NETWITNESS

DATA SHEET

NetWitness Incident Response and Cyber Defense Services

Comprehensive security services to improve threat detection and response

Overview

Security programs need to continually evolve to stay ahead of attackers and the latest threats. Attackers continue to advance and use increasingly sophisticated techniques to infiltrate organizations. They invest significant resources conducting reconnaissance to learn about organizations and to develop techniques specifically designed to bypass the security defenses being used.

The bottom line is that effective defense is not purely about buying the latest security technologies; it is about establishing an effective security program that brings together security expertise, processes and technology to improve the organization's ability to prevent, detect and respond to attacks.

Key challenges for organizations

As organizations begin to understand that their primarily preventive, technology-centric security approach is no longer sufficient, they often come to realize that they don't know how to significantly improve. They don't know what skills they need and in what amount and in what priority order, what processes they should be following, or what technologies they have and which they lack that can be part of their improvement plan. This uncertainty is often most acute in their threat detection and response program.

Many organizations also have a history of buying narrowly scoped security technologies to address the latest attacker technique, but often without much sustained security improvement to show for them. To gain budgetary approval for incremental resources, the security organization needs a credible plan with short, intermediate, and longer term success milestones.

Once organizations recognize that they need to significantly improve their threat detection and response capabilities, they often turn to building or significantly building out their security operations center (SOC.

But if they have never done this before, doing so on their own can be a daunting task. Where to start? Hire people, with what skills, work on processes and integration with other internal organizations, or buy technology? Should the organization work with specialized Managed Security Service Providers (MSSPs instead of building the program fully in-house? How to divide up the roles and responsibilities in any go-forward plan? What should the six, 12 and 18 month plan and associated milestones be? How much will this cost?

Many organizations, having read about recent breaches at industry peers, reflect on their own limitations in threat detection and response, often rightly wondering about their true security posture. They wonder if they have been breached or are currently exposed.

When organizations run into a suspected breach that is impacting the business, they often recognize that they don't have the breach management or forensics expertise to know what to do and in what order.

Furthermore, many organizations don't have the tools or expertise to know how to determine whether they are dealing with a lower-risk commodity attack or have been infiltrated by a sophisticated cybercriminal or nation state attacker

Why use NetWitness Incident Response and Cyber Defense Services?

The NetWitness Incident Response and Cyber Defense Services help organization implement a holistic security program for targeted attack defense—across the three interrelated areas of expertise (including organizational model), processes and technology—with a particular emphasis on their threat detection and response programs.

Whether the organization's security monitoring program is in its formative stages or is based on a well-established SOC and is just in need of benchmarking and refinement, Incident Response and Cyber Defense professionals can deliver customized strategic advice as well as specific tactical services to help organizations continuously improve their ability to detect, investigate and respond to threats and to maximize the value received from NetWitness products and other security solutions.

The NetWitness Incident Response and Cyber Defense Services:

- Assess an organization's security gaps and provide a detailed improvement plan that is specific to the organization.
- Provide deep expertise to help holistically design and build out an organization's security monitoring program or SOC.
- Provide incident detection and breach response services to help organizations detect, understand and respond to attacks from even the most sophisticated threat actors.
- Deliver both formalized as well as on-the-job training to improve the skills of both junior and more senior analysts.
- Have deep expertise with the NetWitness Platform and can help organizations accelerate and maximize the value attained by using these products for threat detection and response

Services portfolio overview

This table provides a summary of the primary Incident Response and Cyber Defense services.

NetWitness Cyber Defense	Services Portfolio for NetWitness Cyber Defense
Strategy & Roadmap	• Focused on advanced threat detection and response • Identification of current capabilities and gaps • Comparison with peer maturity levels • Development of a prioritized remediation roadmap
Roadmap for the NIST Cybersecurity Framework (CSF)	• For organizations with little or no security program • Aligns with NIST CSF guidelines and recommendations • Prioritizes areas for enhancement of security controls • Includes tailored action plans with timelines and owners
Controlled Attack & Response Exercise	• Controlled attack to test capabilities for incident response • Addresses both technical and operational controls • Scoring methodology includes “capture the flag” • Highlights areas for process enhancement
SOC Design & Implementation Service	• Addresses the design and buildout of the SOC • Includes organization structure, roles & responsibilities • Development of Use Cases & Response Procedures • Can include second-seating by ACD for knowledge transfer
Roadmap for Cyber Threat Intelligence	• Review and roadmap for foundational Cyber Threat Intelligence requirements • Enhances countermeasure capabilities, preparedness and ability to defend against targeted attacks
NetWitness Use Case Development	• Gathers customer use case requirements through interviews and documentation reviews • Development of up to 10 NetWitness use cases
Incident Response Plan	• Development of an Incident Response Plan • Conduct an incident walkthrough exercise to practice and familiarize the customer’s security team with the Incident Response Plan
NetWitness Incident Response	**Services Portfolio for NetWitness Incident Response Services**
IR Response & Retainer	• IR retainer portfolio with varying SLA levels • Surge access to resources and expertise • Use of the NetWitness Platform for advanced forensics • Remediation and takedown of advanced threats • Recommendations for IT infrastructure hardening
IR Discovery, Subscription & Jumpstart Services	• Proactive hunting for advanced threats with the NetWitness Platform • “Be the hunter” knowledge transfer by NetWitness IR experts • Preferred practices for packet capture and analysis • Tips & tricks for endpoint anomaly detection

Support

NetWitness world-class global support organization can enhance your security solution with a comprehensive support plan that provides users access to expert advice for questions about installation, implementation, patches, upgrades, product-related issues and much more. NetWitness provides the resources you need to quickly and proactively resolve product-related issues and questions to ensure business continuity. NetWitness also offers two Personalized Support Services offerings that will take your support experience to the next level. The first, a Designated Support Engineer, provides you a single POC for all of your support-related questions and saves your organization time by having them familiar with your environment. The second, a Technical Account Manager, provides you a single POC for all of your NetWitness relationship needs. The TAM will advocate for you on your behalf internally at NetWitness, assist you with escalations and serve as a bridge between your organization and various parties within NetWitness.
For more information about NetWitness Support and Services, see the NetWitness Support page.

Next steps

For more information about NetWitness' portfolio of services, including Incident Response and Cyber Defense Services, please visit **netwitness.com/services**, or contact your NetWitness sales rep or channel account manager.

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

NETWITNESS