Splunk Add-on for Investigate.

Many security products provide visibility into what's happening on your own network. But how do you see what's happening on the internet, beyond your perimeter? That's where attackers are staging infrastructure in preparation for their next attack.

With the Splunk Add-on for Cisco Umbrella Investigate, you can automatically enrich security events inside Splunk with Cisco's intelligence on domains, IPs, and networks across the internet.

By leveraging Investigate's threat intelligence from within Splunk Enterprise Security, you can gain more context about a domain, IP, or ASN related to the event, allowing you to make faster, more informed decisions when responding to critical incidents and researching potential threats.

Key capabilities of the Investigate Add-on

Threat intelligence add-on in Splunkbase
Add intelligence about the relationships between domains, IPs, ASNs, and file hashes inside Splunk, helping security analysts get the most complete view of an attacker's internet infrastructure.

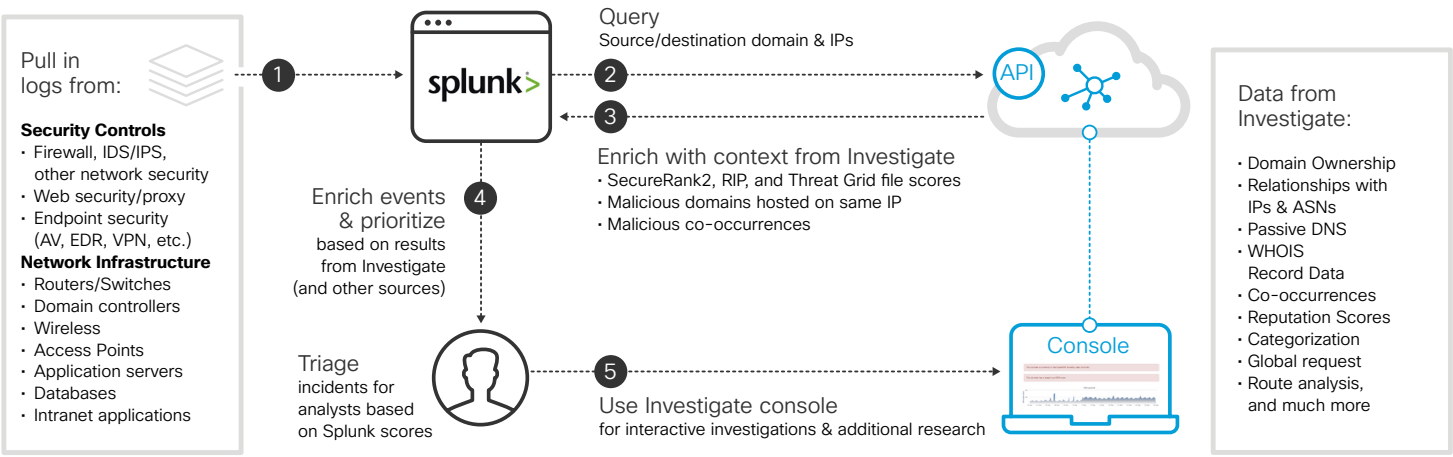
Better prioritize incident response
To properly triage incidents, security teams need to get accurate and relevant information quickly. Investigate's unique view of the internet enriches your security event data with real-time context about malicious domains, IPs, and networks to help better prioritize investigations and incident response.

See what connections you've been missing
Kick start investigations by uncovering valuable connections commonly overlooked such as passive DNS, domain ownership, co-occurrences, related domains, geolocation, categorization, blocked requests and reputation scores.

Speed up investigations
By automatically populating security events with intelligence from Investigate, security teams have more context related to the event and can make faster, more informed decisions during investigations – versus manually going to and correlating data from multiple sources.

Benefits of Investigate

- **Internet-wide visibility**
  Investigate connects the dots between attackers' infrastructure, which helps attribute domains to specific attacks and malicious activity.
- **Predictive intelligence**
  Our statistical models accurately identify malicious domains, IPs, and ASNs across the internet, and even predict where future attacks may be staged.
- **All of the information you need in a single source**
  Including real-time and historical information about the domain ownership, relationships with IPs, co-occurrences, reputation, global request and route analysis, and much more.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)