GoSecure

SECURITY COMPROMISE ASSESSMENT

Have you been breached? It's the question every organization should be asking in today's threat environment. You need to identify ongoing and past attacks that may be compromising your sensitive data across the network, endpoints and the cloud. Our GoSecure Security Compromise Assessment will answer these questions and help understand how best to move forward.

KEY BENEFITS

GoSecure Security Compromise Assessment delivers 60 days of GoSecure Managed Detection and Response (MDR). Our team of experienced threat hunters identify the hidden malware and advanced adversaries that have breached your IT infrastructure.

- Identify threats compromising your sensitive data and business operations.

- Assess your defensive capabilities and how they perform against sophisticated attacks.

- Improve your ability to detect and mitigate future compromises.

SCA delivers a C-Level report summarizing all risk to your environment, including: network traffic analysis, endpoint detection and response and more.

IDENTIFY PAST AND ONGOING ATTACKS ON YOUR IT ASSETS

The GoSecure Security Compromise Assessment (SCA) delivers comprehensive and detailed investigation of advanced malware and advanced adversary activity. It covers the network, the endpoints and the cloud - identifying past and ongoing threats in your IT infrastructure. Our SCA applies a hybrid approach using automated malware/anti-virus scans and active human threat hunting, including:

- A dedicated and experienced threat hunting team.
- A remote threat hunting agent deployed on those endpoints determined to be in scope.
- Automated antivirus and malware scans. Network traffic monitoring.
- Log analysis.

Backed by our team of Active Response Center threat hunters, our SCA alerts you as soon as a threat is detected. For every alert, we offer guidance and provide recommendations to secure the network and to re-establish and maintain an effective security posture.

Unparalleled Detection
Leveraging a Big Data approach coupled with a hybrid threat intelligence model, MDR achieves un-surpassed detection of threats in today's complex environments.

Endpoint Protection
Active mitigation capabilities to protect your endpoints whether the target system resides inside or outside your corporate network.

Collaborative Model
Offering a client partnership approach, the Active Response Center becomes an extension of your own.

24/7 Cybersecurity Force
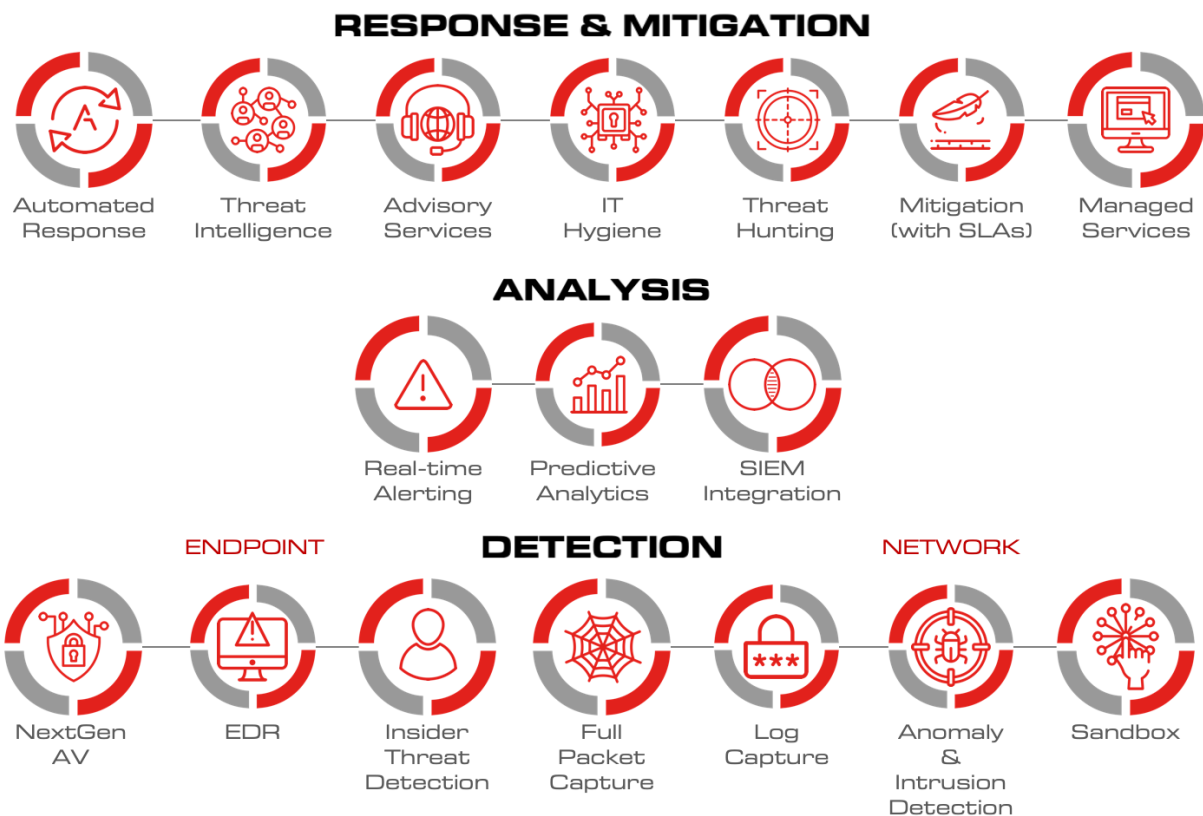Guaranteed access to trained incident responders at any hour.

Dedicated Hunt team
Trained to ferret out even the seemingly innocuous indicators of compromise.

The GoSecure Security Compromise Assessment approach includes:

- An assessment of the site's network security architecture to ensure proper deployment and maintenance of the technical network infrastructure.

- Ensuring that the agent can communicate back to our SCA team cluster by creating exceptions on the endpoint's own firewall or on the actual firewall devices, as needed.

- Comprehensive analysis of the environment focused on finding evidence of ongoing or past compromise. A view into systemic risks and exposures.

- Identification of security hygiene issues, such as poor patch management.

- Recommendations to improve your organization's ability to more effectively respond to future incidents.

- Flexibility to deploy on-premise or on cloud-hosted technology.

RESPONSE & MITIGATION

Automated Response | Threat Intelligence | Advisory Services | IT Hygiene | Threat Hunting | Mitigation (with SLAs) | Managed Services

ANALYSIS

Real-time Alerting | Predictive Analytics | SIEM Integration

ENDPOINT **DETECTION** NETWORK

NextGen AV | EDR | Insider Threat Detection | Full Packet Capture | Log Capture | Anomaly & Intrusion Detection | Sandbox