NetWitness® Incident Response Services

Enabling readiness, response & resilience

Executive summary

Technical forensic analysis services

The NetWitness global Incident Response Practice provides a portfolio of services for organizations that need rapid access to technical security expertise to assist with identifying and remediating cybersecurity attacks. Incident response retainers, proactive incident discovery/compromise assessment and knowledge transfer services are also provided. These services enable organizations to conduct proactive hunting and get ahead of the threat before a breach occurs.

Early detection and rapid response are the most critical capabilities for targeted attack defense. Many reports indicate that well-resourced adversaries consistently bypass traditional security defenses. The issue is less about being able to keep the bad guys out, which is increasingly hard to do on an ongoing basis. It's more about detecting and responding to them as soon as they are in. Once detected, a rapid response is needed to mitigate broader compromise and prevent the attackers from achieving their objectives. The NetWitness Incident Response Practice enables organizations to respond to security incidents without having to accept the inevitability of loss.

Analytic intelligence

The key to early detection and rapid response

Attackers leave clues. The question is whether the victim is able to detect these clues and respond rapidly. The NetWitness global team of incident response professionals are experts at detecting such clues quickly enough for organizations to get ahead of the threat.

As signature-and perimeter-based defenses have proven inadequate, security professionals need tactical insight into activities taking place on their systems. Through the capture and analysis of network and end-point data using the award-winning NetWitness® Platform for packet capture and anomaly detection, NetWitness incident response consultants can proactively gather analytic intelligence, review the overall state of the environment and identify areas of concern, including:

- Anomalous activities on network and host systems
- Detection and analysis of adversary tools, tactics and procedures
- Identification of the assets that may have been targeted

NetWitness's capabilities in incident response include access to threat intelligence relating to current attacks and campaigns. This also includes the ability to assess the scope of adversary activities and make informed decisions in a timely manner. With the preservation of potential sources of evidence and visibility and context across the enterprise, organizations can develop an intelligence-driven program of their own for incident management.

The odds to date have consistently been stacked in favor of the adversary, especially when defending against nation-state attackers. But by bringing the right expertise to the table, organizations can detect attacks faster and much earlier in the incident lifecycle. This puts them in a much better position to protect themselves in a complicated and unpredictable threat environment, which has ranged from cybercrime (e.g., ransomware) to cyber espionage (e.g., intellectual property theft), and more recently, even to growing concerns about cyber terrorism.

IR services portfolio

Proactive and rapid response services

Working with the NetWitness Incident Response team, organizations can benefit from the expertise gained through a diverse range of global engagements. The service offerings available include:

- **IR retainers** — NetWitness offers a portfolio of retainer services which provide for the proactive engagement of our IR team for surge access to technical forensics resources provided under a variety of optional and accelerated service levels. As time is of the essence in preventing a breach, Service Level Objectives include response to incidents within hours. Deliverables include a Preliminary Analysis Report, which scopes the nature of the incident and provides recommendations for next steps and remediation.

- **IR discovery** — the IR team uses the NetWitness Platform to proactively hunt for indications of adversary activity. Deliverables include a Findings Report that provides remediation recommendations for any threats that have been identified.

- **IR response**— this service provides rapid access to IR expert "boots on the ground" when attack activities are suspected. Deliverables include a Findings Report that highlights the scope and nature of the incident and provides recommendations for next steps and remediation.

- **IR jumpstart for analytic intelligence and subscription services** — these services enable customers of the NetWitness Platform to optimize their product investments by working hand in hand with the NetWitness IR team to conduct proactive "hunting" and analysis activities. They include knowledge transfer during the hunting and analysis process and can be conducted periodically throughout the service period when delivered on a subscription basis.

The NetWitness IR team has gained first-hand experience in dealing with sophisticated adversaries and targeted attack campaigns. This knowledge and expertise is shared with our customers. Complementing NetWitness with the skills and knowledge transfer from the NetWitness IR team, organizations can take a significant step toward enhancing their security posture given today's threat environment.

ACME INC.
INCIDENT DISCOVERY
SAMPLE DELIVERABLE

NetWitness Incident Response Practice

TABLE OF CONTENTS

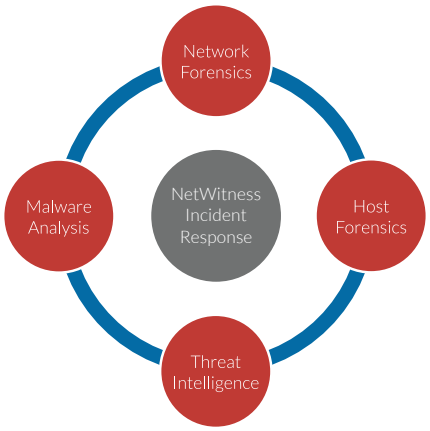
The NetWitness approach

Comprehensive forensic analysis framework

The Practice uses a comprehensive framework for data forensics and incident response. This ensures that the incident response process takes into consideration data from multiple sources including in-house systems, open source research and threat intelligence sources. The approach taken includes:

