Anomali Adaptive Response App for Splunk

Anomali supports the Splunk Adaptive Response Initiative, delivering rich context regarding IOCs, actors and campaigns seamlessly within the Splunk interface.

- Anomali integrates threat intelligence from the following:
  - Anomali Labs
  - 3rd party sources
  - Open source intelligence
  - Anomali community

- Anomali delivers IOC feeds to Splunk to identify matches against customer log events.
- Splunk displays the matches in the Incident Report view.
- An individual match indicates a single IOC was detected.

However, that specific IOC is likely associated with an actor and campaign, for which hundreds of other IOCs may be related.

- Anomali maintains this relationship information
- We see the IOC is a single datapoint in a much larger security threat
- To get full context of the potential breach we need to search for all related IOCs

With the Anomali integration and Splunk Adaptive Response, users can perform this analysis with a single click, without ever leaving the Splunk console. Simply select Anomali Check Indicator.

The Anomali App for Splunk then presents all associated IOCs, in the timeline, with categorization for each step of the Kill Chain model. In one single view, organizations can see the extent of a potential breach that started with a single IOC detection.
Anomali Adaptive Response App for Splunk

With the Anomali integration with Splunk Adaptive Response users can perform this analysis with a single click, and without ever leaving the Splunk console. Simply select Anomali Check Indicator.

The Anomali app for Splunk then presents all associated IOCs, in the timeline, with categorization for each step of the Kill Chain model. In one single view organizations can see the extent of a potential breach that started with a single IOC detection.

About Anomali

Anomali™ is the pioneer of an enterprise class threat intelligence platform, combining comprehensive threat data collection, prioritization, and analytics with secure collaboration in a vetted community. Offering the broadest enterprise security infrastructure integration available, the ThreatStream platform enables organizations to proactively identify and combat cyber threats targeting their operations.