Increasing Risk and Demand

Organizations ready for a SOAR platform have a plethora of disjointed tools that generate an overwhelming number of alerts that are difficult to make sense of and piece together. It is difficult to connect the relationship of different alerts but also assign priority and remediate them. Analysts are crushed by the overwhelming number of alerts, false positives, and menial tasks. This can often lead to missed security incidents and inefficiency.

Zscaler & Siemplify Security Operations

Zscaler and the Siemplify Security Operations Suite form a solution allowing SOC teams to prioritize and automate the remediation of security threats.

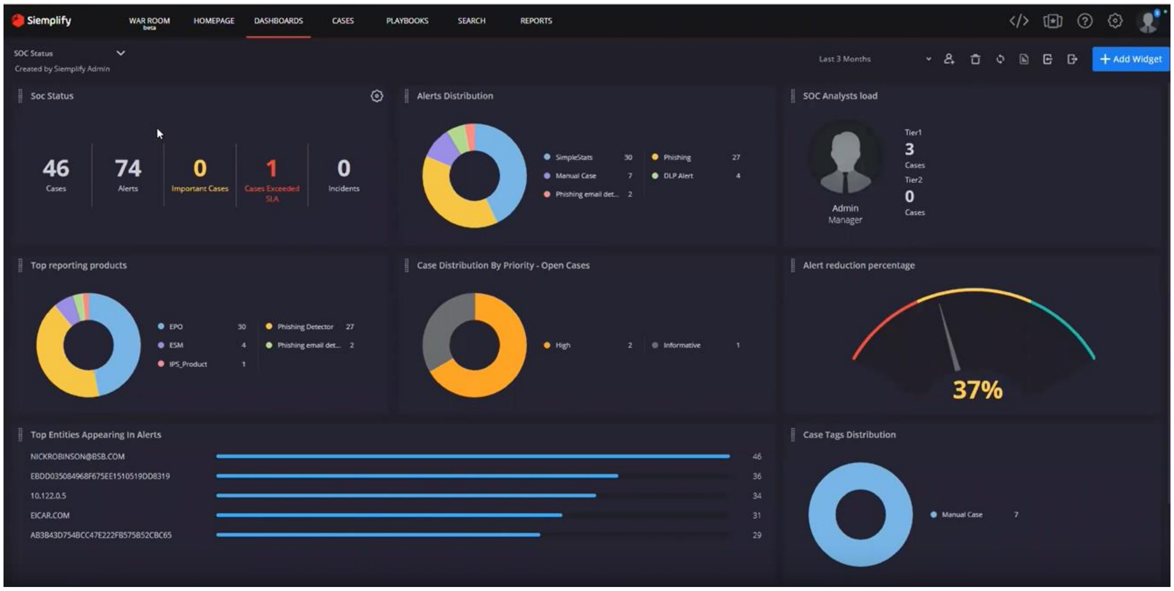
Zscaler Internet Access delivers a security stack as a service from the cloud providing full content analysis of all traffic including SSL communications and trusted content, across all ports and protocols. Zscaler can help deliver airtight internet security with Cloud Firewall, Cloud Sandbox, Content and URL filtering, Data Loss Prevention (DLP) and CASB. The Zscaler service provides unprecedented visibility of user, device and network activity. Zscaler delivers 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.

Siemplify Security Operations Platform is an intuitive, holistic workbench that makes security operations smarter and more efficient and effective. Siemplify combines security orchestration, automation and response (SOAR) with context-driven case management, investigation, and machine learning to make analysts more productive, security engineers more effective, and managers more informed about SOC performance. Unlike other SOAR products that focus solely on automation or other limited use cases, Siemplify provides a complete SOC workbench that delivers a single, intuitive experience that analysts love. The powerful context-driven engine allows security engineers to customize for any use case.

Security teams can use Siemplify's playbook builder to standardize their approach to security alerts. With the playbook builder, Siemplify users can combine API calls of all their tools, including Zscaler, to create the entire set of operational procedures. Siemplify's unique **Threat Centric** approach to grouping alerts in its' platform not only reduces noise, but also creates a cohesive story in a messy amalgamation of security tools.