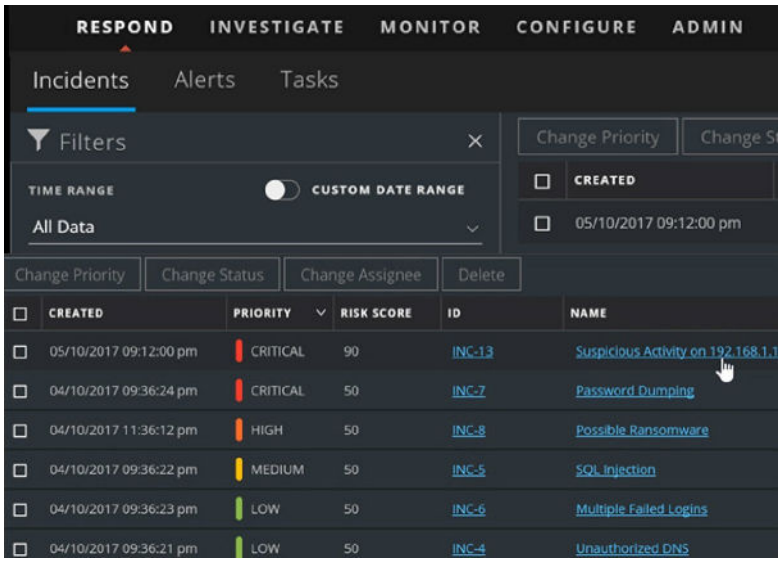
- **Network analysis** — data from packets and logs collected by NetWitness are used to identify suspicious communications by stealthy actors who are adept at bypassing defenses without triggering alerts.
- **Host forensics** — executables, files and libraries are used to identify unauthorized services and processes deployed by the attacker and running on endpoints.
- **Threat intelligence** — research is conducted to gain insights and harvest intelligence about the adversaries' attack infrastructure, tools and techniques. This can be particularly beneficial in profiling actors who are persistently targeting the organization in an ongoing campaign.
- **Malware analysis** — while malware can be very sophisticated, it tends to be relatively small in terms of file size, helping the attackers to conceal their efforts and avoid detection. By conducting basic and advanced static and dynamic analysis, an incident response team can develop blocking techniques and gather further intelligence to make the organization more resilient against further intrusions.

While the NetWitness Platform provides the team with comprehensive capabilities for incident response, it is not a prerequisite, and the Practice also works with organizations that rely on third-party solutions.



NetWitness Incident Response Services

The Forensic Analysis Framework includes packet capture, logs, and file and text analysis, which is facilitated by the ability to tag metadata, fully reconstruct suspicious network sessions and inspect endpoints.



The NetWitness® Platform

The Respond interface includes a dashboard that prioritizes incidents based on criticality, tracks the status of the remediation effort and enables the analyst to pivot to a nodal view of alert indicators. This facilitates rapid response, for example, by identifying C2 sessions and the related alerts for business files that may have been accessed, zipped, encrypted and staged for exfiltration.

Setting the stage for detection and analysis

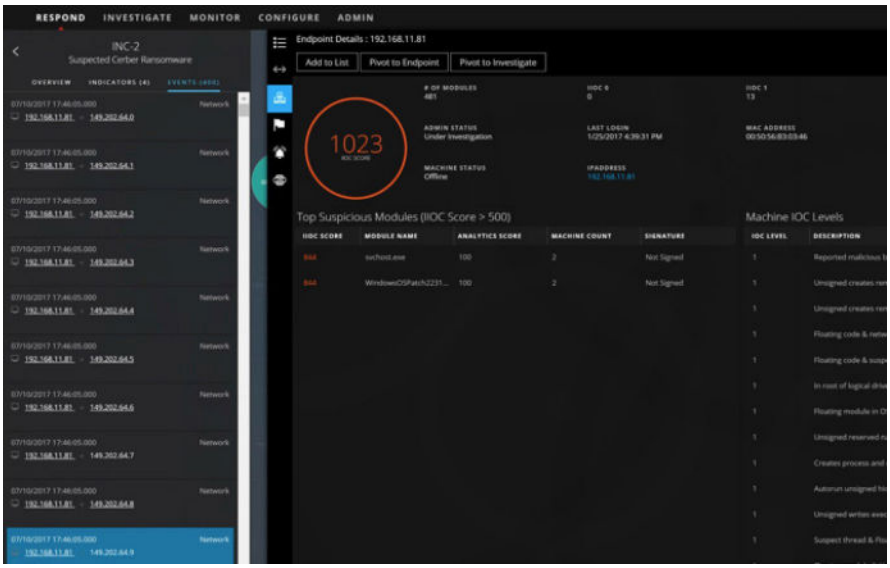
Start by capturing the right data

NetWitness's approach to incident response combined with the NetWitness Platform for logs, packets and endpoint anomaly detection helps organizations to ensure that the right data is being captured so that they can identify and remediate threats earlier in the attack lifecycle.

