The Future of **SOAR Technologies** in the Ever-Evolving Threat Landscape

IDC INFOBRIEF | SEPTEMBER 2021

Author:
Yeşim Araç Öztürk, Research Manager
IT Security, IDC

Sponsored by Logsign

What is SOAR?

By providing fast access to valuable security information, SOAR makes research and response processes more efficient. It provides the information we need to make the best decisions as quickly as possible.

The rising number of threats, shortages of skilled experts, and budget limitations are driving organizations toward SOAR technologies.

ORCHESTRATION

Orchestration is the machine-based coordination of an integrated solution stack by means of collecting and centralizing event data and context. It aims to manage people, processes, and technologies based on built-in case workflows.

AUTOMATION

Automation is the machine-driven execution of workflows with minimal human interaction. The engine runs predictable and repeatable batches of tasks. Decision making remains in the hands of the analyst.

MEASUREMENT

Measuring requires the clear display of strategic and tactical security information to support ongoing research, prioritize activities, formalize prioritization and response, provide feedback to the solution stack, improve workflows, and inform strategic management decisions.

RESPONSE

Response includes automating machine-based constraint workflows and the ability to update/edit controls across a connected IT stack.

What is SOAR Not?

It is not a SIEM platform.

SIEM collects and stores security data at a central point. This data is used to create actionable intelligence. SOAR integrates security tools, applications, and systems. It enables the automation/reorganization of repetitive manual tasks.

It is not a replacement for governance, risk, and compliance (GRC).

SOAR can perform some governance functions. However, it does not provide a deep GRC process.

It is not a threat or vulnerability management tool.

As an integrated tool, SOAR can “talk” to vulnerability and threat management programs.

It is not a replacement for human analysts.

Human analysts must validate, at the investigation stage, pivotal points where the next step of automation is appropriate. They must also fine-tune playbooks.

It is not a panacea.

SOAR requires a set of security solutions and a minimum of qualified analysts. It is not a stand-alone solution.

Security Operations Problems

DYNAMISM

Security alerts volume escalation

As the number of tracked assets and objects increases, so does the number of alarms.

Detection, triage, and response speed

Industry-average mean time to detect (MTTD) and mean time to resolve (MTTR) are counted in months.

FRAGMENTATION

Disconnected point products

According to IDC research, 27% of companies in Europe deal with more than five different vendors to manage their security stack.

Static independent controls lack orchestration

Integration was cited as a top five security concern by 62% of European organizations.

SUPPLIES

Costs increase — but budgets are frozen

The pandemic continues to negatively impact budgets. Budget cuts indirectly affect the success of security programs.

Scarce security team resources

Staffing remains a top concern for 48% of organizations.

Source: IDC, European Security Strategies Survey, 2019 (n = 700)

SOAR Drives Security at Scale

Aligning people, processes, and technology to deliver better incident response and automation across your security operations center (SOC)

A security operations (SecOps) approach introduces aspects around security at each stage of the software development life cycle.

The traditional SOC is not compatible with SecOps. Security analysts are tasked with incident response. Operations teams are busy building or running IT systems.

SOAR allows SecOps teams to respond faster to alerts. Many actions can be automated and performed instantly without waiting for human intervention.

Integrated with the existing tools of your SOC or security team, SOAR helps improve your SecOps MTTR.

«By 2023, to reduce security complexity faced by limited staff, **55%** of enterprise **security investments will be on unified ecosystem and platform frameworks.**»

Source: IDC FutureScape: Worldwide Future of Trust 2021 Predictions

Orchestration and Automation Across the SOC

- ✓ Orchestration enables organizations to integrate security tools. It facilitates interactions between tools and automated responses by leveraging predictive analytics.
- ✓ Orchestration emphasizes correlations and patterns, allowing events to be predicted.
- ✓ Orchestration accelerates SecOps tasks that can take humans minutes or hours to execute.

The automation of security alerts is becoming mainstream.

