OBSIDIAN | CROWDSTRIKE

SOLUTION BRIEF

Stay Ahead of Identity-Based Attacks from Endpoint to SaaS

Insights from the Obsidian Security-CrowdStrike incident response partnership

Introduction

SaaS applications play a key role in the success of modern businesses. However, it is important to note that these applications come with significant security risks that must be addressed to ensure the protection of critical business data. Attackers are aware of this and are constantly trying to breach an organization's network of SaaS applications to get their hands on sensitive information. Recent public attacks such as Microsoft, MGM, and HPE show that attackers are becoming more sophisticated and are using various methods to infiltrate a company's SaaS ecosystem.

To address this issue, Obsidian and CrowdStrike have collaborated to develop a robust Incident Response (IR) strategy that quickly detects and resolves incidents while also paving the way for avoiding future ones. This solution ensures end-to-end protection of all applications in an organization's SaaS environment and effectively responds to SaaS-related security incidents.

Over the past year, our teams have encountered numerous advanced persistent threats (APTs) to SaaS. We have compiled a detailed strategy to help prevent these threats from negatively impacting your business.

INCIDENT RESPONSE

How CrowdStrike leverages Obsidian to investigate and mitigate today's surging SaaS breaches

Adversary-in-the-Middle (AiTM)

This type of attack involves phishing or smishing, a tried and true method that aims to steal tokens. It's crucial to understand that even if your organization has widely implemented MFA, it doesn't guarantee complete protection against phishing or smishing attacks targeting authentication tokens. To address this, CrowdStrike leverages Obsidian to identify and notify about login attempts and the associated risk factors such as unusual location, devices, or VPN usage.

Helpdesk Social Engineering

In this scenario, a malicious individual contacts the help desk by pretending to be an employee of an organization, often someone with significant permissions, such as an IT professional. They confirm their fake identity by acquiring the victim's Social Security number, which, unfortunately, is relatively easy to obtain. The attacker then requests a password reset and the activation of a new MFA device. Once this is done, they move on to access valuable assets such as IT documents, VPN configurations, and may even conduct searches to gain insight into the organization's infrastructure.

To prevent such attacks, CrowdStrike deploys Obsidian to detect if a new MFA has been activated and whether the IP address, device, and location that made the request is suspicious. Even if the help desk resets the password, Obsidian can still alert on various suspicious activities to aid in remediation, such as unusual SMS activation, document reconnaissance, and inbox rules after the password change.

SIM-Swapping and Self-Service Password Reset (SSPR)

Cybercriminals can steal a user's phone number and use SSPR to change their password and gain access to the victim's account. All they need is the victim's phone number and username. The attacker will receive a link to reset the password via SMS. CrowdStrike uses Obsidian to detect such password reset attempts. Obsidian compares the request to the IP address, location, and device ID of the person who made the request and quickly determines if it is anomalous based on historical data.

PLATFORM INTEGRATION

Obsidian and CrowdStrike work better together

When you connect the Obsidian Security and CrowdStrike Falcon platforms, you get full visibility and uncompromising security that extends from devices to the cloud. That's because the CrowdStrike and Obsidian platforms benefit from underlying graph architectures, enabling more flexible data management and higher fidelity threat detections for endpoints and SaaS, respectively.

In practice, this means your team will have a consolidated picture of every user's associated endpoints and SaaS accounts. Obsidian correlates normalized SaaS telemetry with insights from the CrowdStrike platform to uncover vulnerabilities and identify threats with unparalleled speed and accuracy—which is critical as bad actors move between compromised devices and the cloud.

