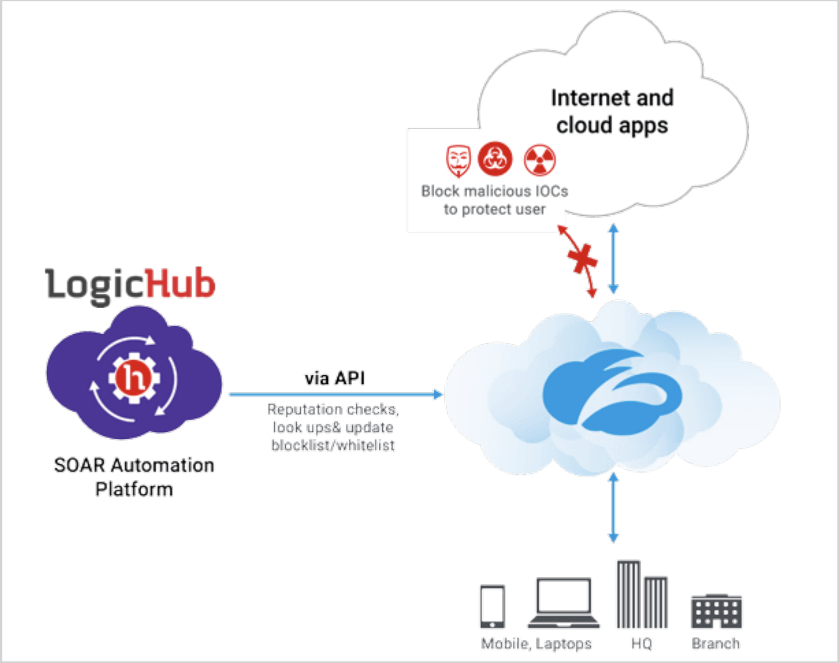
LogicHub zscaler™

Zscaler and LogicHub Autonomous Threat Detection and Incident Response Automation

Compatibility:
LogicHub SOAR+ security automation platform and Zscaler Internet Access

Zscaler Internet Access delivers a security stack as a service from the cloud providing full content analysis of all traffic including SSL communications and trusted content, across all ports and protocols. Zscaler can help deliver airtight internet security with Cloud Firewall, Cloud Sandbox, Content and URL filtering, Data Loss Prevention (DLP) and CASB. The Zscaler service provides detailed, real time log consolidation across all locations giving unprecedented visibility of user, device and network activity. Since Zscaler Internet Access is delivered as a cloud based service, it allows enterprises to deliver consistent and comprehensive security, even as enterprises open new locations, on-board new users, add new applications or transform to cloud-first, mobile-first architectures.

Now, users can leverage the cloud security capabilities of Zscaler with the security orchestration, automation, incident response, and autonomous threat detection of LogicHub SOAR+.


Internet and cloud apps
Block malicious IOCs to protect user
LogicHub
SOAR Automation Platform
via API
Reputation checks, look ups& update blocklist/whitelist
Mobile, Laptops
HQ
Branch

Integration Features

- Automate Threat Detection and Hunting: Reduce MTTD by identifying unknown threats in real-time and gain deeper visibility into new threats by automating the expertise of a skilled analyst to hunt unknown threats by using Zscaler actions (reputation checks, lookup and addition and deletion of indicators from custom blacklists for real-time enforcement and malware analysis, by performing file reputation lookups from Zscaler sandbox results) within LogicHub playbook tasks or stand-alone case commands.

- Automate Alert Triage: Investigate and threat rank every alert by automating complex investigation playbooks quickly and easily as well as analysis and decision making by applying deep correlation, data science operators.

- Automate Incident Response: Contain, mitigate, and respond with confidence by creating automations quickly and easily and ensure thorough investigations and catalog evidence documentation consistently

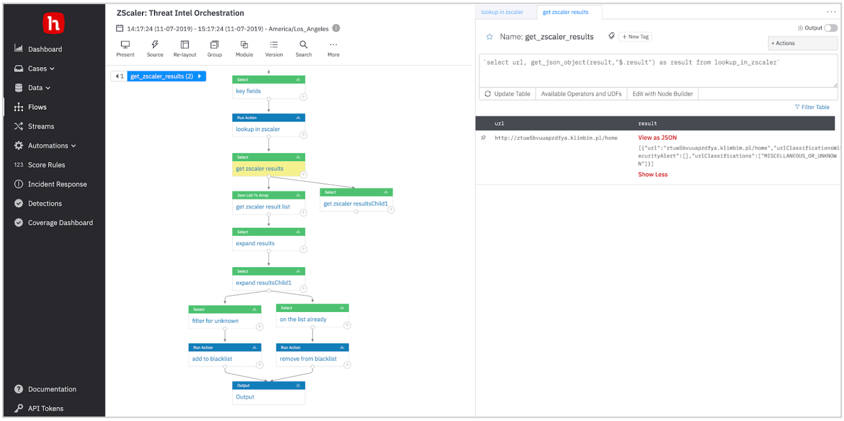
- Integration with Zscaler and your other tools is seamless, rapid, and allows for further enrichment data.

