RED TEAM ACTIVATED: TESTING A GLOBAL RISK INTELLIGENCE PLATFORM

CUSTOMER SNAPSHOT

INDUSTRY	Technology – Software & Services
CUSTOMER	SaaS provider specializing in real-time risk intelligence for enterprise and public sector clients
SERVICES PROVIDED	Red Teaming

"Many vendors would have failed to add value in our environment – Bishop Fox didn't. They proved they can handle bleeding-edge companies."

— **SENIOR DIRECTOR OF CYBERSECURITY**

THE CHALLENGE:

To ensure its real-time AI platform could withstand sophisticated threats, a global SaaS company partnered with Bishop Fox for its first full Red Team assessment. The goal: simulate real-world adversaries to test internal detection and response capabilities.

The company faced several specific security challenges:

- Identify weaknesses a standard pen test might miss.
- Validate their internal team's and third-party SOC's responses to real-world attacks.
- Improve visibility into high-value systems.
- Prioritize future security investments.

"We did this to find the skeletons in the closet. This isn't for compliance; it's for real risk reduction."

— **SENIOR DIRECTOR OF CYBERSECURITY**

THE SOLUTION:

Having previously engaged Bishop Fox for application testing, the customer trusted the firm to deliver a comprehensive Red Team simulation tailored to its modern, cloud-native architecture. The engagement began with a collaborative scoping session to understand the company's AWS environment, business risks, and unique threat landscape. From there, Bishop Fox designed a two-phase assessment:

GOALS OF ENGAGEMENT

- **External Assessment (Partial-Knowledge):** The firm's Red Team successfully compromised a user account that did not use the client's supplied identity security provider via password spraying. This enabled them to access internal systems and expose over 250,000 customer and employee records, including sensitive PII and API keys. Despite later signs of suspicious activity, the incident was not detected in real time.
- **Assumed-Breach Scenario:** Using limited-access VPN credentials, the firm's Red Team identified an internal Docker registry, deployed a backdoored container through the CI/CD pipeline, and gained full access to the company's internal network ultimately escalating privileges to root the AWS environment.

"We didn't just want to see if our systems would break; we wanted to know if our team would actually catch it when they did. It was obvious Bishop Fox had done this 100 times before. Fast, organized, and respectful of our time – that's rare."

— **SENIOR DIRECTOR OF CYBERSECURITY**

Throughout the engagement, Bishop Fox's team demonstrated deep technical expertise, seamless execution, and a collaborative mindset.

THE OUTCOME:

The customer strengthened secrets management, logging, and detection tooling, and now treats red teaming as a core part of its annual security program. Future assessments will evolve to test stealthier attack paths and Kubernetes-centric infrastructure.

KEY RESULTS

- Exposed gaps in secrets management and credential hygiene
- Discovered multiple high and critical vulnerabilities, including full AWS root compromise
- Provided clear, actionable remediation guidance

"This work didn't just strengthen our defenses; it shaped how we're budgeting and investing in security going forward."

— **SENIOR DIRECTOR OF CYBERSECURITY**

ABOUT BISHOP FOX

Bishop Fox the leading expert in offensive security, providing comprehensive assessment of modern environments with continuous attack surface management, red teaming, and penetration testing for applications, cloud, network, and products. We've worked with more than 25% of the Fortune 100, half of the Fortune 10, eight of the top 10 global technology companies, and all of the top global media companies to improve their security.

LEARN MORE AT BISHOPFOX.COM