LogicHub

SOLUTION BRIEF

The LogicHub Difference

SOAR+

	Traditional SOAR	LogicHub SOAR+
Security Tool Integration	✓	✓
Workflow Automation	✓	✓
Threat Intelligence Enrichment	✓	✓
Basic Response Automation	✓	✓
Case Management	✓	✓
Decision Engine to Separate Signal from Noise		✓
Advanced Analytics and Machine Learning		✓
Large Scale Data Set Handling		✓
Threat Hunting Automation		✓
Out-of-the-box Threat Detection Playbooks		✓
Rapid Production-Grade Integrations		✓

Security Orchestration, Automation, and Response (SOAR) is an established product category in today's IT market. Gartner, who coined the term, defines SOAR as "technologies that enable organizations to collect security threats data and alerts from different sources, where incident analysis and triage can be performed leveraging a combination of human and machine power to help define, prioritize and drive standardized incident response activities according to a standard workflow. SOAR tools allow an organization to define incident analysis and response procedures (a.k.a., plays in a security operations playbook) in a digital workflow format, such that a range of machine-driven activities can be automated."

For any security product to meet Gartner's definition of a SOAR platform, it must include the first five features listed in the table above. In addition to these basic features, the LogicHub SOAR+ security automation platform provides unique features designed to deliver a better experience for security analysts. These features combine incident response with autonomous threat detection and threat hunting to improve the value, scope and accuracy of SOAR playbooks, accelerating alert triage, threat hunting and incident response. SOAR+ dramatically reduces analyst workloads while improving security operations center (SOC) effectiveness.

Let's examine each of these features in turn, including the SOAR+ features that distinguish the LogicHub SOAR+ security automation platform from traditional SOAR products.

Traditional SOAR Features

Security Tool Integration

To collect data and events for analysis and to issue commands as part of remediation playbooks, a SOAR platform must integrate with other security tools and IT systems. These systems include next-generation firewalls, email servers and services, cloud environments, third party tools and services such as reputation databases, Security Information and Event Management (SIEMs), and more.

Obviously, it's important for a SOAR or SOAR+ platform to support a broad range of integrations out of the box. But since no platform can automatically support all the integrations needed for every IT environment of every organization, what's equally important is how easy it is to add new integrations, including custom, proprietary integrations. LogicHub offers ready-to-use integrations for leading security and infrastructure solutions as well as for many popular IT tools and applications, providing a holistic ecosystem for threat detection automation. (See https://www.logichub.com/product/integrations.) Thanks to its modern RESTful Integration Framework, LogicHub can also integrate with any system or service, even those without a published API, within two weeks. For more information, see the Rapid Production-Grade Integrations section below.

Workflow Automation

SOAR automates the performance of routine, low-complexity list of tasks that a SOC playbook prescribes for investigating or mitigating a possible threat. These tasks might include gathering and enriching data and performing actions to respond to attacks or potential attacks, such as closing ports, running anti-virus scans, adding IP addresses to a blacklist, and so on.

For example, instead of requiring a security analyst to manually look up the reputation of an IP address and then to update a firewall rule if the address' reputation is bad, a security automation platform can perform both these steps automatically in seconds (or less).

Like SOAR platforms, the LogicHub SOAR+ platform performs robotic automation like this, but it also performs cognitive automation, assessing the importance of various events and pieces of data to accelerate the decision-making process used by security analysts for threat hunting. This cognitive automation dramatically reduces MTTR rates and helps SOCs defend against threats much more promptly.

Threat Intelligence Enrichment

Enterprises are awash in security data. Nearly every IT system produces a log file. All those log file entries can be collected and correlated for analysis. In addition, there are IDS/IPS, DLP, User and Entity Behavior Analytics (UEBA) systems monitoring various suspicious events across networks and IT systems and raising alerts of their own.

Event reporting and log files are merely a first order of security data. To make sense of all these events and log entries, the SOC team needs context. They need to scan networks, emails, file attachments for malware and suspicious behavior. They need to know the reputation of files, programs, domains, and IP addresses. When data is enriched with context like this, it becomes much more useful to SOC teams.

To achieve this enrichment requires a rich library of integrations, as well as open APIs and a framework to easily create new integrations. Data enrichment ultimately depends on the breadth of integrations available and the ease with which new, valuable integrations can be built.

