

FireCompass

Industry: E-commerce

Employees: 1001 - 5000

Products: FireCompass
RECON & ATTACK

Customer Profile

The Customer is an e-commerce platform for Beauty & Fashion Products.

They help their customers in providing product reviews, beauty how-to videos, expert articles on beauty products, and a magazine. Also, helps to choose products and services best suited for consumers' needs.

About FireCompass

FireCompass is a SaaS platform for Continuous Automated Red Teaming (CART) and Attack Surface Management (ASM). FireCompass continuously indexes and monitors the deep, dark and surface webs using nation-state grade reconnaissance techniques. The platform automatically discovers an organization's digital attack surface and launches multi-stage safe attacks, mimicking a real attacker, to help identify breach and attack paths that are otherwise missed out by conventional tools.

Large E-commerce Company

Challenges

01. Enumerating Digital Attack Surface & Asset Inventory Creation

The CTO's initial goal was to centralize control of the company's digital assets and understand the attack surface. However, these assets existed in siloed environments, and various departmental groups controlled the assets. Gathering an accurate, complete inventory (domains, sub-domains, IPs, mobile apps, landing pages, portals, forms, etc) would be a daunting task, given the number of unknown digital assets created in a decentralized manner and the security/IT group's lack of visibility.

02. Continuous Monitoring of Digital Cyber Risks

The CTO's other challenge was to analyse their current risk posture and monitor for future breach risks - like exposed UATs, Preprod Environments, Vulnerabilities, Subdomain Takeover Risks, Phishing Domains, Malicious Infrastructure, Employees' Personally Identifiable Information (PII) etc. on a continuous basis.

Solution

Attack Surface Discovery

- Domains/Subdomains/IPs/Applications
- Enumeration Preprod, UAT Systems, Online DBs Identification and Reporting

Attack Surface Monitoring

- Vulnerabilities (Through Passive Scanning) Monitoring
- Malicious Infrastructure Monitoring
- Open S3 Buckets Identification and Monitoring
- Code Leaks Identification and Monitoring
- Phishing Domains Monitoring

Red Teaming

- Continuous automated Red Teaming
- Active vulnerability assessment
- Infrastructure Security Assessment
- Penetration Testing

FireCompass

Industry: e-commerce

Employees: 1001 - 5000

Products: FireCompass
RECON & ATTACK

Customer Profile

The Customer is an e-commerce platform for Beauty & Fashion Products.

They help their customers in providing product reviews, beauty how-to videos, expert articles on beauty products, and a magazine. Also, helps to choose products and services best suited for consumers' needs.

About FireCompass

FireCompass is a SaaS platform for Continuous Automated Red Teaming (CART) and Attack Surface Management (ASM). FireCompass continuously indexes and monitors the deep, dark and surface webs using nation-state grade reconnaissance techniques. The platform automatically discovers an organization's digital attack surface and launches multi-stage safe attacks, mimicking a real attacker, to help identify breach and attack paths that are otherwise missed out by conventional tools.

Large E-commerce Company

Results

30% decrease in Attack Surface

With the help of FireCompass solution, the company has created an inventory of their digital assets, and removed assets which were not in use or not required.

Continuously Updated Asset Inventory

FireCompass - the internet wide continuous monitoring tool has helped the customer to have an up-to-date inventory of their digital internet facing assets, which were missing earlier.

Discovery and Mitigation of Unknown Shadow IT Risks

FireCompass helped the customer to track the exposed digital assets including:

- Exposed documents & files
- Compromised / malicious infrastructure
- Exposed pre-prod servers, database servers, RDP Servers
- Exposed backend APIs

Near Real-time Monitoring of Digital Risks

FireCompass helped them to monitor their attack surface on a daily basis, reducing chances of missing out new risks, and notified about some of the critical risks like online cameras with default passwords, online systems with vulnerabilities, leaked credentials, etc.
