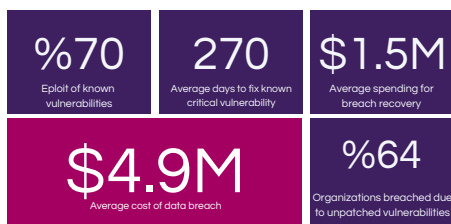




Why to use Offensive Security Manager Now



Organizations face complex security challenges that demand sophisticated solutions. Proactive cybersecurity is essential, as dealing with attacks after they occur is much harder. Offensive Security Manager (OSM) acts as a guard, closing security gaps and protecting against cyber criminals. With AI-driven capabilities, OSM offers comprehensive threat management and remediation, enhancing security posture, anticipating threats, and enabling swift responses.

Rapidly Increasing Risk

In 2023, over 25,000 vulnerabilities were reported, averaging 68 daily, with 60% classified as critical or high severity. Manual testing is insufficient; organizations need robust systems and immediate access to knowledge to prioritize and mitigate risks effectively.

Offensive Security Manager (OSM) elevates protection by focusing on issue and knowledge management instead of vulnerabilities. Using AI-driven capabilities, OSM continuously monitors and analyzes security data, identifying and prioritizing risks in real-time.

Lack of Risk Focus and Process Visibility with Tracking

The average time to patch a critical vulnerability is 270 days, leaving systems exposed for extended periods.

Offensive Security Manager (OSM) addresses patching delays by implementing robust process management with SLAs, escalations, and notifications.

Increased IT Environment Complexity

Managing vulnerabilities across network, web, container, and source code layers requires specialized tools and expertise. Each layer has unique challenges, and coordinating efforts with limited resources and skills demands a holistic, integrated security approach.

Offensive Security Manager (OSM) solves this problem by providing a holistic, integrated approach to managing vulnerabilities across network, web, container, and source code layers.

Lack of Skilled Resources

55% of organizations face a shortage of skilled cybersecurity professionals, struggling to find qualified staff for vulnerability management. Additionally, 75% of security teams are overwhelmed by the volume of daily alerts, leading to alert fatigue and missed critical threats.

Offensive Security Manager (OSM) addresses resource constraints by leveraging automation, AI-driven data enrichment, and streamlined process management.

Underutilized Tools and Disconnected Teams

Underutilized analysis tools in network, web, container, and source code layers stem from the extensive time and expertise needed to understand and solve problems. Security teams must decipher complex issues and coordinate with various teams, causing delays. This underscores the need for integrated and automated solutions to streamline processes and enhance security.

Offensive Security Manager (OSM) solves this problem by leveraging AI for data enrichment, issue prioritization, attack behavior prediction, and risk prediction across network, web, container, and source code layers.

Maintaining Regulatory Compliance

50% of companies struggle with regulatory compliance. Navigating the complex landscape of regulatory requirements is a persistent challenge, with half of the companies reporting difficulties in achieving and maintaining compliance.

Offensive Security Manager (OSM) simplifies maintaining regulatory compliance by providing built-in compliance frameworks and automated monitoring.

Financial Impact

The average cost of a data breach is \$4.88 million and increasing each year. Organizations spend \$1.5 million average annually on breach recovery.

Offensive Security Manager (OSM) mitigates the financial impact of data breaches by providing proactive and comprehensive security management.

Schedule a demo:

<https://www.ofsecman.io/schedule-demo>