Using integrations to various security tools, third-party services such as reputation database, sandbox platforms, and LogicHub's own modules and Machine Learning (ML) classifiers, LogicHub ingests, analyzes, and enriches security log data, ensuring that security analysts have the rich data they need for fast, accurate threat detection and analysis.

Basic Response Automation

A traditional SOAR automates incident response robotically. This automation saves time and reduces the SOC's Mean Time to Response (MTTR) for threats. While a SOAR platform helps alleviate some of the pain of processing SIEM alerts, it performs robotic automation based on simple "If-Then-Else" logic, which is suitable for handling routine tasks that don't require decision-making.

Traditional SOARs are actually designed to automate post-detection incident response. They are far less intelligent than SIEM systems, since they can operate only within the confines of binary logic. These limitations would be acceptable only if a security analyst team experienced zero false positives and was not concerned about false negatives.

LogicHub is designed to automate much more challenging tasks such as finding new unknown threats in an environment.

Case Management

Case management is an important part of any SOAR platform. It helps gather the various sources of information and keeps an audit log. The case management screen is the primary dashboard for most security analysts.

The LogicHub SOAR+ platform applies automation to make case management more efficient and effective. One difference from traditional SOAR platforms: LogicHub creates cases only for events that are deemed suspicious, rather than opening cases for every event it analyzes. This selectivity, based on advanced analytics, greatly reduces the volume of cases that security analysts need to evaluate and helps keep the focus on the truly important events.

Another difference: Focusing on the analyst experience, LogicHub's automated case management features turn enhanced threat hunting playbooks into actionable incident response recommendations that security analysts can apply with the click of a button. These recommendations help analysts mitigate threats and resolve problems more quickly.

LogicHub SOAR+ Features

Decision Engine to Separate Signal from Noise

The LogicHub SOAR+ security automation platform adds a decision engine to SOAR capabilities and automates analysis of gathered data for threat detection and threat mitigation. The decision engine automatically performs comparisons and deep correlations that analysts normally have to do themselves manually. This analysis might take analysts hours or days, but LogicHub performs it instantly.

The LogicHub decision engine can analyze thousands of events simultaneously, thanks to the platform's support for large scale data sets (see below). By analyzing these alerts and eliminating false positives, LogicHub SOAR+ fully automates the end-to-end alert triage process, requiring far fewer resources, and significantly improving threat detection efficacy while reducing the Mean Time to Detection (MTTD) or "Dwell Time."

LogicHub SOAR+ also improves the efficacy of SOC teams, especially those who struggle to process alerts from multiple security systems such as SIEM, UEBA (User and Entity Behavior Analysis) systems, phishing inboxes, and any other systems that generate large volumes of alerts. Through automation, LogicHub enables security analysts to manage alerts coming in from a large number of systems, accelerates threat analysis, threat detection, and analyst decision-making, and improves their accuracy as well. Compared to SOAR, decision automation applies ML and data science techniques that are far more sophisticated and adaptive. It fully automates alert triage and determines which remediation steps, if any, should be performed in response to a potential threat.

Advanced Analytics and Machine Learning

LogicHub applies multilevel analysis across dozens of data points to correlate the scoring of alerts and events. LogicHub is the only platform to provide automated analysis and decision support to analysts, using machine learning, correlation, and advanced analytics.

Deep correlation and other AI techniques, such as machine learning, enable SOC teams to detect threats that traditional manual investigations overlook. In addition, threat detection techniques leveraging ML become more accurate and effective over time by automatically refining algorithms based on success and error rates and applying input from security analysts. LogicHub's SOAR+ security automation enables SOCs to make the most of their security analysts' expertise, while automating work for speed and efficiency.

SOAR solutions, which rely on basic "If-Then-Else" logic, are incapable of automating processes that require sophisticated logic and analysis. By supporting more complex analysis, the LogicHub SOAR+ Security Automation Platform provides a powerful automation engine that security analysts need for addressing the complexity and sophistication of real-world situations and threats.

Large Scale Data Set Handling

LogicHub is the only security automation platform that can scale to handle extremely high data volumes and not be constrained by the limitations of traditional relational databases. Performing big data analysis requires a strong underlying platform such as Apache Spark (https://spark.apache.org/). LogicHub SOAR+ is built on Apache Spark, which gives it the ability to analyze not just a few incidents but thousands at a time.

