NETWITNESS

SOLUTION BRIEF

NetWitness Orchestrator for Threat Intelligence Analysis

Stay proactive with the ability to quickly prioritize threats and understand how they impact your organization

Security organizations must contend with a rapidly growing number of threats and incidents. Without threat intelligence it is nearly impossible to determine which indicators of compromise will have the greater negative impact on the organization. NetWitness Orchestrator leverages threat intelligence to automate tasks and speed decision making. Other benefits include:

Determine Indicators of Compromise (IOC) relevancy to your organization

Map indicators relevant to your organization through NetWitness Orchestrator with features such as tagging and customizable attributes. Our Collective Analytics Layer accelerates the time to understanding what IOC's are relevant by crowdsourcing intelligence data.

Gather artifacts from internal cases and incidents to turn into intel

By encouraging information-sharing across your security teams, you'll establish a feedback loop that allows for increased threat intelligence insight and relevance to your organization. NetWitness Orchestrator supports various integration mechanisms like a flexible REST API, easy import of even unstructured data, and an easy-to-use playbooks interface.

Disseminate information to other teams and tools

Get relevant and actionable insights from intelligence sources within NetWitness Orchestrator. Then, act by providing those insights to the necessary people and technologies.

Correlate data to understand relationships between indicators

Correlating data to understand relationships between indicators is critical for threat intel analysts. With Graph View, easily pivot from one indicator to another to quickly understand relative information and build a fuller picture of things like specific threat actors or vulnerabilities.

Aggregate intelligence to achieve actionable insights

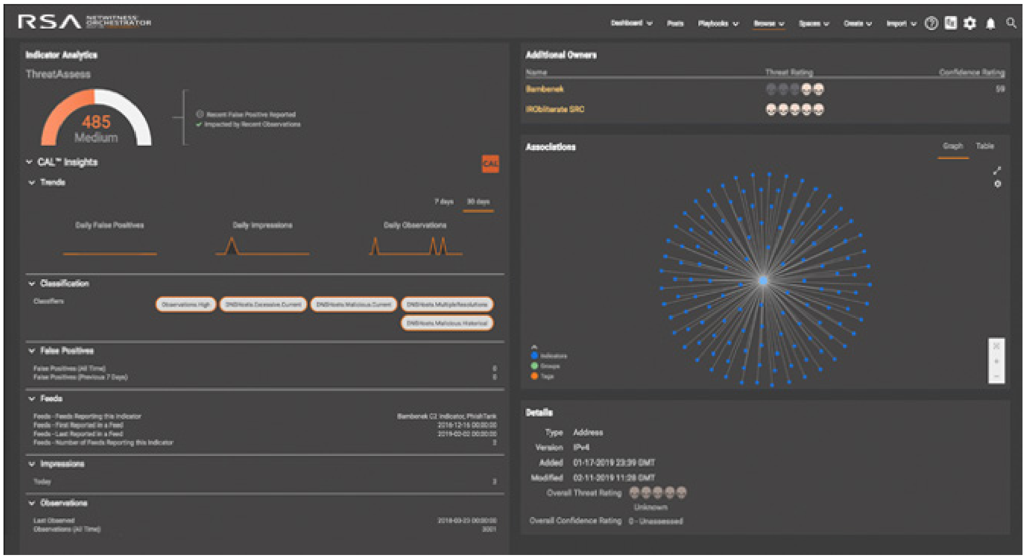
Within NetWitness Orchestrator, you can aggregate all sources of intel, such as data feeds and technology blogs, as well as log, endpoint and network data to identify correlations and achieve actionable insights.

Flexible data model to support multiple analysis methodologies

Whether you use the Diamond Model of Intrusion Analysis, Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK, or something entirely different, ThreatConnect will support you. You're able to pivot between indicators and groups to spot patterns and tag indicators for easy organization and analysis.

Strengthen threat hunting efforts with increased visibility

NetWitness Orchestrator serves as a threat intel aggregator and repository, housing all indicators and intelligence collected from external data feeds, the Connected Analytics Layer, and other internal technology solutions. This additional insight automatically applies awareness and understanding of the external threat environment, adding an important piece of the puzzle to your threat hunting efforts.



Indicator Analytics

ThreatAssess

Recent False Positive Reported

✓ Impacted by Recent Observations

CAL™ Insights

Trends

Classification

Classifiers

False Positives

False Positives (All Time)	0
False Positives (Previous 7 Days)	0

Feeds

Feeds - Feeds Reporting this Indicator	Bambenek C2 Indicator, PhishTank
Feeds - First Reported in a Feed	2016-12-16 00:00:00
Feeds - Last Reported in a Feed	2019-02-02 00:00:00
Feeds - Number of Feeds Reporting this Indicator	2

Impressions

Today	3

Observations

Last Observed	2018-03-23 00:00:00
Observations (All Time)	3001

Additional Owners

Name	Threat Rating	Confidence Rating
Bambenek		59
IRObliterate SRC		

Associations

Details

Type	Address
Version	IPv4
Added	01-17-2019 23:39 GMT
Modified	02-11-2019 11:28 GMT
Overall Threat Rating	Unknown
Overall Confidence Rating	0 - Unassessed

Integrates with your security defense arsenal

Broad visibility across the NetWitness Platform and your other security systems allows for indicators of malicious activity to be sent to NetWitness Orchestrator, cross-checked with known bad indicators, and determine proper response efforts, both manual and automatic, to be taken base don the findings.

NetWitness Orchestrator in action

Threat hunting

Security teams are inundated with triage and response efforts, oftentimes making proactive security exercises like threat hunting take a back seat to responsive problem investigation. With NetWitness Orchestrator you can make threat hunting a regular exercise to proactively identify security vulnerabilities. Working with the rest of the NetWitness Platform security analysts can investigate anomalies and gaps that lead to business impacting threats. Now investigations that took days or weeks can be done in a matter of minutes.

About NetWitness

NetWitness, an RSA® Business, provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats. For more information, go to netwitness.com.

NETWITNESS
An RSA Business

©2021 RSA Security LLC or its affiliates. All rights reserved. RSA, the RSA logo and NetWitness are registered trademarks or trademarks of RSA Security LLC or its affiliates in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 6/21 Solution Brief W473201