Splunk and IronNet

Changing the Game in Cybersecurity by Combining Best-in-Class SIEM and NDR to Deliver Actionable Collective Defense

Complementary Capabilities

SIEM and NDR are naturally complementary solutions. Together, Splunk's best-in-class ability to serve as the enterprise's security nerve center and IronNet's market-leading advanced behavioral analytics and Collective Defense capabilities enhance threat detection and response. Analysts can identify and remediate not just known threats but also new, novel threats and campaigns identified by combined custom correlation capabilities.

Multiple Capabilities, Single Pane of Glass

Splunk customers can leverage immediate access to the critical data they need to drive advanced threat hunting, triage, and remediation in a single pane of glass. They can take advantage of novel data collection and behavioral analytics from IronNet's NDR platform, IronDefense, and contextual data and actionable threat results from Splunk Enterprise Security. This integration fits into their existing workflow to accelerate their ability to evaluate and stop potential threats.

Delivering Collective Defense in Splunk

Bringing threat correlations from across multiple companies and industries into Splunk Enterprise Security from the IronDome Collective Defense platform adds value and visibility. In addition to enhancing new and novel threat detection, Splunk customers can leverage IronNet's ability to securely pass information across the public-private sector divide. This capability is combined with Splunk's ability to visualize the details of dynamic, multi-step attacks and identify the relationship between various events.

Seamless, Rapid Investigation and Response

IronNet's integration with both Splunk Enterprise Security and Splunk Phantom enables rapid investigation and response. Customers can seamlessly leverage our combined advanced detection and correlation

©2021 IronNet Cybersecurity Inc. All Rights Reserved

capabilities. They can efficiently conduct multi-step investigations that leverage each platform's supervised and unsupervised machine learning (ML) capabilities. This is enhanced by our combined smart automation and visibility capabilities to quickly respond to threats.

Combining Analysis and Action at Scale

With IronNet, Splunk customers large and small will be able to better secure their environments. Customers are empowered by the combination of IronNet's network analytic and Collective Defense correlations with Splunk Enterprise's advanced artificial intelligence (AI)/ML capabilities and user behavior analytics visualized in the Splunk Enterprise Security system. With this situational awareness, they can take action through Splunk Phantom's SOAR platform.

Generating Real Value for Different End Users

The integration of IronNet's advanced behavioral detections within an enterprise and the correlation of resulting data across multiple organizations into Splunk's data platform makes both Splunk Enterprise Security and Splunk Phantom more valuable. The combination will help drive additional Splunk platform adoption among security operations center analysts, threat hunters, incident response teams, and senior executives.

Driving Collective Defense

By leveraging IronDome's Collective Defense capabilities, security teams using Splunk can identify and defend against new and unknown threats by correlating potential threats across multiple companies and industries at scale and speed.

Crowdsourcing Intelligence and Decisions

IronNet's integration helps Splunk customers drastically shorten the time between detection of a potential threat and remediation. By crowdsourcing threat intelligence across multiple companies and industries and collaborating on threat analysis and remediation dynamically and in real-time, IronNet's integration provides the data needed to make timely decisions.

Securely Bridging the Public-Private Divide

The IronDome platform is uniquely positioned to deliver the ability to create shared situational awareness across the public-private sector divide on behalf of Splunk customers. This first-ever Collective Defense platform is possible through seamless threat sharing and correlation capabilities, as well as IronNet's deep, trusted relationships in the public and private sectors. All shared data is carefully protected to provide anonymity.

Changing the Game Together

The combination of Splunk's and IronNet's capabilities promise to deliver Splunk customers the ability to detect threats capable of evading traditional cyber tools. They also have access to the industry's only real-time threat visibility, sharing, and collaboration solution for on-prem, cloud, and hybrid environments. Together, IronNet and Splunk are fundamentally changing the game in modern cybersecurity.

©2021 IronNet Cybersecurity Inc. All Rights Reserved