Advance planning and preparation is key. Initially, consideration is given to the information that accelerates detection and analysis. Examples of the analytic intelligence concepts used by the IR team include:

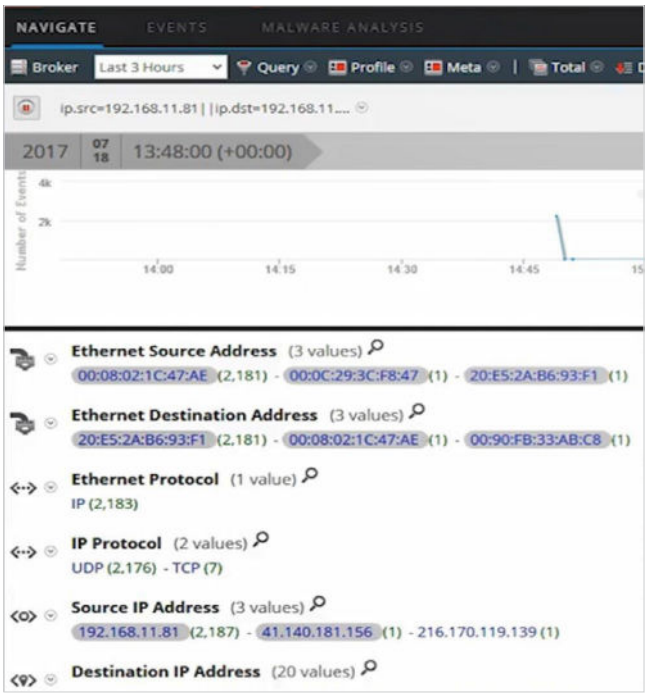
- **Data directionality** — by categorizing data such as "outbound to internet" organizations can more rapidly detect unusual activity such as beaconing from compromised hosts to outside domains.
- **IP address space** — by categorizing RFC 1918, traffic organizations can reduce payload capture, which helps to accelerate the analysis of smaller and more relevant data sets
- **Session characteristics** — by categorizing encrypted sessions, organizations can capture metadata without capturing obfuscated payloads, which also helps to accelerate the analysis of smaller and less computationally intensive data sets.
- **Filters and parsers** — by applying logic at the time of capture, the right metadata can be gathered for enrichment.
- **Correlation templates** — by anticipating threat scenarios, organizations can proactively generate rules to detect unusual activity such as traffic to suspect

locations, privilege escalation and session anomalies relating to HTTP headers, user agents and domain name services. Templates reduce the need for complex syntax development each time a query needs to be run.



The NetWitness® Platform

The Endpoint interface displays a machine risk score based on the analysis of suspect files and libraries, which provides the analyst with a valuable tool for the detection and analysis of anomalies that have by passed traditional defenses.



The NetWitness® Platform

The Investigate interface includes a Navigate dashboard, which enables the analyst to proactively hunt for suspicious activities that may have bypassed traditional signature-based defenses. The Incident Response Practice looks for anomalies, which may include traffic directionality, unusual inbound payloads, outbound encrypted files, C2 session indicators, suspicious email and web domains, and atypical ports and transport protocols.

"Be the hunter"

