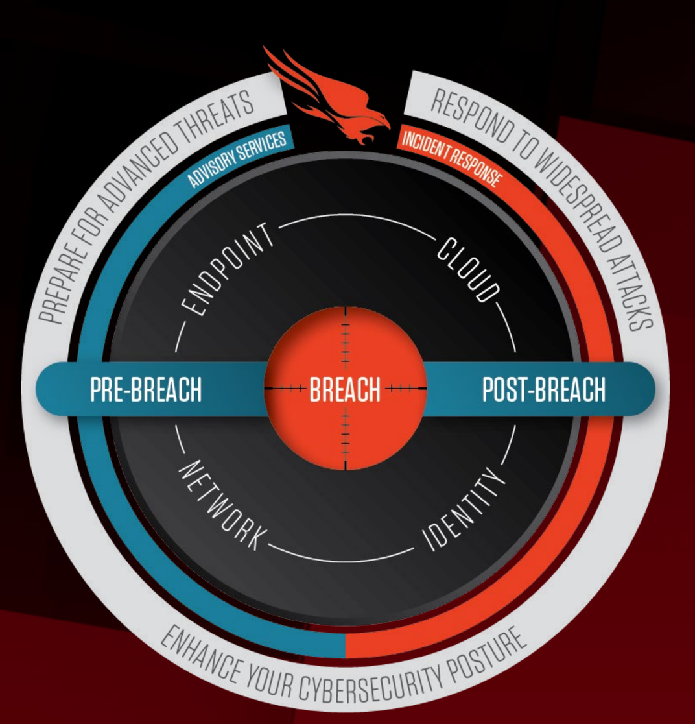
CROWDSTRIKE



CROWDSTRIKE INCIDENT RESPONSE

A modern approach to rapid response & recovery from today's widespread security incidents

Widespread Ransomware Attacks

Threat Actor: Cozy Bear has leveraged large-volume spear phishing campaigns to deliver an extensive range of malware types as part of an effort to disrupt entities across a variety of sectors. A distinct characteristic of this adversary's modus operandus is the persistence and focus on specific targets, typically manifested through repeated attempts to re-acquire and establish access to networks where they have previously lost operational control.

Navigating through the labyrinth of ransomware attack.

How will your respond?

INTELLIGENCE-LED, RAPID RECOVERY APPROACH

0. **Rapid Technology Deployment:** cloud-based deployment of the Falcon platform and sensor
1. **Immediate Threat Visibility:** enables us to quickly understand the full threat context and navigate the fastest path to business recovery
2. **Active Threat Containment:** block and prevent the spread of the attack to other systems on the network
3. **Accelerated Forensic Analysis:** collect relevant artefacts from select subset of infected systems and conduct triage analysis of threat tradecraft
4. **Real-Time Response & Recovery:** armed with the intelligence of knowing what actions a threat actor executed, surgically undo and remove the threat to recover the endpoints with speed and precision
5. **Enterprise Remediation:** reduce the number of systems requiring full remediation (reimage or rebuild) to a manageable number of systems
6. **Monitoring & Threat Hunting:** monitor the environment for hands-on-keyboard threat activity and stop any reinfection that may occur
7. **Managed Detection & Response:** stop future attacks by detecting threats within 1 minute, investigating attacks within 10 minutes, and responding to threats within 1 hour

CROWDSTRIKE VALUE

- Intelligence-led rapid response
- Greater visibility for better decision making
- Recover systems with real time response
- Accelerated investigation
- Lower cost remediation
- Reduced adversary impact
- Minimize downtime
- Avoid business interruption

GET BACK TO NORMAL BUSINESS OPERATIONS FASTER

TRADITIONAL RECOVERY APPROACH

0. **On Premise Technology Deployment:** ship servers, fly in consultants and install locally before response and recovery can begin
1. **Run Security Scans:** perform retroactive and iterative scans looking for Indicators of Compromise
2. **Limited Threat Visibility:** lack of real-time, Intelligence enriched telemetry, and 24/7/365 threat hunting
3. **Collect Full Disk Images:** capture a full disk image of every infected system (could be petabytes of data that takes days to capture)
4. **Collect All Log Files:** capture all log files (also could be petabytes of data that takes days to capture)
5. **Reimage Systems from Backup:** if backups are available, attempt to restore system data prior to compromise of every infected system
6. **Rebuild Systems:** rebuild / reinstall operating systems of every infected system
7. **Rerun Scans:** reinstall or redeploy scanning technology to every rebuilt or restored system
8. **Reinfection Occurs:** Start process over, go back to step 5

INCREASED RISK

- Slow technology deployment
- Requires boots on the ground
- Delayed incident response
- Limited visibility to actual threat
- High risk of system reinfection
- Long reimage and recovery time
- Lower chance of successful remediation
- Prolonged and expensive investigation

FACE SIGNIFICANT BUSINESS DISRUPTION COSTS

CROWDSTRIKE MAXIMIZING IR EFFICACY

AS MUCH AS:

5X REDUCTION IN TIME

10X REDUCTION IN COST

- Reduce recovery cost
- Avoid business disruption cost

Download the full Incident Response eBook to learn more about the seven key ingredients to maximize IR efficacy and respond to widespread ransomware and other malware attacks with speed and surgical precision.

GET THE EBOOK

Learn more: **https://www.crowdstrike.com/services/**

Follow us:

CROWDSTRIKE

We Stop Breaches