Overview

IronDefense, IronNet’s flagship product, delivers scalable behavioral analytics and integrated hunt to a variety of public and private sector enterprises. Designed by national security analysts and top intelligence data scientists, IronDefense provides machine-speed detection at scale to identify advanced threats that are often missed by existing commercial cybersecurity solutions. IronNet’s collective defense platform, IronDome, shares these behavior-based detections with communities of similar risk profiles to create a defensive fabric across companies, sectors, and nations.

The IronDefense App for Splunk enables security teams to manage alerts more efficiently by integrating teams, processes, and tools together to triage and investigate suspicious network activity.

How It Works

The IronDefense App for Splunk enables IronNet customers to stream alert, event, and IronDome data from IronDefense into their own Splunk instance. Customers are then able to see anomalous network activity detected by IronDefense and enriched by IronDome using the Splunk interface. If the user wants to view results in IronVue for further investigation and hunt, he or she can pivot from the Splunk dashboard to IronVue with one click. The IronDefense App for Splunk is also integrated to allow customers to report their assessments of IronDefense discoveries, enabling collective defense and analytic improvements by the IronNet team.

In IronDefense, an alert is the result of multiple events that share similar behavior or Indicators of Compromise (IoC), such as the same malicious domain. You may have one event that produces an alert or 10,000 events that produce one alert. Compiling all shared event data into one alert reduces the amount of alerts an analyst is required to triage. To minimize Splunk data volumes, by default, only events and alerts above a severity level of 500 are sent to Splunk. This threshold can be adjusted from 0 to 1,000 using the Splunk user interface to customize the desired volume of alerts sent to Splunk.
Core Features

The IronDefense App for Splunk enables a variety of new and unique means of consuming and visualizing the results from IronDefense. IronNet customers can submit an alert status, provide analyst ratings, add a comment to an alert, optionally share data with IronDome, create a report, and more, all within the Splunk user interface. Key capabilities are described in further detail below.

Seamless Integration with IronVue

Each IronDefense event includes a unique URL that enables security teams to quickly pivot into IronVue, IronDefense’s user interface, for deep-dive investigation and triage of detected anomalies. Security teams can quickly go from dashboard information to a thorough investigation, including full PCAP analysis, with a single click.

Insights from and Contributions to IronDome

Integration of the IronDefense App for Splunk with IronDefense’s IronAPI allows IronNet customers who subscribe to IronDome to send their analysis of IronDefense alerts to IronDome. Ingest and display of IronDome notifications in the Splunk app allow IronNet customers greater insight into how their enterprise environment’s alerts correlate to alerts from within their sector, thus enabling faster triage and more proactive defense.

Customizable Dashboard

Splunk users can leverage the IronDefense App to customize reports and dashboards of the results from their IronDefense solution. The IronDefense App comes with a default dashboard that aggregates key threat detection metrics into a summary view for reporting purposes. As with all Splunk dashboards, the IronDefense dashboard is customizable and can be modified to meet the operational requirements of your network and security teams.

Custom Reports

IronDefense events include data that does not map to the Splunk Alert Common Information Model (CIM). This additional data is available for custom report generation within the Splunk interface through building custom queries. Customers can organize information using the fields passed from IronDefense into Splunk and visualize information in a variety of ways to meet reporting needs.

Where to Download the App