Plixer

SOLUTION BRIEF

Plixer and SOAR integration

Strengthening your security posture:

The Plixer platform is a Deep Network Observability solution that provides actionable data and monitoring intelligence to help organizations detect and respond to security incidents. One of the key strengths of the Plixer platform is its ability to act as a notification engine, providing real-time alerts and notifications to security teams when network anomalies are detected.

In addition, the Plixer platform contains security intelligence that enables you to detect suspicious behavior and potential security threats. The Plixer platform can also integrate with external tools, like SIEM and SOAR solutions, to enhance your incident management and response.

This integration allows security teams to receive alerts from the Plixer platform and respond to incidents quickly and efficiently. By leveraging the Plixer platform's actionable data, monitoring intelligence, notification profiles, and integration capabilities, organizations can improve their overall security posture and reduce the risk of cyber threats.

As you might have guessed, the increasing sophistication of cyber threats and the growing complexity of IT environments have made it challenging for organizations to detect and respond to security incidents. In this document, we will discuss the basics of SOAR, its benefits, key features, and use cases. We will also explore how SOAR systems receive alerts from external tools, like Plixer's platform, and provide specific examples of how a SOAR system can respond to security incidents.

What is SOAR?

SOAR (Security Orchestration, Automation, and Response) is a technology stack that combines security orchestration, automation, and response capabilities to streamline incident response processes. SOAR systems integrate with various security tools and automate incident response actions, reducing the time it takes to detect and mitigate security incidents. SOAR systems also provide a centralized platform for incident management and reporting, enabling security teams to gain a holistic view of their security posture.

Benefits of SOAR:

- Faster incident detection and response times
- Increased efficiency and productivity of security teams
- Reduced risk of human error in incident response processes
- Improved visibility and reporting of security incidents
- Streamlined incident response workflows

Key features of SOAR:

- Automated incident response actions
- Integration with security tools via APIs, webhooks, or email notifications
- Orchestration of incident response workflows
- Incident management and reporting capabilities
- Dashboard and analytics for security operations monitoring and reporting

Use cases for SOAR:

- Threat detection and response
- Vulnerability management
- Compliance management
- Incident response orchestration
- Security operations automation

How SOAR systems receive alerts:

SOAR systems can receive alerts from external tools through various means, such as APIs, webhooks, email notifications, and other integration methods. For example, a SOAR system can integrate with network traffic analysis tools, vulnerability scanners, and security awareness training solutions to receive alerts and automate the response to security incidents.

Examples of SOAR response actions:

- Quarantine a compromised host
- Block a malicious IP address
- Apply a patch to a vulnerable system
- Isolate a vulnerable system
- Provide additional training to an employee
- Re-route traffic to reduce congestion

What is the most common way a SOAR receives an alert?

The most common way a SOAR system receives an alert is through integration with a Security Information and Event Management (SIEM) tool. SIEM tools are commonly used to collect and analyze security events from various sources in an organization's environment, such as firewalls, intrusion detection systems, and endpoint protection solutions.

SOAR platforms can integrate with SIEM tools to receive alerts generated by them, enabling security analysts to orchestrate and automate the response to security incidents. The integration between a SOAR platform and a SIEM tool allows the SOAR system to receive security events in real-time, and correlate them with other events to provide better context for analysts to investigate and respond to incidents.

However, it's important to note that SOAR systems can also receive alerts through other means, such as Network Detection and Response tools like the Plixer platform, Endpoint Detection and Response (EDR) tools, APIs, manual triggers, scheduled triggers, and threat intelligence feeds. The way a SOAR system receives alerts may depend on the specific use case and the security tools deployed in an organization's environment.

Here are some specific examples of how a SOAR system can receive alerts from external tools:

1. The Plixer platform Integration: A SOAR system can integrate with the Plixer platform to receive alerts via the API. The Plixer platform can send alerts to the SOAR system based on network traffic anomalies, such as bandwidth spikes and traffic congestion.
2. Vulnerability Scanner Integration: A SOAR system can integrate with vulnerability scanners like Nessus and Qualys via APIs, webhooks, or email notifications. When a new vulnerability is detected, the vulnerability scanner can send an alert to the SOAR system.
3. Security Awareness Training Integration: A SOAR system can integrate with security awareness training solutions like KnowBe4 and PhishMe to receive alerts via email notifications or APIs. When an employee fails a phishing simulation or reports a suspicious email, the security awareness training solution can send an alert to the SOAR system.

Why is SOAR important?

SOAR is a vital tool for modern-day networking environments, and its usage is becoming increasingly common. SOAR platforms enable organizations to streamline their security operations by automating repetitive tasks, integrating disparate security technologies, and enabling rapid response to security incidents.

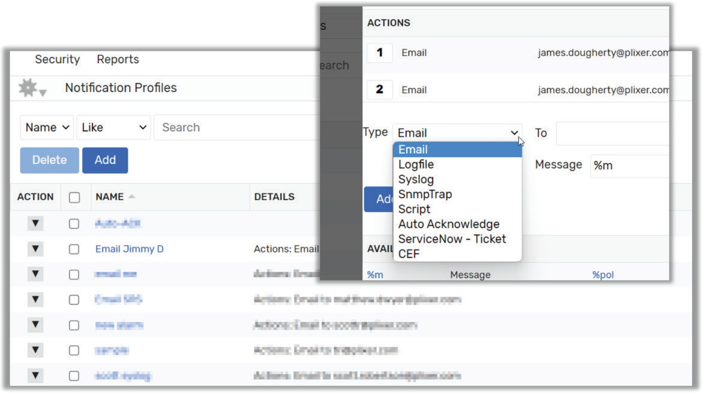
Manual incident response processes are time-consuming and error-prone, and can delay the identification and mitigation of security threats. SOAR provides a solution to this problem by enabling organizations to automate their incident response processes and integrate their security tools.

