SECURITY ON·DEMAND

ThreatWatch Response & Remediation Service Overview

MITIGATE CYBER-ATTACKS AND SPEED RESPONSE TO COMPROMISED SYSTEMS

Detection Windows are Shrinking

Hackers have all the time in the world to probe your defenses, but the defenders have to be right 100% of the time. One slip-up or weakness in the defense is all it takes to become compromised. Historically, the time it took an attacker to compromise your systems was months and months, perhaps even a year or more. Recently it was reported that the time it takes for a Russian based hacking group to compromise a system is just 19 minutes.* You can't detect and respond that quickly, no human can.

Attackers are Ahead of the Defenders

Threats are still evading system defenses. They know how to hide within the data and they use AI and machine learning to avoid detection.

Today, your organization must be able to:

- Detect the unknown threats that can attack your systems
- Prevent confidential information leakage or data loss
- Know if someone is going to bring your operations to a halt.

The Solution: ThreatWatch Response & Remediation (RAR)

- ThreatWatch Response & Remediation Service (RAR) is designed to provide an automated capability to respond to or contain an attack or suspected compromise.

- Security On-Demand's approach is to combine log events with forensic data gathered from each endpoint or server to create a holistic view of threat indicators that may not be able to be identified through system logs alone.

- ThreatWatch RAR helps to improve detection accuracy and reduces false positives that often plague and slow down IT resources in taking decisive action. Sometimes minutes count in acting decisively to protect against the impact business operations from a fast-moving threat, such as Ransomware.

ThreatWatch Response & Remediation (RAR) Service Includes:

24x7

Threat Validation: When there are threat indicators that indicate that an endpoint or server is likely compromised, the SOC will launch a targeted analysis on the endpoints in question to verify potential malicious activity to validate potential threats.

Threat Response: Once the threat is assessed and validated, a risk and confidence score will be assigned to the anomaly as part of the investigation and appropriate action will be taken based on the response and containment decision directives

Quarantine Exclusions: Just as important as what should be quarantined, it's also vital to know what should never be blocked. This Client has full control over these decisions.

Response Coverage: The Security Operations Centers are ready to act 24x7x365 in accordance with threat levels, severity, and impact based on pre-agreed actions matrix to ensure full accountability.

Client Portal: The client portal will provide on-going and past investigations as well as actions taken to quarantine or isolate a malicious process that is affecting a client’s network or systems.

Reporting: Reports can be provided on a monthly basis via the Client Portal that provides information on alerts and events.

Optional Service Co-Management: Co-management of the service allows clients to actively participate by sharing the toolset with the Security Operations Team. The client may also use this for investigations and analysis on an as needed basis to help with forensics investigations or for other purposes.

ThreatWatch Response & Remediation will help you:

- Reduce complexity & cost of operations
- Detect threats faster and reduce impact from potential breaches
- Mitigate brand impact and business risk
- Meet regulatory compliance needs (PCI, HIPAA, GLBA, etc)
- Cover departmental cyber-skills gap
- Reduce false positives that waste your staff's time
- Extend your threat monitoring coverage to 24x7