INTEGRATION BENEFITS

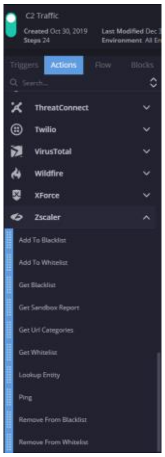
- The Siemplify Platform can edit Zscaler's white and black lists based on data correlated from other security tools
- Siemplify leverages Zscaler Cloud Sandbox to guide the execution of security playbooks.
- Zscaler Threat results are integrated into the investigative process to add context to security cases.
- Reduce repetitive tasks, automatically close noisy, low level cases to increase efficiency

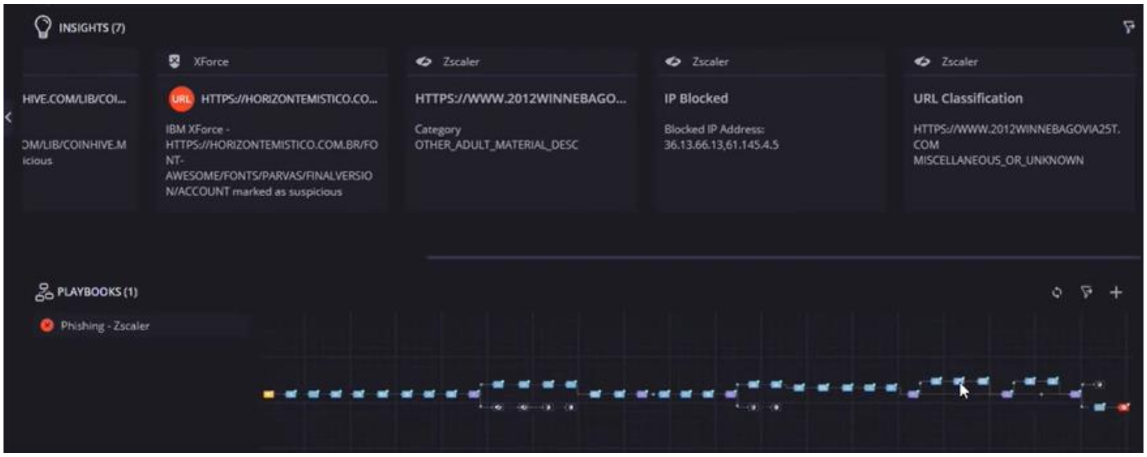


Zscaler Integration

The Siemplify platform is powered by API calls into other 3rd party security solutions such as Zscaler. Siemplify can connect actions from different platforms to increase operational efficiency and standardize best practices. The Siemplify platform leverages Zscaler's networking security, threat data, and sandboxing capabilities. Siemplify has 200+ integrations enabling management from a single holistic workbench.

Zscaler's threat indicators are combined to enrich context to a group of alerts in order to categorize the nature of a threat. Zscaler sandboxing results can further enhance the potential malicious nature of related entities inside of a case. Once the case has been investigated, Siemplify can make API calls to Zscaler's to update blocklists that are confirmed to be malicious in nature.





HIVE.COM/LIB/COI...
OM/LIB/COINHIVE.M
icious

URL HTTPS://HORIZONTEMISTICO.CO...
IBM XForce - HTTPS://HORIZONTEMISTICO.COM.BR/FONT-AWESOME/FONTS/PARVAS/FINALVERSION/ACCOUNT marked as suspicious

HTTPS://WWW.2012WINNEBAGO...
Category
OTHER_ADULT_MATERIAL_DESC

IP Blocked
Blocked IP Address:
36.13.66.13,61.145.4.5

URL Classification
HTTPS://WWW.2012WINNEBAGOVIA25T.COM
MISCELLANEOUS_OR_UNKNOWN

About Siemplify
Siemplify, the leading independent security orchestration, automation and response (SOAR) provider, is redefining security operations for enterprises and MSSPs worldwide. The Siemplify platform is an intuitive workbench that enables security teams to manage their operations from end to end, respond to cyberthreats with speed and precision, and get smarter with every analyst interaction. Visit us at siemplify.co or follow us on Twitter at @Siemplify

About Zscaler
Zscaler enables the world's leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its 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% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match.