USE CASES

AUTOMATED THREAT HUNTING

Most organizations today aren't able to proactively identify and hunt for threats. They are stymied by lack of resources and manual processes that limit hunting frequency. Manually collecting artifacts from various point systems, sifting through logs or performing network packet captures isn't scalable in today's threat environment, where it's no longer enough to be passively vigilant.

LogicHub SOAR+ integration with Zscaler gives analysts a centralized view into an organization's inbound and outbound traffic and allows the analyst to look at Zscaler artifacts, capture suspicious indicators and perform reputation checks or lookups all with a single playbook. This tremendously reduces the number of manual steps and time that an analyst would require to identify and hunt for threats. Once Zscaler deems an IOC as malicious, LogicHub can also automatically have Zscaler enforce a block policy from within its playbook, without requiring the analyst to log into multiple systems or switch screens.



ZScaler: Threat Intel Orchestration

14:17:24 (11-07-2019) - 15:17:24 (11-07-2019) - America/Los_Angeles

Name: get_zscaler_results

```
`select url, get_json_object(result,"$.result") as result from lookup_in_zscaler`
```

url	result
http://ztuw5bvuuapzdfya.klimbim.pl/home	[{"url":"ztuw5bvuuapzdfya.klimbim.pl/home","urlClassificationsWi ecurityAlert":[],"urlClassifications":["MISCELLANEOUS_OR_UNKNOW N"]}]

Zscaler delivers threat prevention, access control and data protection from the cloud. The integration allows the analyst to focus on hunting for threats across using correlated data across the platform, all from within a LogicHub playbook, thereby automating security operations workflows and significantly reducing the time and effort required to perform proactive hunting.

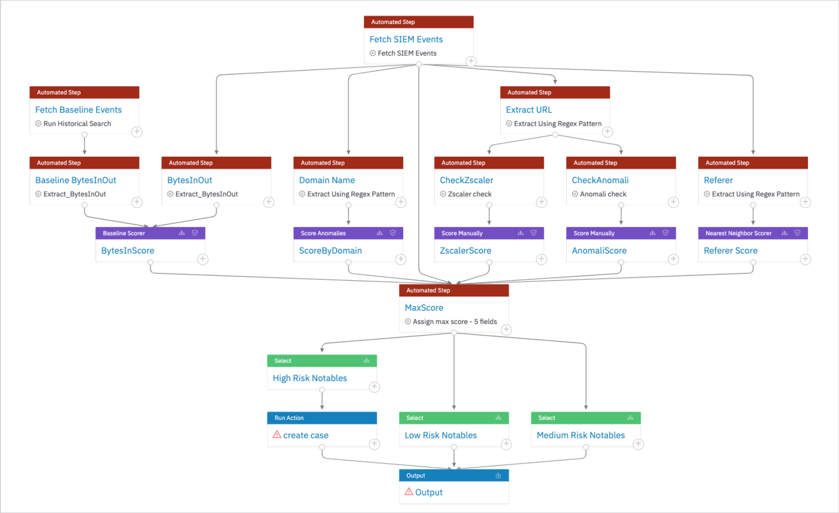
Benefits

- Reduce your alert false positives by 95% and reduce MTTR by 10x by using advanced analytics and machine learning.
- Interactive case management prioritizes the critical events for effective investigations and fast resolutions.
- Accelerate security operations workflows by automating manual tasks and provide deep visibility into operational KPIs.

INCIDENT RESPONSE AUTOMATION - ALERT TRIAGE

Today's SOCs must overcome many challenges to protect the organizations they serve. Among the top challenges are an increasing volume of alerts, an increasing number of products, tools and technologies in use in the enterprises, and an overstretched SOC team. Adversaries have grown in sophistication, requiring more detailed threat detection and complicated analysis steps. These challenges result in increased time to resolution for incidents, missed detection, and alerts that are ignored due to high volume and lack of time.

The LogicHub solution automates the processes that make up the security analyst's playbook, including collecting the right data by using Zscaler actions (malware analysis, sandbox verdict results, reputation checks, ...), making sense of the data, generating decisions, and taking action when a decision has been made or a conclusion has been reached. The central component is analysis and correlation, but equally important are the mechanisms to integrate with other systems to bring in data, classify the results, identify those that require action, and take action as needed by leveraging the APIs of Zscaler and other security tools.



The LogicHub SOAR+ approach to SOC automation focuses on enabling the decision making in alert triage by mimicking the real workflow of analysts. The branching logic and data analysis, such as Zscaler actions, that LogicHub offers is essential to effective alert triage.

LogicHub SOAR+ proactively triages alerts and only creates a case when there is a true positive and assures analysts are examining attention worthy incidents.

About Zscaler

Zscaler (NASDAQ: ZS) enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access™ and Zscaler Private Access™, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100 percent cloud-delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances are unable to match. Used in more than 185 countries, Zscaler operates a multi-tenant distributed cloud security platform, protecting thousands of customers from cyberattacks and data loss. Learn more at zscaler.com or follow us on Twitter @zscaler.

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. Learn more at logichub.com and follow us on Twitter @logichubhq and LinkedIn https://www.linkedin.com/company/logichub.

a: 301 N Whisman Rd., Mountain View, CA 94043
w: www.logichub.com
e: info@logichub.com
p: (650) 262-3756