CRITICAL INCIDENT RESPONSE TEAM (CIRT)

Compromise Assessment

Uncover hidden threats and secure your networks

Your advanced security programs may be missing threats

In the ever-evolving cybersecurity landscape, even the most advanced security tools and methodologies can miss critical threats due to:

Alert fatigue: The sheer volume of alerts can overwhelm security teams, leading to ignored or missed true positives.

Tool permissiveness: To avoid business disruption, security tools may be configured to be too lenient.

Outdated rules: As a network evolves, previously written alerting rules may become obsolete and ineffective.

Fast-changing threats: Threat actors constantly adapt and update their tools and methodologies. This can outpace static defenses.

Wipro's CA offering, delivered by our specialized Critical Incident Response Team (CIRT), uses tried-and-true incident response methodologies to ensure that you don't miss what your current setup might overlook.

Our Proactive Approach & Cutting-Edge Tools

Deploy

- Our DFIR agent can query over 350+ (and counting) forensic artifacts.
- Remains at rest until activated by an analyst for zero impact on your network's performance.

Utilize

- Our OpenXDR engine ingests and interprets network log data, giving you a comprehensive overview.

Leverage

- Audit logs and settings of various SaaS services like Microsoft 365,
- Salesforce, GitHub, etc., for a holistic security perspective.

Top 3 Use Cases:

Onboarding New SOC or Incident Response Retainer

- Kickstart your new security operations with a clean slate by identifying previously missed issues.
- Improve alert accuracy and reduce false positives.

Mergers & Acquisitions (and Divestments)

- Mandate a CA in acquisition contracts to enforce cybersecurity due diligence.
- Option to pass CA costs onto the target company.
  Ensure no data leakage during divestitures.

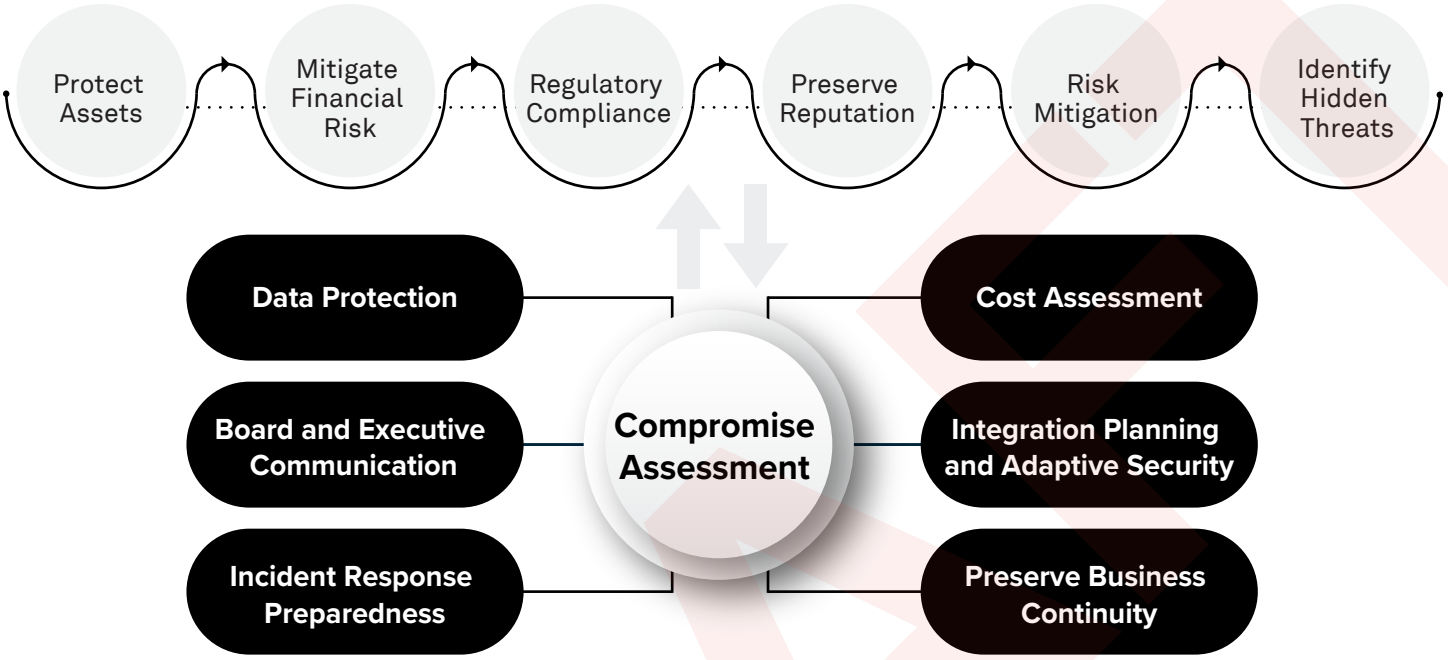
Annual Security Health Check-Up

- Consider it as a preventive "doctor's visit" for your network.
- Proactively detect and remedy vulnerabilities

An Industry-Leading Solution

Compromise Assessment is a proactive cybersecurity measure that involves analysis of an organization's environment to identify potential or actual security breaches or compromise.

It is used to identify activity that current security tooling may have missed: unauthorized access, lateral movement, system/application vulnerabilities, data exfiltration, mis-configurations, etc.



Our Strategic Partnerships

OBSIDIAN · STELLAR CYBER · Trellix · CYBLE · VECTRA · b!nalyze · Right-Hand CYBERSECURITY · Recorded Future

Connect with us to get started

If your organization is currently under attack, in need of proactive services, or you want to learn more about how Wipro's Critical Incident Response Team can secure your digital frontier, please contact us.

Ryan Anschutz
Americas Lead, Critical Incident Response
ryan.anschutz@wipro.com

Jeff Hamm
EU & APMEA Lead, Critical Incident Response
jeff.hamm@wipro.com

Wipro: Cybersecurity by Cybersecurists

Wipro, a leading technology services and consulting company, provides cybersecurity expertise to the world's leading organizations. Our strategy-first model, Wipro CyberTranform℠, optimizes today's enterprise journey to the cloud and modernizes identity and security programs through a risk lens and expert compliance knowledge. Wipro CyberShield℠, which defends business operations by providing on-demand cyber resilience management, is an as-a-service model at scale. We secure the modern enterprise by transforming risk into opportunity with solutions that increase business agility and create a competitive advantage for our clients. To learn more, visit **wipro.com/cybersecurity**

wipro cybersecurity
by cybersecurists