OBSIDIAN

SOLUTION BRIEF

Obsidian for SaaS Incident Response

Prevention, detection, and rapid response for SaaS security incidents with Obsidian Security

The Importance of Incident Response for SaaS

The importance of a thorough incident response strategy cannot be understated as organizations prepare to identify, investigate, and resolve threats as effectively as possible. Most security veterans are already well aware of this fact, and their teams have proactively defined plans that cover every step of an incident lifecycle. But as businesses migrate increasingly to SaaS, incident response teams are challenged to adapt and evolve their strategies to protect applications over which they have far less visibility and control.

The National Institute of Standards and Technology (NIST) has established guidelines around the incident response lifecycle, a process which they separate into four distinct phases: **preparation; detection and analysis; containment, eradication, and recovery; and post-event activity.** These principles serve as an invaluable reference for other organizations to develop and improve their own response capabilities.

When it comes to the security of SaaS applications, most teams will find that their response capabilities fall short. Effective incident response for SaaS necessitates a complete understanding of the environment—your users, your applications, and your connected integrations—which security teams relying on legacy solutions just don't have.

Complete Incident Response with Obsidian

With industry-leading posture management and threat detection capabilities for SaaS, Obsidian Security helps teams respond to incidents affecting business-critical applications and implement measures to prevent them from reemerging. Whether it's an account takeover, an insider threat, or a compromised third-party integration, Obsidian provides complete coverage for every step of the incident response life cycle.

Making Obsidian a part of your incident response toolkit couldn't be any easier with frictionless integration directly into your existing workflow. Organizations using CrowdStrike endpoint detection and response, for example, can connect Obsidian to extend visibility into SaaS and investigate threats as they move from devices to cloud applications. Integrate with ticketing platforms like Jira and ServiceNow, or SIEM and SOAR platforms to operationalize Obsidian detections in your team's preferred way.

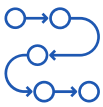
CROWDSTRIKE

CrowdStrike uses Obsidian for SaaS incident response

The world-class Incident Response Services team at CrowdStrike published a blog breaking down "multiple investigations into an intrusion campaign targeting telecommunications and business process outsourcing (BPO) companies." In each investigation, they leveraged Obsidian to uncover and eradicate attacker presence in SaaS platforms including Microsoft 365, Azure Active Directory, and Google Workspace. Learn more.

Detection and Analysis

Obsidian continuously collects and normalizes data around how your users and integrations are behaving. Our cutting-edge machine learning models use this baseline to identify threats with unmatched speed and accuracy, giving your security team the opportunity to respond to incidents earlier.



Containment, Eradication, and Recovery

Triage in SaaS environments can be difficult due to the complexity of interconnected applications, integrations, and users. When Obsidian identifies a threat, it details every action an adversary takes from initial access to impact, along with any lateral movement across services. With this context, your team can contain incidents and mitigate persistence completely.

Post-event Activity

Every thorough incident response should conclude with a period of reflection, review, and improvement. With a unified timeline of malicious activity and rich context to support every threat detection, Obsidian helps your team revise key findings and compile more detailed postmortem reports.

Prevention

Obsidian surfaces risk across your SaaS environment in its different forms—weak configurations, excessive privileges, and insecure third-party integrations—along with a measure of severity to help your team prioritize the most impactful decisions. Addressing these vulnerabilities minimizes opportunities for incidents to reoccur in the future.

Get Started

Interested in learning more about Obsidian Security and how our platform can help you improve your SaaS incident response capabilities? Get started with a no-cost risk assessment of your SaaS environment and receive a full report including actionable recommendations to improve your security posture.

© Copyright 2023 Obsidian Security, Inc. All rights reserved.
Other brands mentioned herein are for identification purposes only and may be the trademarks of their holders.