Finding the needle in the haystack

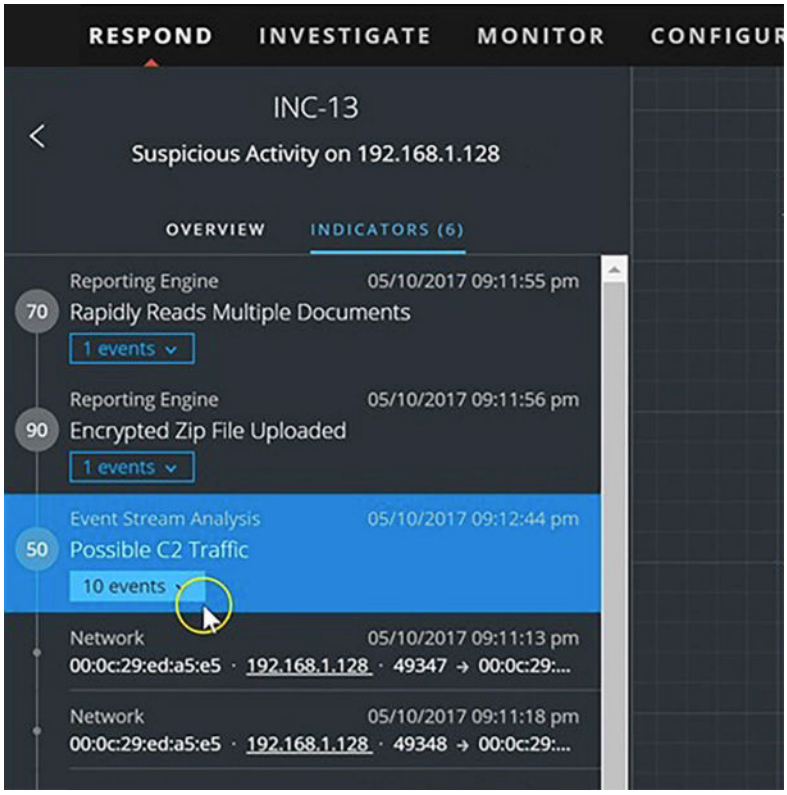
The asymmetric nature of cyber attacks may make breach prevention seem impossible. Organizations cannot anticipate the time and nature of an attack. Yet it is possible to detect anomalies early in the attack cycle and accelerate investigations to identify related tactics such as lateral moves to other IT assets.

For example, web shells are frequently used to gain access to a host system, providing the attacker with an initial foothold. Clues that can be used to detect web shell activity include:

- HTTP request methods such as "GET" and "POST"
- HTTP header blocks such as version, file paths, host name, user agent and content length

By gathering this data, organizations can begin to hunt for anomalies:

- **Request anomalies** — for example, inbound sessions that contain "POST" methods but without a "GET" request often associated with command and control exploits.
- **Referrer anomalies** — "POST" sessions without an IP referrer address may be a suspicious malware indicator, as human browsing behavior typically includes referrer data.
- **Domain anomalies** — the attacker's infrastructure often includes legitimate but compromised domains, from which additional instructions and payloads are downloaded. Repeated sessions at evenly distributed time intervals may denote beaconing to compromised domains.
- **Payload anomalies** — small and packed files, obfuscated data and encoded strings are potential risk indictors and may merit further investigation.



The NetWitness® Platform

Analysts can proactively hunt for the indicators of potential network beaconing activities and C2 nodes.

The NetWitness® Platform

NetWitness Live Connect facilitates gathering, analysis and dissemination of community-based threat intelligence, enabling customers to collaborate with peers and stay ahead of adversaries

Why we are better

NetWitness targeted attack detection

Protecting an organization's critical assets requires the right combination of technology and expertise. Security teams need to look for subtle clues, indicators of compromise and risky behavior rather than expect that preventive control mechanisms will succeed in blocking sophisticated adversaries. NetWitness broader value proposition for incident response services includes:

- **Global coverage** — resources facilitate a "follow-the-sun" model, with IR experts located in the Americas, Europe and Asia.
- **Practice accreditation and expertise** — the IR Practice is one of a short list of incident response organizations that has been certified by the National Security Agency. Our practitioners average over 10 years of experience each. Backgrounds include government and commercial defense agencies, federal and local law enforcement, and corporate IT security.

- **Industry experience** — the Practice has helped hundreds of customers identify and respond to compromise, including situations of active intrusion that lacked traditional indicators or notification by law enforcement. Threat actors across all industry segments and organization sizes have been engaged, including nation-states, criminals, hacktivists and insiders.

The NetWitness Platform provides organizations with the opportunity to gather early signs of compromise. When combined with the skills and knowledge transfer capabilities of the NetWitness IR team, organizations can begin to retake the high ground and protect their organization's most critical assets.

Putting it all together

Technical and operational expertise

The NetWitness Advanced Cyber Defense (ACD) Practice provides complementary consulting services and represents a team of professionals that has built and managed SOCs around the world, sharing resources and preferred practices with Dell EMC's global Cyber Security Intelligence and Response Team (CSIRT), which protects almost 200,000 people in over 100 countries. The ACD team provides a variety of related advanced threat services. This includes the Controlled Attack & Response Exercise, which is designed to stringently test the capabilities of an organization's incident response team in a set of "capture-the-flag" exercises. Results are scored based on flags captured, difficulty levels, and they are reviewed with the customer to identify areas for improvement.

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.

In addition to the services outlined above, Education services are available from RSA University, and product maintenance and Personalized Support Services are available from NetWitness Customer Support.

For more information, go to **netwitness.com**.

NETWITNESS
An RSA Business