As cyber threats continue to evolve and become more sophisticated, SOAR tools provide a robust defense against these threats by enhancing the efficiency and effectiveness of security teams. Furthermore, SOAR can be a vital part of the Response (R) stage of an Network Detection and Response (NDR) strategy, allowing security teams to quickly detect, investigate, and respond to security incidents, ultimately reducing the risk of a successful cyber-attack.

How does the Plixer platform integrate with a SOAR?

Notification profiles

Notification profiles offer the flexibility of creating a single profile that can be applied to multiple policies or objects in polled maps. These profiles support various notification methods, including Email, Logfile, Syslog, SNMPTrap, Script, and Auto Acknowledge. To ensure that the alert contains the desired information, users can enter the necessary data and select additional details from the "Available Variables for Message" list. Users can also specify the number of minutes to wait before triggering the selected action, with 0 as the default value. In case multiple notification alerts are added to a single Notification Profile, users can modify the order of notifications by assigning lower or higher numbers to the left of each notification and using the "Re-order Alerts" button.



1 Email	james.dougherty@plixer.com
2 Email	james.dougherty@plixer.com

Type: Email

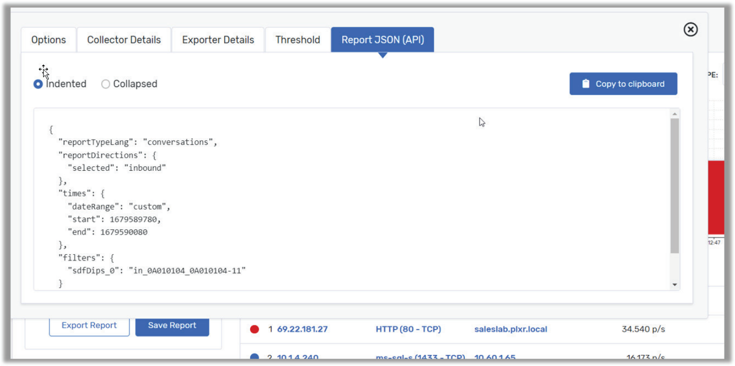
To:

Message: %m

ACTION	NAME	DETAILS
▼ □	Email Jimmy D	Actions: Email

%m	Message	%pol

Reporting API



```
{
  "reportTypeLang": "conversations",
  "reportDirections": {
    "selected": "inbound"
  },
  "times": {
    "dateRange": "custom",
    "start": 1679589780,
    "end": 1679590080
  },
  "filters": {
    "sdfDips_0": "in_0A010104_0A010104-11"
  }
```

● 1	69.22.181.27	HTTP (80 - TCP)	saleslab.plxr.local	34.540 p/s
● 2	10.1.4.240	ms-sql-s (1433 - TCP)	10.60.1.65	16.173 p/s

The reporting API in the Plixer platform provides a valuable tool for security teams to access and analyze network conversation data. This API allows users to pull dynamic conversation data from the Plixer platform into external applications for further analysis and processing. The reporting API can be used to generate custom reports, perform trend analysis, and identify patterns in network traffic that may indicate potential security threats.

In the context of our SOAR discussion, the reporting API in the Plixer platform can be a critical component in incident response and management. By accessing conversation data through the reporting API, SOAR systems can gain valuable insights into network behavior and identify potential security incidents. This information can then be used to trigger automated response actions, such as quarantining an infected device or blocking suspicious traffic. The reporting API in the Plixer platform also enables integration with other security tools, allowing for a more comprehensive approach to incident response and management. Overall, the reporting API in the Plixer platform provides a powerful tool for security teams to proactively identify and respond to security incidents in their network.

Custom services

Custom services can provide significant value when considering integrating external tools into a SOAR platform. A custom service is a tailored integration that is specific to an organization's unique requirements, providing functionality beyond what is available through pre-built integrations. This level of customization can improve efficiency and reduce the workload on security teams by automating processes and workflows that are specific to their environment. Additionally, custom services can allow for more accurate and timely data sharing between tools, enabling faster incident response times and more effective threat detection.

Summary

In conclusion, the Plixer platform is a valuable addition to any organization's SOAR deployment as it provides powerful network traffic analysis capabilities that can help detect and respond to security incidents quickly and efficiently. By leveraging the Plixer's actionable data, monitoring intelligence, notification profiles, and integration capabilities, organizations can improve their overall security posture and reduce the risk of cyber threats. Additionally, the Plixer's ability to act as a notification engine, coupled with its monitoring intelligence, makes it an ideal tool to integrate with SOAR systems, enabling security teams to receive real-time alerts and automate incident response actions, thus improving their efficiency and productivity. In short, adding the Plixer platform to your SOAR deployment can help you streamline your incident response processes, reduce the risk of human error, and ultimately strengthen your security posture.

About Plixer

Plixer gives you visibility and context of event space and time so you can better understand what's happening in your IT environment. Our 20+ years of network monitoring and management solutions help us provide innovative solutions that help you secure and optimize your digital enterprise. **Don't miss a thing.**

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.