ZAFRAN

Win the Exploitation Race

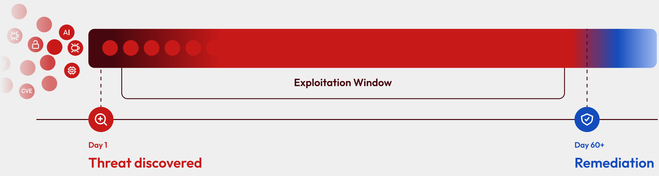
Zafran Risk & Mitigation Platform leverages existing security controls to protect organizations during critical exploitation windows

The problem

Exponential growth in emerging threats, coupled with increasingly swift exploitation , leaves organizations exposed to attack during the inevitable exploitation window, the time between a vulnerability is detected and remediation occurs.

60% of all data breaches were a result of a known vulnerability that was not remediated in time

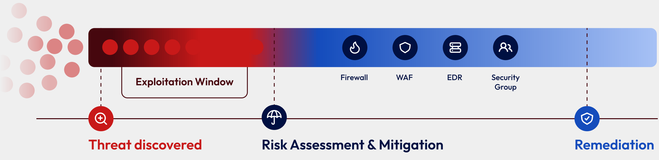
Verizon Data Breach Investigations Report



Solution Approach

Zafran brings a new approach by leveraging existing security tools (EDR, firewalls, cloud tools, etc.) to determine whether vulnerabilities are truly exploitable or already mitigated by compensating controls. Correlating control configuration, runtime, internet exposure, and threat intelligence exploit analysis, Zafran pinpoints true vulnerabilities and enables the automation of upstream mitigations to proactively reduce exposure at scale.

- **Hybrid environment (on prem & cloud)**
- **Agentless**
- **Control configuration**
- **Human in loop automation**



Use Cases

Applicable Risk Assessment

Anazlye risk taking the controls and exploitability into account and measure risk over time

New approach to Vulnerability Management

Reduce time under risk by considering existing compensating controls configurations

Security Control gaps & Blindspots

Bridge gaps between planning and executions of your defense-in depth strategy

Mitigation & Automation

Mobilize controls to proactively reduce risk at scale by evaluating existing controls effectiveness against the threat

How We Do It

Easy deployment through API integrations with existing security stack

Integrate & Discover

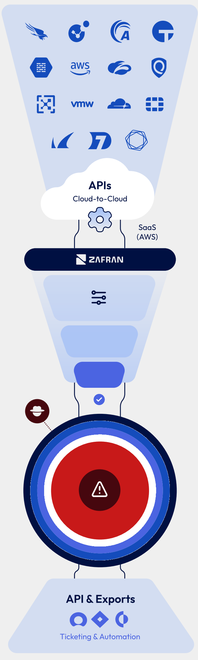
- **Agentless** approach connecting to the organization existing security tools via cloud-to-cloud **API keys** (on prem & Cloud)
- **Runtime inspection** to collect vulnerability data, asset details and **dynamic SBOM**
- **Security Control Analysis** to gather VM tools data, Network controls (firewall, WAF, WAP, IDS, IPS) configurations, and Host controls (EDR) configurations

Assess & Pinpoint

- **Analyze control configurations, asset context, runtime, internet & network exposure**, exploit threat intel holistically and normalize the data
- **Correlate controls and threats** for a comprehensive Applicable Risk assessment, accounting for existing mitigations
- **Pinpoint exploitables,** security controls gaps & blindspots and exposed assets for effective prioritzation

Mitigate & Automate

- Leverage ever-growing **mitigation knowledge base,** covering network, web, and endpoint mitigations, translating them to the customer's specific assets and available controls
- **Proactively preform upstream mitigations**, adjusting existing tools to block exploits and reduce exposure at scale
- Integrate to existing processes and tools to **automate mitigation process** (Ticketing, Email, XSOAR)



Zafran was founded by a team of cybersecurity experts with experience from Israeli intelligence and leading threat intel and cyber companies and is backed by Cyberstarts and Sequoia Capital. Zafran is bringing a new approach to win the exploitation race without business disruption. Zafran is based in New York with operations in Tel Aviv.

zafran.io

info@zafran.io