# NetWitness® Incident Response Services

## Reduce Threat Impacts. Improve Resilience.

As cybercrime continues to accelerate, there is a shortage of qualified security professionals to ensure organizations remain protected. Job-hopping by the most experienced cybersecurity professionals also increases risk. As these trends converge, businesses are in a vulnerable spot without the resources to mount an effective defense.

## Enhance your security response with an experienced team

NetWitness Incident Response Services ensure you're ready to identify cyber threats fast and defend against them on an ongoing basis. Reduce business risk and improve your overall security posture with the support of a team that identifies, mitigates and eradicates threats, establishes risk management programs, and fulfills compliance requirements.
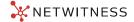
## Identify security gaps

Be prepared to 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, and 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?

### Key Features

- Identification of security gaps and delivery of a detailed improvement plan

- Deep expertise to holistically design and build your security monitoring program or SOC

- Incident detection and breach response services to help detect, understand and respond to attacks

- Formalized, as well as on-the-job training to improve the skills of analysts of all levels

- Robust experience with the NetWitness Platform to help you accelerate and maximize your ROI from NetWitness for threat detection and response

# NetWitness Incident Response Offerings

| | |
|---|---|
| **CARE** | Identify weaknesses in your security posture, assess your organization's ability to detect and respond to a realistic attack scenario, and receive recommendations for improving overall security posture. CARE utilizes a set of simulated adversary attacks that mimic the tactics, techniques, and procedures (TTPs) of real-world adversaries. |
| **IR Discovery** | Receive real insight into the scope of potential cyberattacks and vulnerabilities with the identification and validation of suspicious behaviors across your network and IT systems. IR Discovery proactively reviews suspicious activities and anomalies without any prior grounds for suspecting nefarious activity. |
| **IR Retainer** | Augment your security team by engaging NetWitness on retainer to facilitate rapid access to incident response resources and expertise should an incident occur. |
| **Retainer Services for Cloud** | Safeguard your cloud-based infrastructure and data with a comprehensive, proactive, and adaptive solution. NetWitness leverages industry-leading expertise and cutting-edge technology to provide an end-to-end security strategy that effectively addresses your organization's unique security needs and ensures continuous protection of your cloud environments. |
| **Tabletop Exercises** | Be prepared to respond to potential cyber threats and attacks with a training program that involves a scenario-based simulation where a team of stakeholders – including IT professionals, executives, and relevant staff – participate in a mock cybersecurity incident. |
| **IR Rapid Deployment** | Receive experienced Rapid Incident Response support determining the scope of a cyberattack when IR Rapid Deployment identifies and validates suspected anomalies and system behaviors across your network and IT systems. We provide customers with a review of suspicious activities and anomalies identified on network and host systems or detected by third parties such as law enforcement. |
| **Analytic Intelligence / Analysts Enablement** | Learn how to apply NetWitness Incident Response methodology and best practices. Analytic Intelligence / Analysts Enablement assists customers in the application of hunting for anomalous behaviors (threat hunting), malware analysis, network and application compromise assessment, and other cybersecurity services. |

## Ready to learn more? Visit www.netwitness.com/services

NETWITNESS