halcyon

Data Sheet

Neutralize Ransomware Before It Strikes with HALO: Halcyon Active Lock Out

Ransomware attackers are becoming more sophisticated by the day. Today's adversaries are no longer simply deploying malware and hoping for a payout–they understand how organizations respond to threats, how incident response playbooks work, and how to delay or evade countermeasures. These threat actors now operate with the precision of military campaigns, using stealth tactics to bypass detection and remain hidden until it's too late.

They exploit poor visibility, inconsistent enforcement of security controls, and human error. The stakes have never been higher, and traditional defenses are often one step behind.

An Overview of Halcyon Active Lock Out (HALO)

HALO is the fusion of Halcyon's cutting-edge anti-ransomware technology with elite threat intelligence and response expertise. This service is purpose-built to disrupt ransomware campaigns before they can do damage proactively.

- **Elite Expertise:** Operated by former specialists from Mandiant, Accuvant, Kivu, and other top-tier response teams.
- **Proactive Engagement:** HALO activates before an incident occurs, targeting ransomware campaigns in motion.
- **Tailored Executive Insight:** We deliver actionable, digestible reports for technical and executive audiences.
- **Zero-Cost Technology During Engagement:** Full access to Halcyon and leading EDR and forensic tooling is available at no additional cost during response.

How HALO Works

Notification

Halcyon notifies Client of confirmed intel as part of HALO

In Action

Halcyon deploys technology and rapidly secures the environment

Containment

Halcyon declares environment is resilient to ransomware

Ransomware

A payload execution or attack is made unsuccessful

HALO Benefits

Early Threat Detection: Identify and respond to threats before ransomware actors gain a foothold.

No-Cost Access to Advanced Tools: Utilize Halcyon and leading EDR and forensic technologies during engagement without upfront cost.

Reduced Downtime Risk: Avoid the operational andreputational damage caused by successful ransomware attacks.

Hands-On Expert Defense: Gain 24/7 access to incident response veterans managing threats in real-time.

HALO is unique in its ability to *intercept* and *neutralize* ransomware before it impacts your operations. Here's how the team engages and defends:

1. **Continuous Threat Surveillance**
   - Our dedicated threat intelligence team monitors ransomware activity 24/7, scouring dark web channels, malware telemetry, and underground chatter.
   - If indicators suggest your organization is being targeted, our HALO team proactively reaches out with intelligence and support offers.
2. **Engagement and Command Activation**
   - We initiate secure out-of-band communication channels and create a war room for coordinated incident management.
   - Our incident commanders collaborate with your leadership and legal counsel to align communication and strategic response.
3. **Rapid Technology Deployment and Visibility Establishment**
   - We deploy Halcyon technology and forensic tools, including leading EDR and forensic technology, for complete inside-out visibility.
   - We extend visibility further with external attack surface management to detect and monitor entry points from the outside.
4. **Environment Hardening and Threat Mitigation**
   - We isolate and protect backups using immutable, secure methodologies.
   - We enforce enterprise-wide MFA and lockdown public-facing infrastructure.
   - Our team reviews and adjusts identity access, deprovisioning high-risk accounts, and cleaning up privileges.
5. **Real-Time Defense Operations**
   - When an attack begins, HALO transitions into active defense, monitoring the environment and disrupting attacker activity in real time.
   - Our expert services remain engaged until the threat is fully neutralized.
6. **Executive-Ready Reporting and Recommendations**
   - We provide high-level briefings to executive teams and boards.
   - Technical stakeholders receive detailed findings and tailored remediation plans.

Ready to Stop Ransomware Before It Starts?

Don't wait until ransomware actors are inside your environment. Partner with Halcyon to proactively disrupt attacks before they begin. If you've detected signs of reconnaissance, lateral movement, or early exfiltration, please **contact our Emergency Response Team if you see exfiltration or other activity pre-ransomware.**