halcyon

Professional Services: Ransomware Greenlight Service

The Ransomware Reality

After a ransomware incident, you need to know your organization can return to business without worry. With ransom requests ranging between $1M and $5M, cybercrime groups continue to reap enormous profits by attacking companies across all industries. Combined with the alarming statistic that 80% of ransomware victims suffer from additional follow-on attacks, it's clear that the traditional incident response (IR) approach lags behind the reality of this new ransomware economy.

While the steps during an IR are necessary, they are more informed by the need to build a chain of custody for legal requirements than the drive to recover and return a business to operational status quickly. The Halcyon Greenlight Service solves this problem.

Disrupting Persistence

From hijacking DLL search order to load malicious DLLs, to modifying SSH authorized keys or creating new Windows services to execute malicious payloads repeatedly, the attackers have myriad ways to maintain low-level persistence once they've gained initial access to an organization. Even after restoring from backups post-ransomware event, completing an incident response engagement, and understanding the root cause of the breach, it's highly likely that the attackers still have access to return and re-ransom your organization.

The Halcyon Greenlight Service answers the question, "Are the attackers still here?" By combining the power of real-time resilience in the Halcyon platform with our expert Threat Research team, the Greenlight Service is a multi-step solution to ensure that all persistence mechanisms are broken, that all endpoints across the organization are protected from additional ransomware events, that the internal security or IT teams are empowered with an audit of all endpoint and network infrastructure, and a complete real-world ransomware table-top exercise to ensure that your teams are ready and confident to respond in the future.

KEY SERVICE FEATURES OF GREENLIGHT:

1. Deployment - We assist and manage all stages of the Halcyon agent deployment across each applicable endpoint in the organization to appropriately phase-in prevention modes and ensure compatibility.

KEY BENEFITS:

- Know definitively that the ransomware group's persistence mechanisms and tools have been eliminated from your environment, giving you the green light to get back to business.
- Protect against future ransomware and advanced attacks with an assisted deployment of the Halcyon platform, plus a hands-on examination of each applicable endpoint's processes and executables by the Halcyon Threat Research team.
- Receive a Ransomware Resilience Report, which audits your current endpoint and network infrastructure posture to provide additional security recommendations to reduce the risk of future incidents.
- Verify that your security processes, team, and plans are set up for success with a real-world ransomware tabletop exercise driven by the Halcyon Threat Research team.

2. Triage - We assume the attackers maintain persistence in the environment post-attack and, therefore, immediately implement our most restrictive endpoint policies to disrupt any lingering threats. To balance this overly paranoid mode of deployment not typically used during a standard rollout, Halcyon's Threat Research team will analyze every process and executable on each endpoint to ensure that only valid processes, applications, and DLLs are running. This stage is required to transition the Halcyon agent into a less restricted and more compatible mode of operation.

3. Credential Refresh - Post-triage, all credentials across the organization must be reset to eliminate the risk that an attacker still has legitimate access to any systems through compromised credentials.

4. Ransomware Resilience Report - Halcyon will analyze, audit, and deliver a report of findings and recommendations after reviewing the organization's endpoint and network infrastructure protections to improve the entire security posture of the environment.

5. Ransomware Tabletop - Halcyon will organize and execute a tabletop exercise with the customer based on real-world ransomware groups' tactics, techniques, and procedures. This simulation aims to ensure your teams are confident and capable of responding to any additional attacks.

6. Ransomware Recovery Service (OPTIONAL) - Halcyon has successfully exploited flaws in various ransomware packages to allow for the potential recovery of encrypted files even without the Halcyon agent running. This optional add-on service is available to ransomware victims who have yet to restore their systems from backups fully.

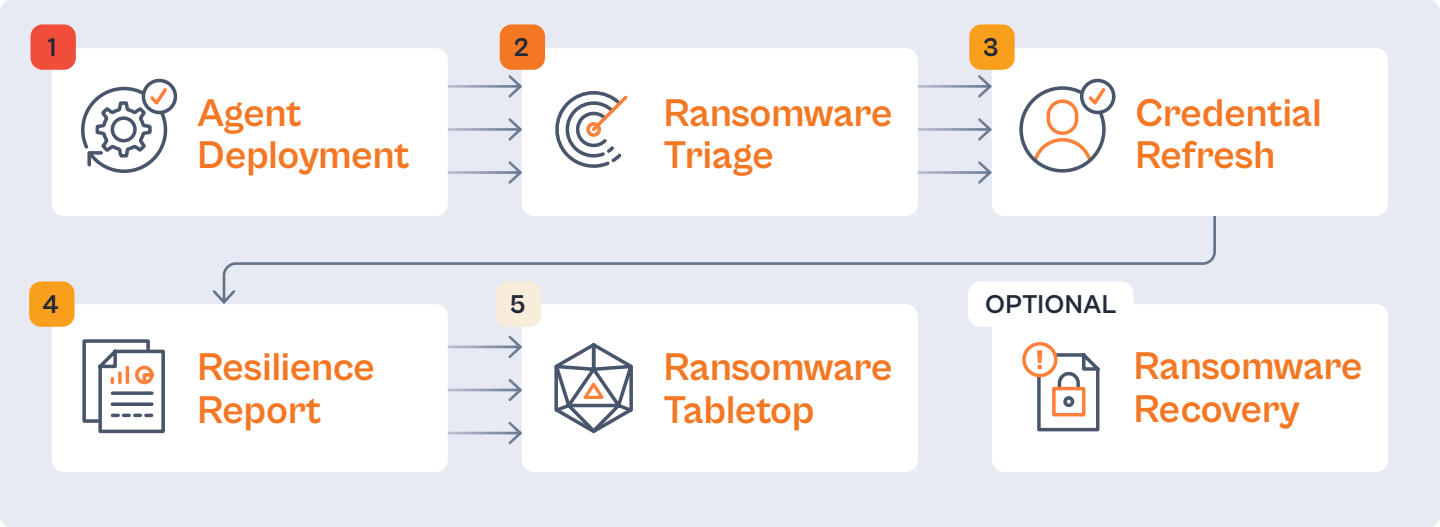

Fig 1: Halcyon Greenlight Service – Key Service Feature Workflow

Why Halcyon?

Halcyon is the first real-time cyber resilience platform built to keep your business operational in the face of catastrophic cyber-attacks. With over 1,500 customers and thousands of threats stopped daily, Halcyon's unique approach was built to minimize or eliminate the need to recover from ransomware attacks with built-in encryption key capture, automated recovery, and next-generation anti-data exfiltration technology.

For more information and to request a formal quote, contact services@halcyon.ai or visit halcyon.ai to learn more.