How attackers traverse the system beyond the endpoint

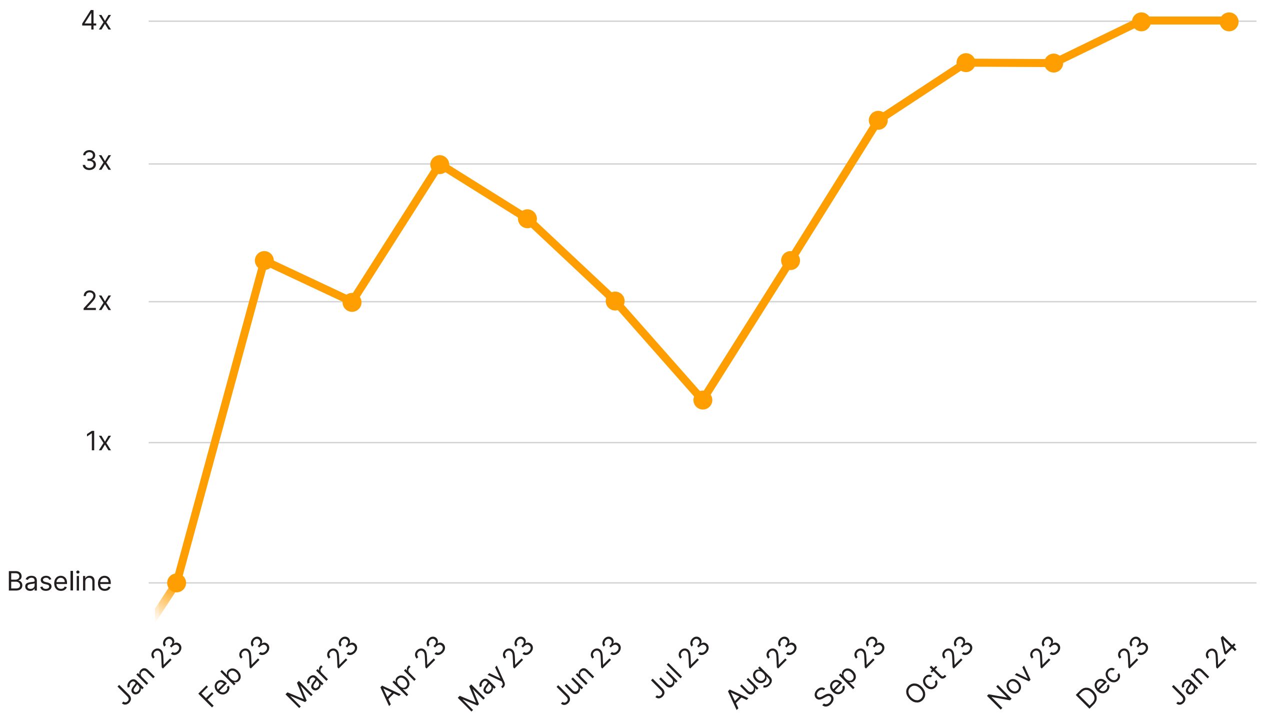
By engaging with partners like CrowdStrike in numerous IRs, Obsidian has gained deep visibility into how attackers breach SaaS applications.

After the initial endpoint breach, attackers are able to move downstream in order to steal more information without getting caught. Some additional damage that may occur includes:

- Creating inbox rules that forward or delete email messages
- Deletion of security notifications
- Service principal changes
- Creation of accounts
- Mailbox permission changes
- Access to SaaS applications (Workday, SFDC, etc.)
- Wire fraud
- Financial theft
- Exfiltration and extortion
- Ransomware

As the usage of SaaS applications grows, attackers target SaaS more than ever due to the treasure trove of sensitive information stored within SaaS applications and the high likelihood of gaining access to numerous downstream applications. This is evidenced by an increasing number of incident response engagements involving SaaS applications over the last year.

The volume of monthly SaaS breaches, 2023–2024



The Obsidian Advantage

Correlate user activity across endpoints and SaaS applications for a more thorough and contextual understanding of user identity, access, and activity in your environment. Obsidian surfaces native detections from CrowdStrike within the platform. At the same time, we correlate endpoint and SaaS data to deliver unified activity timelines and more robust threat detections across your entire organization.

Harden your security posture and minimize risk by proactively addressing vulnerabilities and policy issues across cloud applications and endpoints. Eliminate opportunities for attackers by tightening application configurations, limiting access from unsanctioned devices, identifying unused accounts and reducing unused privileges, and aligning with a number of other security best practices.

Mitigate threats quickly and confidently with a complete picture of malicious activity moving between endpoints and SaaS applications. Your security team will have immediate answers to critical questions during the investigation of an incident.

Obsidian Security on the CrowdStrike Marketplace

Obsidian Security is proud to be available on the CrowdStrike Marketplace, a one-stop destination and world-class ecosystem of third-party security products. This makes it easier than ever for existing Falcon customers to try, buy, and integrate with the Obsidian platform.