Synack App for Splunk

Improving Splunk security operations with premier security testing from Synack

Synack App for Splunk (via Splunkbase) helps our customers painlessly integrate Synack's diverse security researcher backed offensive testing data right into data-rich Splunk environments, reports, queries, and dashboards.

Why Integrate Splunk and Synack?

The Synack Premier Security Testing Platform combines the best of human intelligence augmented with machine intelligence to offer more effectiveness and efficiency than traditional alternatives. When you integrate Synack inside Splunk's dashboard, you can understand and analyze your Synack data alongside the rest of your Splunk-resident security and IT data. Merging Synack offensive security testing results together with the rest of your security data within Splunk will help you view your security more holistically and optimize your security efforts. You can get the complete picture without the extra work; when you no longer need to chase down data from different offensive and defensive security teams (e.g.Red versus Blue) and projects from around your organization, you save effort and time. Now, for example, you can compare vulnerability data from multiple Synack infrastructure and application testing programs without hunting the network admin or application owners.

This can vastly enhance the capabilities within the Security Operations Center (SoC) and enable faster response to incidents or threats to apps or infrastructure. Custom reports and analytics allow users to see the holistic picture with preferred metrics and reporting for any audience. The possibilities are almost limitless, but the major use cases we hear from our customers for Splunk/Synack integration are:

- **Threat hunting:** Understand threat lifecycles by using Synack vulnerability data to seek active and historical threats
- **Incident management:** Have complete security information available for security incident management, including if an incident relates to a Synack tested asset
- **Containment:** Prevent exploits from spreading by correlating exploitable vulnerabilities and locations with web logs to determine if there are other locations where a Synack-found vulnerability can be re-exploited
- **Intrusion detection and protection:** Correlate exploitable vulnerabilities and locations with network traffic to define new rules for detection and prevention as part of your remediation or Synack-assisted patch verification
- **Improved scanner efficiency:** Correlate exploitable vulnerabilities with scanner data (such as WhiteHat or Qualys) for better scanner efficacy (such as activating scripts or plugins only for targets with true, Synack-verified, exploitable weaknesses)
- **Threat intel:** Build out predictive patterns to improve security by correlating exploitable vulnerabilities and locations with other threat intel data

How it works

Utilizing the Splunk integration comes with an out-of-thebox Synack dashboard for your Splunk instance. You can use Synack's provided dashboard or you can also build your own. During testing, your vulnerabilities are displayed within the Splunk dashboard as they are found and triaged by Synack. You can then disseminate and assign those vulnerabilities to members of your team and track their progress along the way, still within Splunk.

All Synack security data is searchable at a granular level using normal Splunk queries. You can easily access a comprehensive history of vulnerabilities to help you look for similarities, root causes, and where improvements have been made. Synack data can be connected with other sources of Splunk data to bolster your security efforts further, such as threat hunting and malware analysis.

Specific Synack fields available in Splunk

FIELD	USAGE
Vulnerability Description	Name
CVSS Score/ Severity	0–10 score indicating severity of vulnerability/ CVSS severity classification based on the score
Impact	Assessment of impact of vulnerability on an organization, written by reporter/ Synack
Exploitable location	Where the exploit was proven to exist
Steps to reproduce	Details on how to reproduce the exploit
Recommended Fix	Suggestion on how to remediate the vulnerability
Patch Verification	Status of patch verification (for users of this free Synack service)

This rich set of data gives Splunk users many options on how to enrich their existing queries and dashboards with the vulnerability data only Synack can provide.

What about security? All processed data passes securely and in encrypted form between Splunk and Synack.

Getting started with Synack for Splunk

The Synack App for Splunk is completely free, quick, and simple. It is a plug-in-and-play integration that seamlessly installs and gets to work within a matter of minutes. You can integrate Synack with both Splunk Cloud and Splunk On-Premises solutions.

It is available now on Splunkbase. Current Synack customers should also contact their Synack Program Manager to get started. If you would like to learn more about premier security testing or would like further information, feel free to visit our help center or contact a Synack representative.