Apache Spark is an open source, fast data analytics and machine learning algorithmic engine used for processing data at a large scale. Spark's cluster computing technology uses data parallelism and fault-tolerance to process data quickly and reliably. The engine's in-memory data processing accesses data much more quickly than traditional disk-based access. Spark helps LogicHub process data quickly, giving security analysts the data they need as quickly as possible.

Threat Hunting Automation

There is no magic bullet for security. Because vulnerabilities and attackers evolve, there will always be a need for human beings to defend against newly created techniques and exploits.

Threat Hunting Automation is a key feature of Logichub. The LogicHub Decision Engine enables playbooks to fully automate the tedious and complex tasks involved with threat hunting, helping to reduce the repetitive tasks in an analyst's workload so they can focus on the most important events and detecting new threats.

LogicHub automates advanced threat hunting activities by applying a machine learning model for malicious process detection to differentiate benign from malicious. In contrast to the robotic automation of SOAR platforms, LogicHub's Threat Hunting Automation takes into account the context of events and other data, discovering anomalies and scoring them to make decision-making as accurate as possible. This more comprehensive and sophisticated approach to automation enables security teams to easily detect and characterize potentially dangerous activity, such as risky PowerShell actions, beaconing or lateral movement, while differentiating this danger activity from benign actions carried out by authorized system administrators.

Out-of-the-Box Threat Detection and Automation Playbooks

To get SOC teams started, the LogicHub platform includes advanced playbooks for activities frequently investigated by SOCs, such as Suspicious Login Activity, IOC Search & Event Enrichment, Proxy Beacon Detection with Zscaler, Threat Hunting in AWS CloudTrail, Malware Alert Triage, Phishing Report Triage, and many others. All LogicHub playbooks can be customized for a particular IT environment either by LogicHub customers or with the help of the LogicHub professional services team.

LogicHub also provides threat detection playbooks based on the MITRE ATT&CK framework, a globally-accessible knowledge base of adversary tactics and techniques. LogicHub autonomously maps attacks in real time to the MITRE ATT&CK framework, delivering users immediate indicators and attack technique context.

Rapid Production-Grade Integrations

Integrations connect data and systems to the LogicHub platform, broadening the scope threat hunting, threat detection, alert triage, and incident response. SOCs need a security platform that offers integrations to a wide range of popular business and security systems and that supports the rapid creation of new custom integrations to make the platform's coverage as comprehensive as possible. LogicHub offers a large and growing number of integrations out of the box and can implement integrations in just days or hours or develop a new custom integration in one to two weeks. Existing customer scripts can be converted in hours or even minutes.

Unlike SOAR vendors whose product development teams decide whether or not they want to offer an integration, which might then take months to develop, LogicHub operates on a no-cost, integration-on-demand model for integrations involving popular tools and applications.

For a customer's perspective on the benefits of LogicHub's integration capabilities, watch this interview with the CISO of Motorola Mobility.

Summary

SOAR platforms provide important basic capabilities for SOCs interested in improving their threat intelligence and accelerating their automated responses to threats.

The LogicHub SOAR+ Security Automation Platform includes all those capabilities along with other unique capabilities to provide a far richer set of features for SOCs and the organizations theyre protecting 24/7/365.

The highly customizable LogicHub SOAR+ Security Automation Platform applies advanced analytics to large data sets, improving the speed and accuracy of threat detection. In addition, it allows customers to tailor and fine-tune playbooks to address security automation challenges such as alert triage, phishing triage, threat detection, threat hunting, and other critical security activities.

Security threats and alert volumes are ever increasing. With the LogicHub SOAR+ solution, SOC teams can apply the power of automation to reduce workloads and improve the speed and accuracy of threat detection and incident response.

About LogicHub

LogicHub, the SOAR+ company, is the only security automation platform that delivers autonomous detection and response automation for security operations teams. By applying machine learning and analytics on large data sets, LogicHub automates security analyst workflows and decisions, helping teams save time, find critical threats, and eliminate false positives.

LogicHub

a: 154 E Dana Street, Mountain View, CA 94041
w: www.logichub.com
e: info@logichub.com
p: (650) 262-3756