NETWITNESS

Incident Response Retainer for Cloud

Service Overview

Service Purpose

Cloud environments create unique security challenges. Assets span multiple providers; configurations change constantly, access patterns are complex, and traditional perimeter defenses don't apply. When a security incident hits cloud infrastructure, the clock starts immediately—but most organizations don't have dedicated cloud incident response expertise on staff, and finding qualified help during an active breach wastes precious hours. By the time external specialists get up to speed on your environment, attackers have often expanded their foothold or completed their objectives.

Organizations running critical operations in the cloud need immediate access to incident response expertise that already understands their environment and can respond the moment a threat emerges.

NetWitness Solution - Incident Response Retainer for Cloud

The NetWitness Incident Response Retainer for Cloud delivers year-round security coverage specifically designed for cloud-based infrastructure. This isn't on-demand consulting where the team learns about your environment during a crisis. The retainer establishes an ongoing relationship where NetWitness maintains familiarity with your cloud architecture, security posture, and incident response capabilities—so when an incident occurs, response begins immediately with experts who already know your systems.

The service combines rapid incident response (1-hour initial triage, 3-hour preliminary analysis) with proactive security activities throughout the year: periodic security assessments, vulnerability testing, compliance audits, risk management, incident response plan maintenance, policy reviews, and staff training. The result is both faster incident response and continuous improvement of your cloud security posture.

How the Retainer Works

Retainer Activation

Before incident response capability goes live, NetWitness works with your team to establish environment access, review infrastructure documentation, assess or develop your cloud incident response plan, and review security policies. This activation phase ensures the team understands your cloud architecture, critical assets, and response procedures before any incident occurs.

Ongoing Security Activities (Throughout the Year)

- **Security Assessments & Audits:** Up to 4 periodic security assessments of the cloud environment, up to 4 vulnerability scans and penetration tests, and up to 2 compliance audits (GDPR, HIPAA, PCI DSS) with recommendations for improvements.
- **Risk Management:** Continuous risk identification, assessment, and mitigation recommendations. Development and maintenance of a risk register with regular reporting.
- **Incident Response Plan Maintenance:** Regular review and updates to your cloud incident response plan based on lessons learned, environmental changes, and evolving threats.
- **Security Policy Review & Development:** Review of existing security policies and procedures specific to your cloud environment, with recommendations for updates to comply with industry standards and best practices.
- **Training & Awareness:** Up to 4 security training sessions for IT staff and employees, plus up to 2 workshops on cloud security best practices, incident response strategies, and regulatory compliance.

Incident Response (When needed)

When an incident occurs, response follows a structured timeline :

1 hour	3 hours	12 hours
Initial incident triage after contact	Remote preliminary analysis begins	Team enroute for on-site analysis if needed

Response includes incident assessment and prioritization, analysis, containment and recommendations for eradication, recovery support, as well as post-incident review, and comprehensive incident reporting and documentation.

Benefits and Outcomes of the Cloud Retainer

- **Immediate Response Capability:** Guaranteed 1-hour initial triage and 3-hour preliminary analysis when incidents occur—no delays finding available consultants or negotiating emergency contracts during a crisis.
- **Environment Familiarity:** The response team already understands your cloud architecture, critical assets, security controls, and incident response procedures. No learning curve during active incidents.
- **Proactive Security Improvement:** Regular assessments, vulnerability testing, and compliance audits throughout the year to identify and address weaknesses before they become incident vectors.
- **Continuous Risk Management:** Ongoing risk identification and mitigation recommendations keep pace with changes in your cloud environment and threat landscape.
- **Maintained Incident Readiness:** Regular updates to incident response plans, security policies, and procedures ensure your response capability stays current as your cloud environment evolves.
- **Team Preparedness:** Ongoing training and workshops keep IT staff and employees current on cloud security best practices, incident response strategies, and compliance requirements.
- **Compliance Support:** Regular compliance audits help maintain alignment with regulatory requirements (GDPR, HIPAA, PCI DSS) specific to your industry.
- **Cost Predictability:** Annual retainer provides budget certainty for both incident response capability and ongoing security activities, avoiding emergency rates during incidents.
- **NIST & ISO27001 Alignment:** Incident response methodology integrates established frameworks, providing a robust and compliant approach to managing cybersecurity incidents in cloud environments.

About NetWitness

NetWitness has been at the forefront of cybersecurity detection and response for over two decades. Built on technology originally developed for the intelligence community, the NetWitness platform has evolved into one of the most capable threat detection and investigation ecosystems available to enterprise security teams today. That same depth of capability underpins every professional services engagement we deliver.

The NetWitness Incident Response team brings together experienced incident responders, threat hunters, malware analysts, and forensics specialists who have worked across some of the most complex and high-stakes investigations in the industry. We do not show up with a generic playbook. Every engagement is shaped by what we find in your environment, informed by current adversary tradecraft, and driven by a genuine commitment to giving your team clarity when it matters most.

NETWITNESS