

IBM. (n.d.). *Integrations - IBM QRadar SOAR*. IBM Security App Exchange. https://www.ibm.com/products/qradar-soar/integrations

IBM. (n.d.). *QRadar SOAR Plug-in app*. IBM Documentation. https://www.ibm.com/docs/en/qradar-common?topic=apps-qradar-soar-plug-in-app

IBM. (n.d.). *IBM Security QRadar SOAR Platform documentation and resources*. IBM Documentation. https://www.ibm.com/docs/en/sqsp/51.0.0?topic=security-qradar-soar-platform-documentation-resources

Palo Alto Networks. (n.d.-a). *Optimize operations with Cortex XSOAR*. Optimize Operations with Cortex XSOAR

Palo Alto Networks. (n.d.-b). *Visit Cortex XSOAR for integrations*. Visit Cortex XSOAR for integrations

Palo Alto Networks. (2023, May 9). *Build your customized Cortex XSOAR ROI report*. Palo Alto Networks Blog. Build Your Customized Cortex XSOAR ROI Report

Palo Alto Networks. (2026, July 10). *Cortex XSOAR use cases (Version 8.6)*. Cortex Documentation Portal. Cortex XSOAR use cases | 8.6 (EoL)

Palo Alto Networks. (2026). *Introduction to XSOAR* [Video]. Introduction to XSOAR

Palo Alto Networks Developer Hub. (n.d.). *Cortex XSOAR developer center*. Cortex XSOAR Developer Hub

Rapid7. (n.d.). *SIEM (InsightIDR) overview*. Rapid7 Documentation. Rapid7 SIEM (InsightIDR) documentation

Rapid7. (n.d.). *Detection rules*. Rapid7 Documentation. Rapid7 Detection Rules documentation

Rapid7. (n.d.). *SIEM (InsightIDR) Ultimate: Quick start guide*. Rapid7 Documentation. Rapid7 InsightIDR Quick Start Guide

Rapid7. (n.d.). *SIEM (InsightIDR) REST API*. Rapid7 Documentation. Rapid7 InsightIDR REST API documentation

Rapid7. (n.d.). *Rapid7 Agent*. Rapid7 Documentation. Rapid7 Agent documentation

ServiceNow. (2026). *Exploring Security Operations*. ServiceNow Documentation. ServiceNow Security Operations documentation

ServiceNow. (n.d.). *IBM Security QRadar SOAR - ServiceNow Store*. ServiceNow Store. https://store.servicenow.com/store/app/9df9e7a21b246a50a85b16db234bcbb0

ServiceNow. (2026). *Security Operations*. ServiceNow Documentation. ServiceNow Security Operations documentation

ServiceNow. (2026). *Security Operations (SecOps)*. ServiceNow Security Operations

ServiceNow. (2026). *Security Operations common functionality*. ServiceNow Documentation. Security Operations common functionality

ServiceNow. (2022). *Security Operations use case guide*. ServiceNow Security Operations Use Case Guide

Sinha, A. (2024). Challenges And Best Practices for Integrating Security Orchestration, Automation, And Response (SOAR) Platforms With Cloud Infrastructure.