Industry - IT & Cybersecurity Services

Cybersecurity Incident Response | Real-Time Threat Detection and Containment

An organization partnered with NGEN to rapidly detect, contain, and remediate a credential-based cyber threat, ensuring zero business disruption while strengthening long-term security resilience.

The Challenge

The organization faced a high-risk security incident that required immediate response:

- Credential compromise after a user entered details into a phishing site
- Need for real-time detection of abnormal login behavior
- Urgent requirement to contain the threat and prevent lateral movement
- Attempted persistence through a malicious inbox rule
- Ensuring the incident was resolved without disrupting business operations

About the Client

The organization relies on secure digital systems and remote access to support daily operations and collaboration. Protecting sensitive data and maintaining uninterrupted access to systems is critical to ensuring business continuity and operational trust.

The NGEN Solution

NGEN deployed an integrated security monitoring and automated response framework to detect, contain, and remediate the threat in real time:

Layered Defense Architecture

- SIEM integration for real-time detection of anomalous login activity
- SOAR automation to immediately disable compromised accounts and document incidents
- Continuous endpoint and network monitoring for user activity and traffic analysis
- Detection and removal of persistence mechanisms, including malicious inbox rules

Unified Security Platform

- Zero Trust, always-on VPN with role-based access controls
- Endpoint Detection and Response (EDR/NGAV) for AI-driven threat protection
- Managed eXtended Detection and Response (MXDR) with 24×7 SOC monitoring and response

The Result

The incident was contained immediately while also strengthening the organization's long-term security framework:

Immediate Business Outcomes

- High-risk login detected within minutes
- Compromised account automatically disabled
- Malicious inbox rule removed before impact
- Zero lateral movement or broader system compromise
- Incident resolved with minimal operational disruption

Long-Term Strategic Benefits

- Stronger, proactive security posture with continuous monitoring
- Improved visibility through centralized logging and controls
- Faster response to future threats with automation in place
- Enhanced compliance and governance across systems
- More resilient, future-ready cybersecurity environment

Client Feedback

"NGEN's rapid response and automated security controls helped us contain a serious threat before it could impact our operations. Their team provided both immediate protection and long-term confidence in our security posture."

10003 Derekwood Lane, Ste.
201 Lanham, MD 20706

(888) 984-8964

www.ngen.com

Contact Us