NETWITNESS

NetWitness Incident Response Services

Reduce Threat Impacts. Improve Vigilance and Resilience.

As cyberattacks continue to accelerate, NetWitness is seeing a significant evolution in the tactics, techniques, and procedures (TTPs) of Advanced Persistent Threat (APT) attackers.

Attack	Trend
Zero-Day Exploits	There has been a rise in the use of zero-day vulnerabilities, with APT groups leveraging these unknown exploits to gain initial access before patches are available.
Supply Chain Attacks	Attackers have increasingly targeted the supply chains of their primary targets, exploiting trusted relationships to infiltrate networks.
Living off the Land (LotL):	APT groups continue to utilize legitimate system tools and processes to conduct their activities, reducing the likelihood of detection by blending in with normal operations
Targeting of Cloud and IoT Devices	With the growing adoption of Cloud services and Internet of Things (IoT) devices, APT attackers have shifted their focus to these areas, exploiting misconfigurations and vulnerabilities.
Vishing & Smishing	Smishing (SMS phishing) and vishing (voice phishing) attacks have improved and expanded and will continue to evolve with advances in AI.

There also continues to be a shortage of qualified security professionals that can ensure organizations remain vigilant, and able to respond and recover from a breach.

Protect your business by answering these questions to identify gaps in your security resources:

- Do my people have the right skills, and can they perform when needed?
- Is my IR plan up to date and appropriate, will it be effective?
- Does the organization have the right controls and security tools in place?
- How quickly can an attack be detected?
- Will management have the information needed to make real-time decisions?
- What happens if my IR plan doesn't work?

Global IR Solutions

The NetWitness IR (NWIR) services team is composed of elite cyber first responders, deployed across the globe, who can act quickly and efficiently to validate an attacker acting on objectives and provide recommendations for containment, expulsion, and remediation. Our flexible methodology allows the practice to partner with our clients, leveraging and augmenting (with the NetWitness platform) their existing people, processes, and technological capabilities.

Through many engagements, NWIR has built an experience base and intelligence network that enables our consultants to rapidly identify attacker activity, the extent of compromise (systems, vulnerabilities, data exfiltration, etc.), and develop appropriate recommendations for attacker expulsion and remediation. Since its inception, NWIR has helped hundreds of clients worldwide, including Fortune 500 corporations in every vertical as well as leading government agencies across the globe.

NWIR understands different threat actors including nation-states, criminals, activists, and insiders. Working closely with technical and legal teams, often under attorney-client privilege, NWIR helps clients meet due diligence standards, as well as regulatory-driven investigations.

- Deep experience to holistically design your incident response program
- Identification of security gaps and delivery of detailed improvement plans
- Incident detection and breach response services to help detect, understand, and respond to attacks
- Robust experience with the NetWitness Platform to help you accelerate and maximize your ROI from NetWitness for threat detection and response

Every day NWIR serves the mission of commercial and government customers, helping them address complex and sensitive security challenges including:

- Defending against advanced threats
- Managing organizational cyber-risk
- Assessing and improving security programs

NWIR helps organizations deploy a security model that efficiently applies resources across prevention, monitoring, and response. This vigilant security posture minimizes the dwell time of malicious actors within IT environments. NWIR's "proactive" offerings help ensure that intrusion and compromise do not result in ruinous operational consequences and mission disruption.

NetWitness Incident Response Offerings

IR Retainer	Guaranteed rapid access to NetWitness IR resources and expertise who help organizations gain situational awareness and develop plans for mitigation and recovery from a cyber crisis. *Specialized offerings available for cloud and isolated, remote locations.*
IR Rapid Deploy	Augment your security team with experienced incident responders who can review suspicious activities and anomalies on network and host systems during a cyber-crisis. This service helps organizations effectively mitigate security breaches and cyberattacks by Identifying, Containing, and ultimately Expelling the Attackers.
Compromise Assessment, Discovery	Real insight into the scope of potential cyberattacks and vulnerabilities through the identification and validation of suspicious behaviors across network and IT systems. IR Discovery proactively searches for suspicious activities and anomalies prior to detection by traditional security controls or 3rd parties such as law enforcement.
Red Team, Security Processes & Control Evaluation	Evaluate IR control and process efficacy by assessing resilience from advanced attacks including the ability to detect and manage zero-day scenarios. The NWIR Red Team utilizes simulated adversary attacks that mimic the tactics, techniques, and procedures (TTPs) of real-world adversaries so customers can experience breach scenarios without associated negative impacts.
Security Program (GAP) Assessment	Systematic process designed to assess an organization's current cybersecurity posture compared against industry best practices, regulatory requirements, and the organization's specific security objectives. This service helps organizations identify potential vulnerabilities, weaknesses, and areas for improvement in their security infrastructure, policies, and procedures, ultimately enhancing overall security posture and resilience against cyber threats.
Tabletop Exercises	Prepare stakeholders across organizational functions to be ready for cyber threats and attacks with awareness and training. IT professionals, executives, and relevant staff participate in a realistic (pulled from actual IR engagements) cyber-attack scenario simulation which helps assess readiness and capability while educating and establishing best practice.

About NetWitness

NetWitness 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.

Ready to learn more? Visit www.netwitness.com