NORSE

PRODUCT DATA SHEET

Using Norse Threat Intelligence with HP ArcSight

Integrating advanced attack intelligence with internal security events to prevent breaches

Use Cases

- Proactive blocking or alerting on high risk connections for advanced malware and targeted attack detection
- Risk-based threat prioritization for improved incident response
- Post-attack forensics to quickly detect and mitigate compromises reducing risk of breach

Integration Specifics

- Combined with Norse attack intelligence, Arcsight provides out-of-the-box functionality and multiple third party connectors that enable active commands for dynamic actions such as triage and incident response, or direct, automated intervention
- Norse supports the CEF format natively to provide rich context to threats
- The integration provides the ability to drill in to a particular event to give instant access the Norse DarkViking portal with full context
- The threat details conform to the CEF format which lets you use your existing workflows and infrastructure with no additional spend

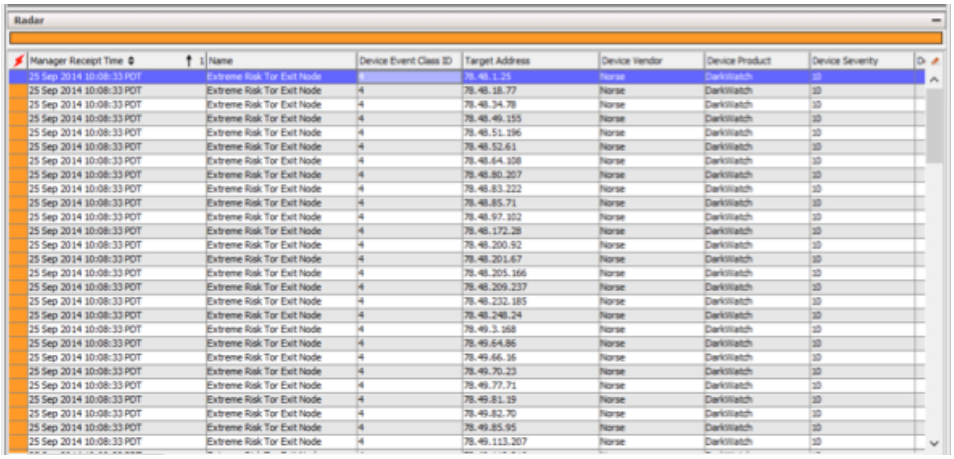
Norse's live attack intelligence combined with HP's ArcSight SIEM dramatically improves customers' ability to proactively detect and prevent the initiation or expansion of breaches. Norse attack intelligence provides contextual, risk-weighted, and continuously updated threat intelligence collected from its global infrastructure, including anonymous darknets and the deep web, from where many bad actors operate. The integration adds critical external context to internal security events enabling rapid advanced threat detection and risk-based prioritization of threats and incident response, and reducing the time for analysts to get from data to insight to resolution.

Norse provides threat intelligence via two complementary methods:

Darklist, a list of the top 3-5 million highest risk IPs on the Internet with basic context. Darklist integrates with ArcSight through a connector that supports the CEF format and connects natively to the ArcSight console. Darklist includes a 0-100 risk score for each IP, the risk category (such as "botnet" or "Tor proxy") to provide context to the score, and highly accurate geolocation.

DarkViking, a real-time lookup-based solution that provides live data, deeper threat context, and years of history for individual IP addresses. Norse users have access to the DarkViking portal and API which lets them retrieve detailed data about any IP including full context and historical information.

Both of these methods are integrated with ArcSight to provide instant correlation and full investigative capabilities for any IP or URL.



Norse threat intelligence integrates with ArcSight to provide critical context about external threats and how they relate to internal events.

Silicon Valley
1825 South Grant Street, Suite 635
San Mateo, CA 94402 | 650.513.2881

Saint Louis
101 South Hanley Road, Suite 1300
St. Louis, MO 63105 | 314.480.6450

ABOUT NORSE

Norse is the global leader in live attack intelligence. Norse delivers continuously-updated and unique Internet and darknet intel that helps organizations detect and block attacks that other systems miss. The superior Norse DarkMatter™ platform detects new threats and tags nascent hazards long before they're spotted by traditional "threat intelligence" tools. Norse's globally distributed "distant early warning" grid of millions of sensors, honeypots, crawlers and agents deliver unique visibility into the Internet – especially the darknets, where bad actors operate. The Norse DarkMatter™ network processes hundreds of terabytes daily and computes over 1,500 distinct risk factors, live, for millions of IP addresses every day. Norse products tightly integrate with popular SIEM, IPS and next-generation Firewall products to dramatically improve the performance, catch-rate and security return-on-investment of your existing infrastructure.