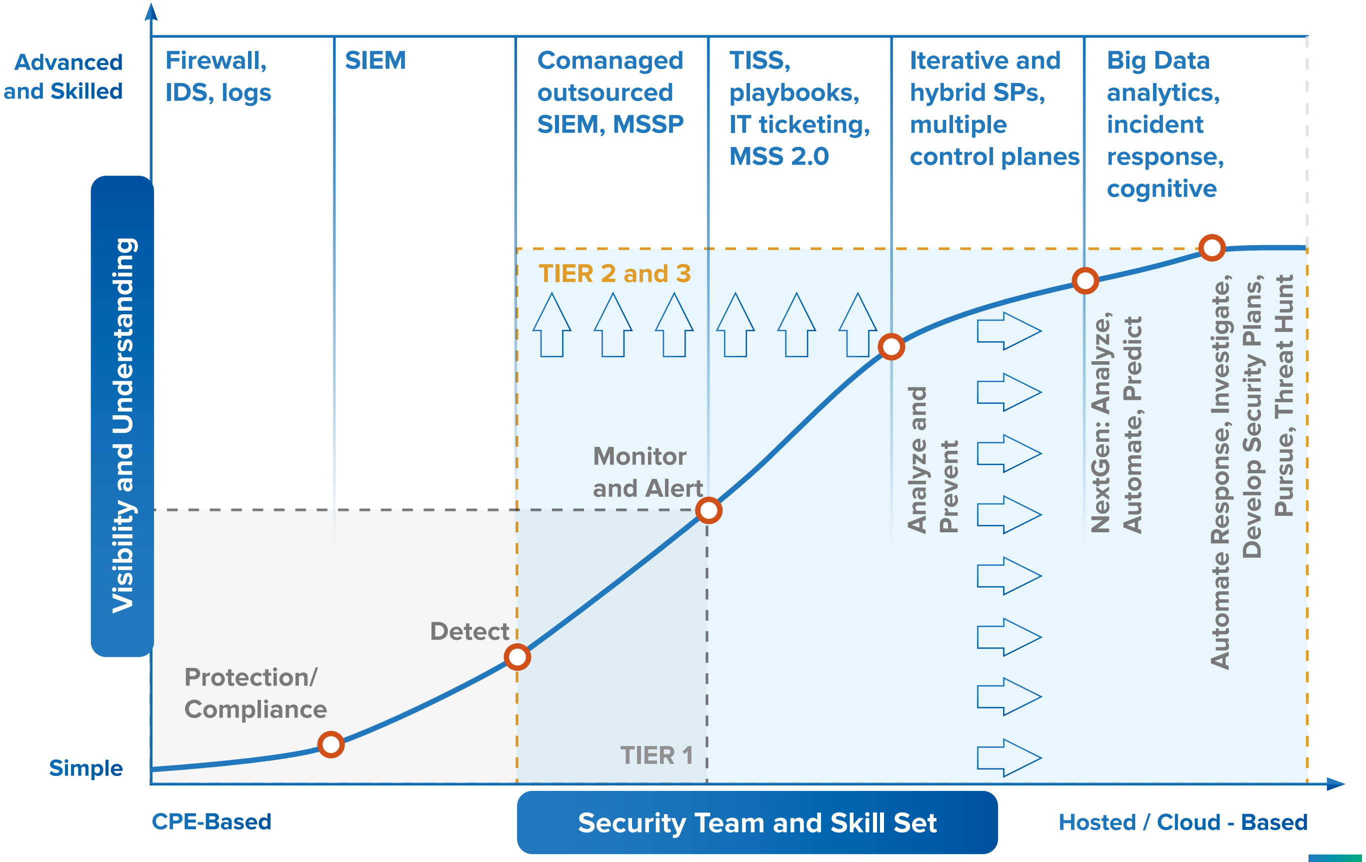
- ✓ Automation streamlines security operations and speeds up incident response in your SOC.
- ✓ By shortening MTTR and reducing the workload of overburdened security professionals, automation significantly improves SOC productivity.

«By 2023, collective risk management requirements between primary and third parties will force **50%** of third-party risk and security service providers to employ advanced analytic tools.»

Source: IDC FutureScape: Worldwide Future of Trust 2021 Predictions

SOAR and Detection and Response Evolution

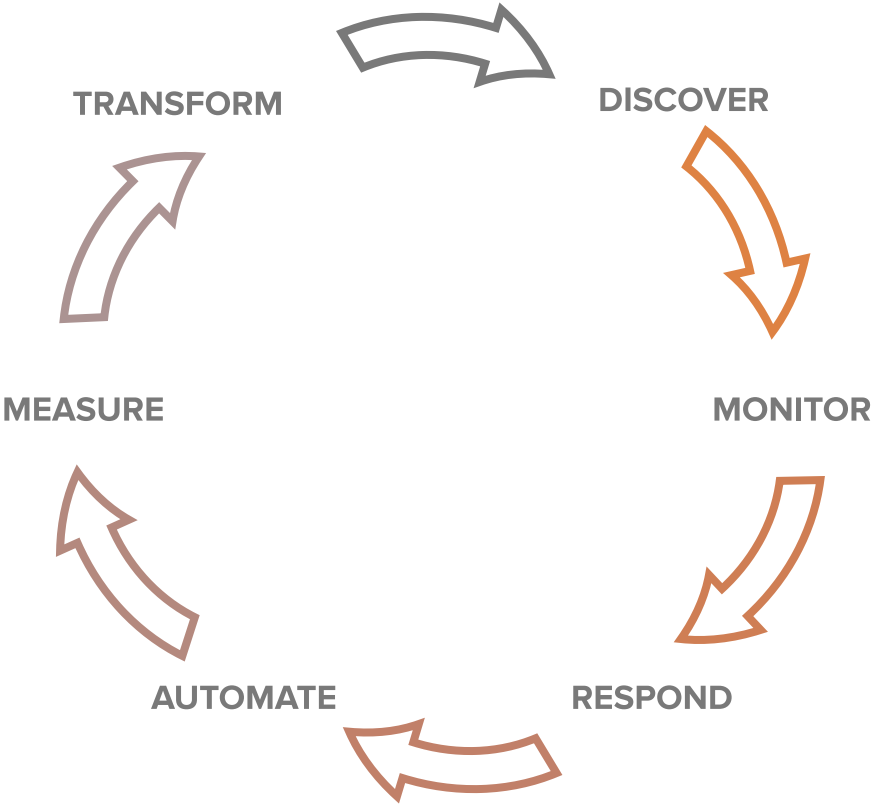
SOAR capabilities enable expansion of the response capacities of tier 1 analysts, allowing them to act faster. Automation and orchestration reduce the number of SOC analysts needed to respond to alarms. Alarm fatigue at the SOC decreases.


