FORTRA®

RED TEAM USE CASE

Insurance Provider

Background

A large insurance provider engaged in rapid technological advancement conducts a Red Team assessment to determine the security strength of their AI-powered tools against real-world attacks. Things like vulnerabilities and misconfigurations that could open potential attack paths are the subject of the engagement. The provider is swiftly undergoing increased AI adoption (e.g., for underwriting, claims automation, and fraud detection) while at the same time operating under evolving regulations. **Red Teaming** will reveal the ability of its new AI-supported tools to withstand adversarial tactics, as well as the carrier's ability to stay within compliance guidelines.

Phase 1: Initial Access Operations

The Red Team starts by gaining needed intelligence on the insurance provider's employees, internal architecture, and external partners (healthcare providers, technology companies, financial services platforms, customer management solutions, and third-party data providers).

- **Reconnaissance:** The Red Team discovers personal information on executives' LinkedIn profiles, along with a new AI-powered underwriting tool lacking sufficient access controls.
- **Spear Phishing:** Using the personal information gleaned in Reconnaissance, they leverage the **Outflank Security Tooling** (OST) Office Intrusion Pack to send a well-crafted spear phishing email to top insurance executives regarding an "update" to the National Association of Insurance Commissioner's (NAIC's) **AI guidelines**.
- **Web Drive-By Attack:** The Red Team places a compromising pop-up on the insurance provider's login page that downloads a keylogger to steal credentials every time a client clicks.

Phase 2: Lateral Movement & Privilege Escalation

Moving laterally gives the Red Team ample opportunity to maximize their malicious effectiveness once inside the system.

- **Credential Harvesting:** With OST's Credential Pack, they extract hashed passwords from memory and perform Pass-the-Hash attacks to gain deeper access.
- **Lateral Movement:** Red Teamers use OST's Lateral Pack to pivot into additional systems across the network and maximize the scope of their attack. These systems can include claims management systems, underwriting systems, and policy administration systems where sensitive client and policy details are stored.
- **Account Takeover:** A misconfiguration in the provider's new AI-powered underwriting tool allows the Red Team to escalate privileges, eventually achieving account takeover (ATO) of a C-suite account with full system access.

Phase 3: Maintaining Persistence & Evasion

Just like a real-world threat actor, Red Teams establish persistence into the provider's internal systems using covert measures.

- **Quiet Transmission:** DNS over HTTPS tunneling and HTTPS encrypted communication are used to communicate with the **Cobalt Strike** command-and-control server and exfiltrate data unnoticed.
- **Asynchronous Communication:** To avoid detection by security monitoring tools, Red Teams leverage asynchronous communication in which malware beacons at certain pre-set intervals, rather than constantly.
- **Remote Access Trojans (RATs):** Red Teams use RATs to establish backdoors into critical, compromised systems like the insecure AI underwriting app. These are used to maintain persistence into the insurance provider's internal assets and exfiltrate data over an extended period of time.

Phase 4: Simulated Attack Scenarios

Once the pieces are in place, the Red Team launches a simulated attack that mirrors the actions of advanced adversaries in the real world.

- **Ransomware Deployment:** They leverage OST's Fake Ransom to put the providers' detection, investigation, and response skills to the test.
- **Business and Client Disruption:** They demonstrate how an outside attacker could compromise the AI-powered underwriting app, grinding all new business to a halt until the issue is resolved.
- **Data Exfiltration:** Red Teamers extract customer policy data, sensitive health records, and personal contact information to draw attention to potential insurance compliance violations (under NIAC, HIPAA, GDPR, and state laws such as NYDFS (New York) and IIPPA (California).

Phase 5: Red Team Engagement & Blue Team Training

To maximize outcomes, the Red Team engagement must include Blue Team collaboration at every key step.

- **Shared Sessions:** Blue Teams are encouraged to look over the shoulder of Red Teams as they launch adversarial tactics in real-time.
- **Extensive Logging:** All attack vectors are recorded and logged for further forensic analysis and review post-engagement.
- **Purple Team Exercises:** After sharing findings, the Blue Team will improve its defensive capabilities based on the Red Team's discoveries when attempting to circumvent them. This creates a **Purple Team** mindset.
- **Incident Response Drill:** Based on the findings, the insurance provider's security team practices detecting, investigating, and responding to additional Red Team attempts to solidify new Blue Team capabilities.

Outcome & Lessons Learned

The purpose of this engagement is to draw attention to exploitable vulnerabilities and other weaknesses that could compromise an insurance provider's AI-based tools, sensitive customer data, or compliance standing.

- **Identified Weaknesses:** Insurance providers glean expert insights into weaknesses in their state-of-the-art technology, and the valuable client information it protects.
- **Security Improvements:** The provider implements recommended Blue Team security strategies and additional security measures such as integrity and compliance monitoring, advanced email security, and misconfiguration management for sensitive insurance software applications. This also includes improved monitoring and compliance oversight for AI-powered tools.
- **Enhanced Cyber Readiness:** The insurance provider makes a habit of performing regular, bi-annual **offensive security** engagements. This new, proactive approach ensures insurance compliance standards are being met and AI-powered technology remains operational and secure, stabilizing insurance revenue streams.

By discovering these security gaps first, Red Teams can give the provider's security team the benefit of time to shore up weaknesses before a real-world attack.

Advanced Red Team Tools

Industry-leading red team tools like Fortra's Cobalt Strike and Outflank Security Tooling empower red teams to create advanced adversarial simulations that keep pace with today's threats and help battle test organizations' security defenses.

Test your security team with the same advanced tactics used in the real world. Get Fortra's advanced red team simulations and top-of-the-line toolkits.

FORTRA®

Fortra.com

About Fortra

Fortra provides advanced offensive and defensive security solutions that deliver comprehensive protection across the cyber kill chain. With complete visibility across the attack chain, access to threat intelligence spanning the globe, and flexible solution delivery, Fortra customers can anticipate criminal behavior and strengthen their defenses in real time. Break the chain at fortra.com.