GoSecure

CASE STUDY

FORTUNE 500 INSURANCE COMPANY

HOLISTIC OFFENSIVE SECURITY TESTING FOR DISTRIBUTED, REMOTE WORKFORCE

"Like many companies, we've increasingly adapted for remote work; however, the type of cyber threats we face required us to look for a partner with the ability to tailor their adversarial emulation exercises to our specific mean time to detect goals."

—Director of DevSec-Ops

A COMPANY WITH A REMOTE WORKFORCE BUILDS CONFIDENCE AND IMPROVEMENTS INTO THEIR ORGANIZATION'S READINESS FOR A REAL-WORLD ATTACK

BACKGROUND

This Fortune 500 company provides diversified insurance and financial services in the United States and maintains strict standards to protect their brand, their employees and their customers. The insurance industry is very much a target for cybercrime and is faced with managing a distributed and remote workforce. Because the security team anticipated that attackers would adjust to the remote and distributed workforce scenario, the company desired extensive testing of their security controls to ensure their controls would detect the likely tactics, techniques and procedures (TTPs) of attackers—and respond quickly. Their requirements necessitated the selection of an experienced partner with the ability to tailor an adversary simulation approach for their sophisticated security team's unique concerns and goals.

SOLUTIONS

With the overarching goal of reducing the Mean Time to Detect (MTTD), the GoSecure team structured the engagement to properly test the controls around the company's distributed and remote workforce. Each aspect of the testing was customized (not scripted), requiring an iterative approach in repeating the simulation exercises. In this way, GoSecure ensured that the people, processes, and technology involved could respond with short MTTD, even against a variety of attackers and TTPs. The custom engagement model ensured the maturity and efficacy of their program. It included:

- Long-Term Lightly Scoped Adversarial Emulation with the red team to test controls and measure respond times.
- Table-top exercise to test processes and personnel interdependencies for possible single points of failure.
- Purple team engagement to ensure the blue team received full transparency on what tactic worked against their defenses, and which response would be most effective.

BENEFITS

This insurance client, in partnership with GoSecure, achieved:

- Strengthened security posture and increased confidence in maintaining a distributed remote workforce.
- Reductions in Mean Time to Detect through operational improvements, real-time detections and alerts.
- Built-in redundancy to improve integration of people, process and technology.
- Improved visibility and knowledge in how to prepare for and respond to any future incidents.
- Validation of the efficacy of the existing cybersecurity programs.

[CONTACT US: +1-855-893-5428]

GoSecure is a recognized cybersecurity leader and innovator, pioneering the integration of endpoint, network, and email threat detection into a single Managed Extended Detection and Response (MXDR) service. The GoSecure Titan® platform delivers predictive multi-vector detection, prevention, and response to counter modern cyber threats. GoSecure Titan® MXDR delivers rapid response and active mitigation services that directly touch the customers' network and endpoints. For over 20 years, GoSecure has been helping customers better understand their security gaps and improve their organizational risk and security maturity through MXDR and Professional Services solutions delivered by one of the most trusted and skilled teams in the industry. To learn more, please visit:

www.gosecure.ai

Your ally to consolidate, evolve & thrive

GoSecure