NETWITNESS

Incident Response Rapid Deployment

IRRAP – Service Overview

SERVICE OVERVIEW

Many organizations will encounter advanced persistent threats (APT) at some point. These complex and sophisticated cyberattacks can evade detection and persist in organizations IT environment for years. APT attacks often cause significant damage and impact to the customer's data, assets, operations, and reputation. Customers need to have the surest way to detect, respond, and recover from APT attacks, and to temporarily elevate or scale up their incident response capabilities to meet the size and sophistication of these threat actors.

NetWitness Solution- Incident Response Rapid Engagement

IRRAP (pronounced I-RAP) is a service that provides customers with an immediate and intensive, incident response capability, deploying a team of experienced and certified security experts, who can assist them with various aspects of incident response, such as threat anomaly detection, incident analysis, forensic investigation, remediation, and recovery. IRRAP aids customers in dealing with APT attacks, so they can isolate, respond, and recover when dealing with sophisticated cybercriminals and nation state threat actors. IRRAP is the fastest way to elevate your response to sophisticated APT Attacks.

Incident Response RAPid deployment Service (IRRAP)

Service Characteristics

Rapid Response: Our team is ready to respond swiftly to any potential cybersecurity incident.

Expertise and Specialization: The team consists of skilled cybersecurity professionals with expertise in various areas such as digital forensics, malware analysis, network forensics and log analysis.

Containment and Eradication: We work to contain the incident and prevent it from spreading further within the organization's network.

Communication and Collaboration: Effective communication is essential, both within the incident response team and with relevant stakeholders within the organization.

External Coordination: In more severe incidents, we work with external entities like law enforcement, regulatory authorities, or third-party incident response providers for additional support.

Client Privacy and Confidentiality: The incident response team respects client privacy and ensures the confidentiality of sensitive information obtained during the investigation.

Continuous Improvement: Post-incident, the team engages in a thorough review of the response process to identify areas of improvement. This includes evaluating actions, tools used, and overall incident management strategy.

How IRRAP - Rapid Engagement Works

- In consultation with the NetWitness IR Team the Customer purchases the recommended number of blocks of IRRP services.
- NetWitness IR deploys a team of experienced and certified security experts, who seek to gain situational awareness, identify the attacker and their objectives, and ultimately contain and eradicate the threat.
- If necessary, NetWitness IR will deploy the NetWitness Platform in the customer's IT environment and configure it to collect and analyze data from various sources, such as logs, packets, NetFlow, endpoint agents, cloud services, and threat intelligence.
- The NetWitness IR team performs a vigorous incident response investigation, using NetWitness Platform and or any other appropriate tools to scan and monitor the customer's IT and Network environment, in addition to using threat intelligence and actionable indicators of compromise to identify and prioritize threats. The NetWitness IR team also uses advanced analytics and other techniques to determine the scope, impact, and root cause of the incident, and to recommend and plan for remediation and recovery actions.
- The NetWitness IR team provides the customer with a detailed report and presentation of results, including the findings, recommendations, and action items.

RESPONSE TO INCIDENTS & SUSPECTED COMPROMISE

Initial review of incident data gathered by the customer

Analysis of data for indications of exfiltration, compromised hosts, beaconing and malware, etc.

Breach remediation & hardening to prevent persistence, including a highly coordinated "takedown," if necessary.

Findings Report & Executive Presentation

Prioritized Remediation Recommendations

Malware Analysis & Reverse Engineering

Netwitness Incident Response Rapid Deployment Service

- RESPONSE to sophisticated attacks at enterprise-scale
- Extensive ability to identify IoCs relating to outbound files & protocols, suspect file extensions & non-descript file names, Trojans, BOTs, C2 nodes, obfuscated & encrypted traffic, unusual SSL & suspect sites & destinations, etc.
- Post-breach hand-off for SOC buildout/enhancement and broader requirements for defense-in-depth relating to IAM and Integrated Risk Management, etc.

IRRAP Service

Service workflow

Service Activation

Service Setup

Initialization	Preparation
Coordinate Kickoff Call	Review organizational assets and potential visibility gaps
Review initial evidences gathered by the Customer	Identify Customer technologies which may assist incident response activities
Establish Contacts, Roles & Responsibilities	Ensure remote access for the IR Team
Establish Secure Communications Channels and Remote Access Plan	

Service delivery

Investigation	Mass-Triage	Reporting
Perform Analysis which may include host and network forensics, log review and malware analysis	Identify "Patient Zero" or attack initial point-of-entry	Draw the final report to present a clear narrative of the attack, including any evidence needed
Define attack magnitude and timeline	Provide guidance with a Remediation Plan"	Provide direction and guidance for additional activities as needed
Define containment and remediation strategies	Build the attack timeline	Plan and organize "Post-Incident" monitoring for the Company
Extract IOCs to prepare for a Mass-Triage	Build the "Compromise systems Matrix"	

Service length may vary

Benefits and Outcomes of IRRAP - Rapid Engagement

- Dealing with APT attacks, by having the surest way to detect, isolate, respond, and recover, from such incidents. Temporarily elevating or scaling up incident response capabilities to meet the size and sophistication of APT style attacks.
- Access a team of experienced and certified security experts, who can provide immediate and intensive incident response support. Employing enterprise class security tools like the NetWitness Platform to scan and monitor their IT environment, and by using threat intelligence and indicators of compromise to identify and prioritize threats.
- A detailed report and presentation of the investigation findings, including tactical and strategic recommendations, and other action items.
- Reduce attacker dwell or free time as there is a significant correlation between the amount of time a cyber attacker goes undetected (known as "dwell time") and the expense of removing them. The longer an attacker remains undetected within a network, the more damage they can potentially cause, leading to higher costs for remediation and recovery.

