

SOLUTION QUICK CARD

CRITICALSTART® Incident Response Monitoring

KEY BENEFITS

- ✓ Resolve incidents in days, not weeks, and return to normal business operations faster than industry norms
- ✓ Promptly respond to security incidents and minimize their impact
- ✓ Reduce risk exposure and identify unknown attacker Tactics, Techniques, and Procedures (TTPs) through application of TTP Playbooks and constant tuning of automated alerts and blocking mechanisms
- ✓ Preserve evidence through comprehensive aggregation of alerts and artifacts
- ✓ Improve your overall security posture with enhanced visibility into activity within your environment
- ✓ Establish baselines through continuous monitoring
- ✓ Control the scope and severity of alerts for which you are notified and the cadence of those notifications

Rapidly identify, contain, and remediate threats to stop the bleeding.

Our IR Monitoring service utilizes the power of our Zero Trust Analytics Platform™ (ZTAP™) to help identify, contain, and remediate threats, as well as to support targeted threat hunting operations during a breach. This service includes:

- Active 24x7 monitoring by seasoned professionals and purpose-built technology
- Context-based alert prioritization tuned from each customer's threat assessment and business impact analysis
- 30-day demo license for integrated EDR products
- Leveraging global and customized/personalized playbooks and threat intelligence

Handle breaches across diverse attack vectors.

We handle criminal and non-criminal matters related to a wide variety of incidents, including:

- Malware-based attacks (*Ransomware, Trojans, etc.*)
- Phishing attacks
- Zero-day attacks
- Password attacks
- IoT attacks
- Critical Infrastructure attacks
- Cryptojacking
- Insider threats (*espionage, fraud, etc.*)
- Financial crimes
- Business Email Compromise



ZTAP dashboards allow our Cyber Incident Response Team (CIRT) and your analysts to communicate and collaborate in real time to investigate and remediate unknown alerts faster.