SOLUTION BRIEF

IronNet and Splunk SOAR

Reduce the impact of cyber attacks through advanced threat detection and automated response

Why we work better **together**

SOLUTION BENEFITS AT A GLANCE

Visibility across the threat landscape

Receive real-time collective threat intelligence, contextual information on new threats, and higher-order analysis of anomalies correlated across communities.

Increase effectiveness of existing SOC resources

Streamline and automate operations to eliminate alert fatigue with curated threat ranking, integrated security tools, and the automation of manual tasks.

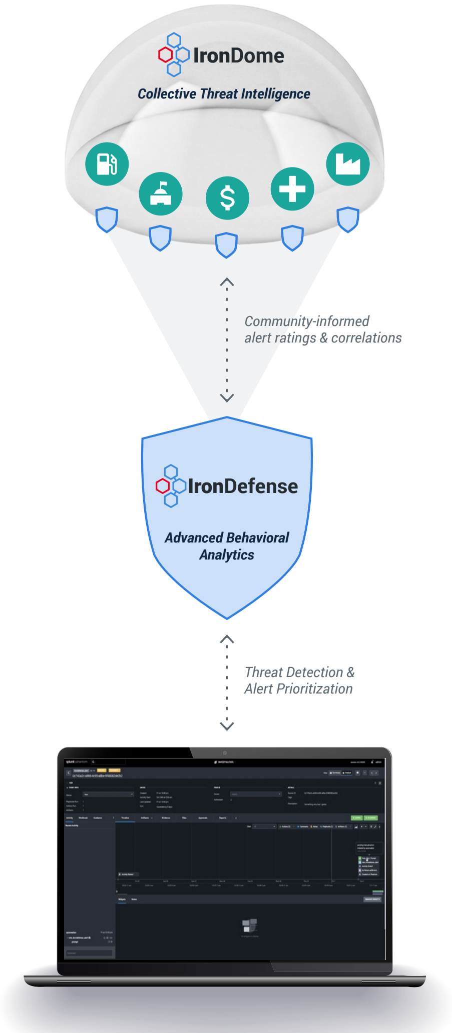
Reduce the impact of an attack

Lessen business repercussions and security risk by detecting threats earlier in the attack lifecycle, protecting against malicious activity before it invades the network.

Designed by national security analysts and top intelligence data scientists, IronNet's scalable Network Detection and Response (NDR) solution and Collective Defense platform provide visibility across communities of enterprises. This approach allows peers to identify advanced threats often missed by existing commercial cybersecurity solutions. IronDefense, IronNet's NDR solution, integrates with Splunk SOAR's security orchestration, automation, and response (SOAR) platform to eliminate alert backlogs and maximize the incident response capabilities of overburdened and understaffed security operations centers (SOC). The IronDefense App for Splunk SOAR enables more advanced threat detection, higher accuracy prioritization, faster mitigation, and proactive protection. IronDefense uses advanced behavioral analytics and collective threat intelligence to find unknown threats while weeding out false positives. Splunk SOAR then automates operational SOC workflows and integrates security tools for seamless threat hunting. Together with IronNet's IronDome Collective Defense solution, analysts have complete visibility into the threat landscape, delivering real-time, community-driven collective threat intelligence insights from peer enterprise SOCs.

Business challenge

Cyber defense teams are isolated, using conventional tools that often miss advanced or unknown malicious threats. These gaps increase the burden of already overworked security operations teams. There is a better way to defend. A collaborative, real-time, behavioral detection approach enables enterprises to optimize their existing cybersecurity investments, reduce the impact of an attack, and gain broader visibility across their business ecosystems.


IronDome
Collective Threat Intelligence
Community-informed alert ratings & correlations
IronDefense
Advanced Behavioral Analytics
Threat Detection & Alert Prioritization

Splunk SOAR and IronDefense work together to enhance the speed and efficiency of detection, triage and response.

How it works

When IronDefense data is ingested into Splunk SOAR, it provides users the ability to take proactive measures on next-generation firewall (NGFW) and endpoint detection and response (EDR) tools to prevent further attacks. These measures include creating blacklists to alert on or block additional malicious activity and quarantining devices. Employing strategies like these permits Splunk SOAR users to expand the utility of IronDefense and increase the ROI of other products integrated with Splunk SOAR. This data ingest also helps drive analyst workflow automation, such as IT service management (ITSM) ticket creation. By leveraging the IronDefense Plugin for Splunk SOAR, users can eliminate the manual and tedious process of creating tickets to initiate remediation efforts to allow SOC analysts to focus their attention on analyzing alerts.

The IronDefense Plugin for Splunk SOAR also enables data upload and sharing. Users can share analyst assessments with IronDefense to enable Collective Defense via the IronDome platform. Events, alerts, and IronDome collective threat intelligence information are all available through the IronDefense Plugin for Splunk SOAR, which means other participants in IronDome will be able to use the information to improve their security posture. Users can also update existing NGFW and EDR alert workbooks to submit observed malicious Indicators of Compromise (IoC) to IronDefense to look for correlations across the IronDome community. By sharing these discoveries with IronDome, Splunk SOAR plugin users are able to understand the trends of attackers by receiving information on whether the same malicious activity has been observed by other IronDome participants.

Contact Us

To learn more about the IronDefense Splunk SOAR integration, visit IronNet.com or contact us at info@IronNet.com.

ABOUT IRONNET

IronNet is a global cybersecurity leader that is revolutionizing how organizations secure their enterprises by delivering the first-ever Collective Defense platform operating at scale. Our solutions leverage our unique offensive and defensive cyber experience to deliver advanced behavioral analysis and collective intelligence to detect known and unknown threats.