Here are some key points:

Increased Damage

The longer an attacker is present, the more time they have to explore the network, steal sensitive data, and deploy additional malware. This can lead to more extensive damage that requires more resources to fix.

Higher Recovery Costs

Extended dwell times often result in more complex and widespread infections, which can be more costly to clean up. This includes costs for incident response, forensic investigations, and restoring systems and data.

Business Disruption

Prolonged attacks can cause significant operational disruptions, leading to lost revenue and productivity. The longer the disruption, the higher the financial impact on the business.

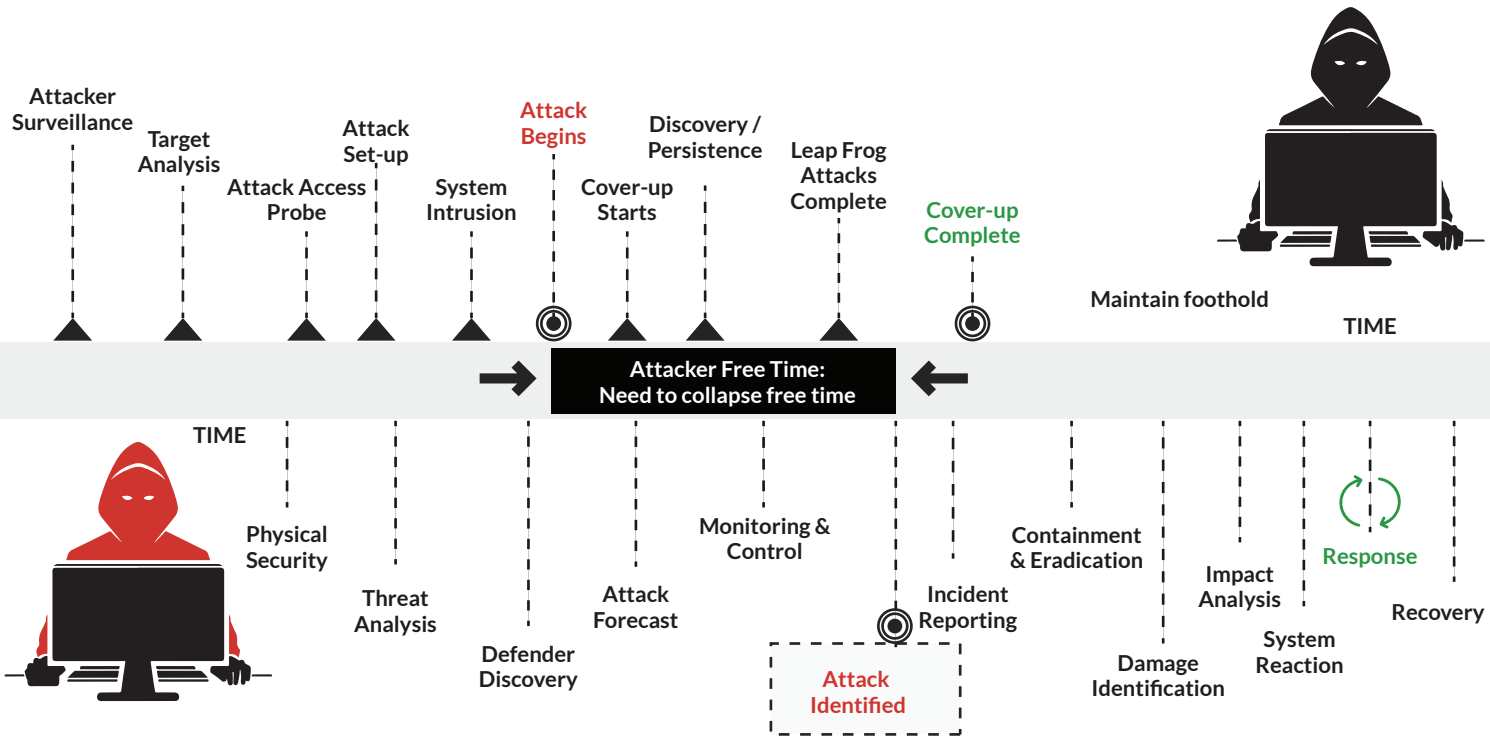
Regulatory Fines and Legal Costs

If sensitive data is compromised, companies may face regulatory fines and legal costs. The longer the attacker is undetected, the more data they can potentially exfiltrate, increasing the risk of regulatory penalties.

Reducing dwell time is crucial for minimizing these costs. Implementing robust detection and response strategies can help identify and mitigate threats more quickly, reducing the overall impact of a cyber attack.

(1) Attacker Dwell Time: Ransomware's Most Important Metric - Dark Reading.
https://www.darkreading.com/cyber-risk/attacker-dwell-time-ransomware-s-most-important-metric.
(2) Hackers often spend over 250 hours undetected in networks.
https://www.techradar.com/news/average-attacker-spends-over-250-hours-undetected-in-networks.
(3) When Time is Ticking: How to Cut the Dwell Time of a Cyber-Attacker.
https://www.ajg.com/uk/news-and-insights/2024/may/how-to-cut-the-dwell-time-of-a-cyber-attacker/.

Reducing Attacker Free Time



About NetWitness

NetWitness Incident Response provides enterprises with expert security services when they need them most. Our team of experienced incident responders, threat hunters, and forensics specialists help enterprises detect advanced threats, investigate security incidents, assess defensive capabilities, and strengthen their security operations. We deliver rapid responses, thorough investigation, and actionable intelligence that empower companies to stay ahead of sophisticated adversaries. The IR practice is part of NetWitness a renowned organization that 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

Ready to learn more? Visit www.netwitness.com

NETWITNESS