protiviti®

Face the Future with Confidence

Compromise Assessment

Detect and Respond to Attacks with Confidence

As the IT landscape continues to increase in complexity, organizations like yours find themselves struggling to detect and respond to threat actors who are targeting sensitive information and customer data. Attackers may spend months gaining footholds and learning about the environment before executing an attack, whether it be a fraudulent wire transfer, theft of large amounts of data, a ransomware attack, or a combination of these or other threats.

Combined with more focus from boards and audit committees, you are likely being asked to answer tough questions about the state of security controls: Would we know if we were being attacked? Has our network been compromised? Are we ready?

Are you ready to respond in the event of a compromise?

Protiviti helps you answer these tough questions and more by conducting a **Compromise Assessment**. This assessment helps clarify the potential threats to your organization, examines your network for indicators of compromise and provides guidance on how to respond if malicious activity is detected.

Our Approach

Gather Information and Understand Your Security Posture

Protiviti will gather information about your organization through facilitated sessions with key stakeholders, information security personnel and application owners. Using this information, we will structure the assessment to focus on the critical components of your environment and the systems and data that would most likely be targeted by an attacker.

Evaluate Detection Capabilities and Perform Threat Hunting

Protiviti's incident response team will perform technical configuration reviews of security devices, examine relevant threat intelligence and dark web information, and perform automated and manual targeted threat hunting in the environment to assess your approach to detection and response.

Report and Debrief

Leveraging the information obtained from the assessment, we will develop a summary memo detailing the risks identified, potential impact to the business and guidance for remediation. We will simultaneously work with your technical leaders to conduct a detailed debriefing of the technical gaps and any threats identified during hunting activities.

Compromise Assessment

Threat Modeling

- Perform a high-level threat modeling exercise to identify the most likely threat actors who would target the organization and the techniques most likely to be used during an attack
- Identify the critical systems, applications and data that would be targeted by attacks
- Leverage the information obtained to determine the most likely attack techniques from the MITRE ATT&CK framework

Detection Capability Review

- Identify the various detection systems in use in the environment, such as Intrusion Detection/Prevention Systems (IDS/IPS) and Security Information Event Management (SIEM) tools to identify potential gaps in network visibility
- Perform configuration reviews of IDS/IPS and SIEM systems to evaluate the organization's ability to detect threats and respond to incidents

Threat Intelligence Analysis

- Identify potential threats using Protiviti's threat intelligence feeds, open source information and dark web accesses
- Provide information on any intelligence located on the dark web or evidence of threat activity

Incident Response Procedure Review

- Review the organization's incident response policy and any associated playbooks and compare them to industry standards
- Interview key incident response team members to understand processes for handling malicious threat actors

Threat Hunting Exercise

- Deploy an industry-leading tool, Carbon Black EDR/Enterprise EDR, to systems in the environment
- Perform automated hunting leveraging Carbon Black's Predictive Security Cloud
- Execute manual hunting using the threat modeling information to attempt to identify any malicious activity on the internal network

Reporting and Debrief

- Deliver an executive summary memo outlining the identified issues, risks and remediation guidance
- Deliver a detailed readout of hunting activities performed
- Conduct a debrief session with client management and technical leadership to outline the testing performed and results

Schedule a Compromise Assessment today by contacting us at TechnologyConsulting@Protiviti.com.

Protiviti.com/TechnologyConsulting

TechnologyConsulting@Protiviti.com

TCblog.Protiviti.com

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 85 locations in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®

Face the Future with Confidence