RansomCARE

Proactive Risk Mitigation & 24/7 Incident Management - On-site and Remote

What is RansomCARE?

RansomCARE is a tailored ransomware defense program, crafted by offensive security experts; designed to mitigate the wide-ranging effects of ransomware attacks on businesses. It consists of 24/7 incident response and management, as well as proactive risk control and mitigation measures to deter attackers and to prevent the spreading of an attack to critical company assets.

RansomCARE reduces risks by providing your business with a robust line of defense against attacks that would otherwise cause devastating downtime and irrevocable financial losses.

How does RansomCARE work for me?

RansomCARE aims to make your company unattractive to attackers, deterring them with too much effort.

1. Security experts provide a **detailed threat map** identifying and categorizing your company's cyber-threat landscape both externally and internally.
2. Based on the risks specific to your enterprise, they create a customized response plan for incidents.
3. A handpicked team of experts is assembled to **handle live incidents**, and evolving **threats are met 24/7 in real time by advanced detection technology, preventative countermeasures and deceptive techniques.**
4. If an incident occurs, unique forensic analysis techniques are used to analyze all assets - disk, memory, and networks.
5. Infected network areas/endpoints/user IDs are isolated from the rest.
6. Attacks are stopped in their tracks.

WHAT SHOULD YOU EXPECT?

- **Stops active ransomware attacks in their tracks**
- **24/7 real time and effective incident response**
- **Advanced and sensitive threat detection and intelligence insights**
- **Multi-faceted prevention countermeasures**
- **Deceptive techniques**
- **Unique forensics analysis techniques**
- **Upgrades cyber awareness, security procedures and policies.**
- **Tailored strategy evolves quickly with changing threats.**
- **Elevates company's security posture and matures organizational cybersecurity program**

How can enterprises keep up with today's ransomware threats? By staying ahead of them.

Protecting organizations against ransomware attacks goes beyond endpoint and network security. According to Gartner, defenses must encompass many different security tools and controls. Figure 1 shows **RansomCARE's lifecycle** which includes many different checks and techniques. Our team of white-hat hackers have a powerful impact as they have access to the same sophisticated tooling and knowledge that is available to major cyber criminal groups. They can quickly point towards the main cyber vulnerabilities that exist, and handle them proactively.

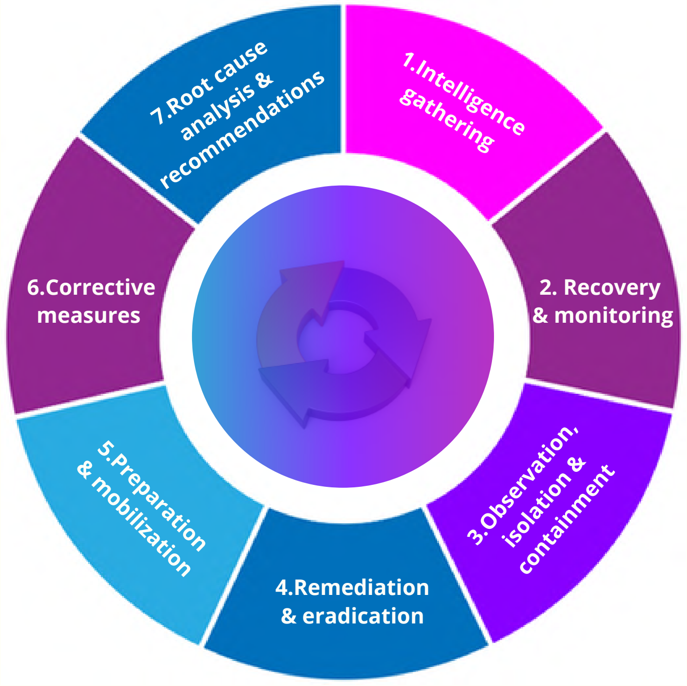
1.Intelligence gathering
2. Recovery & monitoring
3.Observation, isolation & containment
4.Remediation & eradication
5.Preparation & mobilization
6.Corrective measures
7.Root cause analysis & recommendations

Figure 1: RansomCARE's lifecycle

24/7 prevention and remediation

If a ransomware attack is already under way, it should be stopped in its tracks and not be allowed to progress and spread to important areas in the organization with critical assets.

Our **nation-state grade experts** investigate ransomware incidents and reveal entry points, essential attack components and the evolution of each attack. **This is crucial in the first few hours of an attack as it can completely change the outcome and prevent catastrophic loses.** Then, they provide focused recommendations on how to block the attackers and related route of access, as well as methods to improve security controls, counter-measures, and implementation of safeguards going forward.

Nation-state grade digital forensics

If you reached us after an attack has been launched, and we have already handled the threat, the next crucial step is to conclude which attack vector was used and how specifically it was exploited, which parts of the enterprise have been compromised (endpoints, network segments, user privileges, etc.) Digital forensics can shine a light into the gaps that were exploited and close them up for good, as well as preventing further damages from the current attack.

> ***"We realized that ransomware attacks were a major cybersecurity challenge that we needed to handle. HolistiCyber's team investigated our greatest vulnerabilities and security gaps and then set us up with new risk control policies and techniques. Now we had a solid incident response plan based on what is most critical to the business. When we actually had an attack, HolistiCyber handled it quickly and we had little downtime."***
> CISO, Healthcare Organization, USA