Advanced and Skilled
Simple
Visibility and Understanding
Firewall, IDS, logs
SIEM
Comanaged outsourced SIEM, MSSP
TISS, playbooks, IT ticketing, MSS 2.0
Iterative and hybrid SPs, multiple control planes
Big Data analytics, incident response, cognitive
TIER 2 and 3
TIER 1
Protection/ Compliance
Detect
Monitor and Alert
Analyze and Prevent
NextGen: Analyze, Automate, Predict
Automate Response, Investigate, Develop Security Plans, Pursue, Threat Hunt
CPE-Based
Security Team and Skill Set
Hosted / Cloud - Based

SOAR: Plan - Execute - Edit

How to Plan SOAR Implementations

- Review your assets and security environment. Identify existing capabilities that need improvement.
- Use adversarial tactics and techniques (ATT) and common knowledge (CK) frameworks to facilitate continuous asset tracking.
- Take advantage of automation to enhance responsiveness.
- To make security truly scalable, information/insights must be shared across the entire environment.
- Take measurements to discover ways to improve your security environment.



SOAR Boosts Maturity Across Enterprise Security

Well-Known Benefits of SOAR

- Provides powerful and fast incident response
- Helps SOCs handle the rising number of alerts
- Addresses visibility and risk-related concerns
- Solves alert fatigue issue for SOCs

Improve Security Maturity by Leveraging SOAR

- Better vulnerability management
- Greater efficiency and efficacy of security teams
- Rapid threat intelligence

Key Questions to Ask Before Investing in SOAR

Does it help with legal compliance?

How do analysts investigate cases when a playbook stops working?

How does the platform support SOC workflow and collaboration?

How does the SOAR platform help companies monitor, measure, and improve SOC performance?

What context does the platform provide for different assets in the alert?

Is there architectural growth support in the SOAR structures you are evaluating?

Are there ready reports and dashboard options that will increase the speed of analysts?

If there are ready-made Threat Intel Feed playbooks, what are their scopes?

What are the capabilities of ready-made playbooks?

Logsign Case Study

TIRSAN

With Logsign SOAR, Tırsan has acquired a platform where events can be analyzed faster, tasks can be resolved automatically and manually with interactive communication, and incident response processes are managed quickly.

> “With Logsign SOAR, detailed analyzes of cyber events that occur from many points are made and incident response processes are automated.”
>
> Hakan Karadelioğlu, *Director of Project and Technology Management at Tirsan*

Turkey’s reliable leader for 44 years and Europe’s 4th largest trailer manufacturer, Tırsan produces its own technology in its award-winning R&D center in order to increase the competitiveness of its customers in more than 55 countries. Working with Company Management Systems (ERP) since 1998, Tırsan implements the most up-to-date technology applications in this field with its own competent teams and reliable business partners.

IDC Recommends a Strategic Approach to SOAR

- Leverage automation and orchestration to make analysts happier and more productive.
- Allow the platform to initiate an automatic response for non-critical assets.
- Identify specific use cases for automation in your organization's complex processes.
- Take the necessary steps to keep security analysts focused on their core tasks.
- Improve productivity and reduce stress. Help analysts feel more enthusiastic about their work.
- Design automated blocking strategies using threat intelligence.

About the Sponsor Logsign

Founded in
2010

65 Employees

Wide customer base for both our products and value-added services.

Strong references in multiple industries

Partners in Europe, Middle East & Africa regions.

LOCATIONS

The Hague, Netherlands
Istanbul, Turkey
San Francisco, USA

Learn more at our website

We build robust and clutter-free cybersecurity for enterprises to successfully minimize disruption by increasing visibility, focusing on staying safe. We do it in the smartest, simplest-to-use way possible! Innovative technologies. Value-centric approach. That's how we roll.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives.

IDC is a subsidiary of IDG, the world's leading technology media, research, and events company. Further information is available on our websites at www.idc.com

IDC TURKEY
Zincirlikuyu Akademiler Sitesi,
D Blok Daire: 74
34340 Beşiktaş – İstanbul, Turkey
+90 212 356-0282
https://idc-community.com/
www.idc.com

Global Headquarters
5 Speen Street Framingham, MA
01701 USA
P.508.872.8200
F.508.935.4015
www.idc.com

in IDC Türkiye

IDC Türkiye

Copyright Notice

The external publication of IDC information and data—this includes all IDC data and statements used for advertising purposes, press statements, or other publication—requires written approval from the appropriate IDC Vice President or the respective Country Manager or business leader. A draft of the text to be published must be attached to the request. IDC reserves the right to reject the external publication of data.