OSM Offensive Security Manager

Excelling in Proactive Security Management

An Innovative Approach

OSM

Whitepaper by

Offensive Security Manager

ofsecman.io

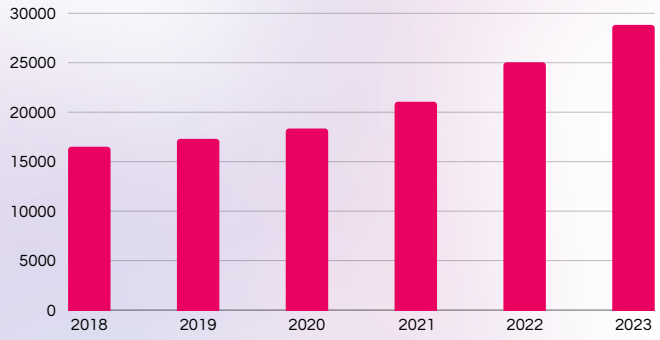
2024

OSM

Executive Summary

Organizations today face complex security challenges that demand sophisticated solutions. Proactive cybersecurity measures are crucial for staying ahead of threats and protecting corporate networks and data. While offensive security is invaluable, it presents unique management challenges that can overwhelm security teams. These teams are under constant pressure to identify, analyze, and mitigate threats in real-time while ensuring compliance and minimizing operational disruptions. Offensive Security Manager (OSM) is designed to address these challenges with advanced AI-driven capabilities, offering a comprehensive solution for proactive threat management and remediation. By implementing proactive measures, organizations can significantly enhance their security posture, anticipate potential threats, and respond swiftly to emerging risks.

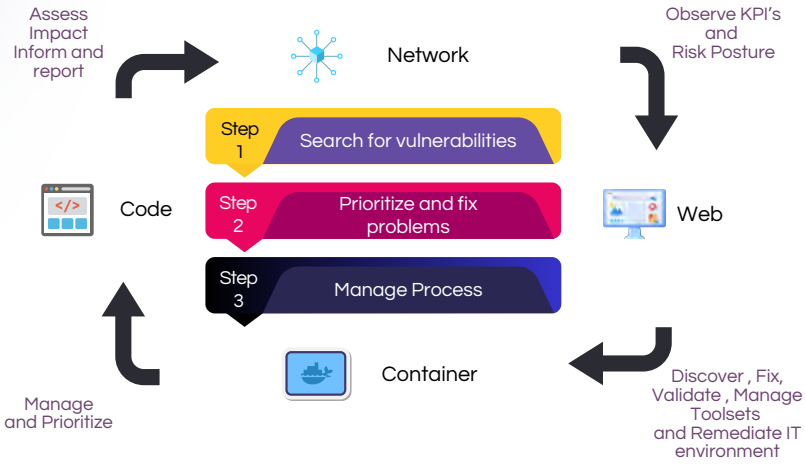
Rapidly Increasing Risk



In today's digital landscape, discovered vulnerabilities are rapidly increasing, with over 25,000 new ones reported in 2023 alone. This surge challenges security teams to prioritize and remediate numerous threats. With 60% of these vulnerabilities classified as critical or high severity, effective vulnerability management is more urgent than ever.

Management challenges and and knowledge gap

Managing vulnerabilities across network, web, container, and source code layers is complex and requires specialized tools and expertise. Network issues involve intricate configurations, web applications face SQL injection and scripting problems, containers have image vulnerabilities, and source code needs thorough analysis. Coordinating these efforts is daunting, especially with limited resources and a skills gap, demanding a holistic, integrated approach for comprehensive security.



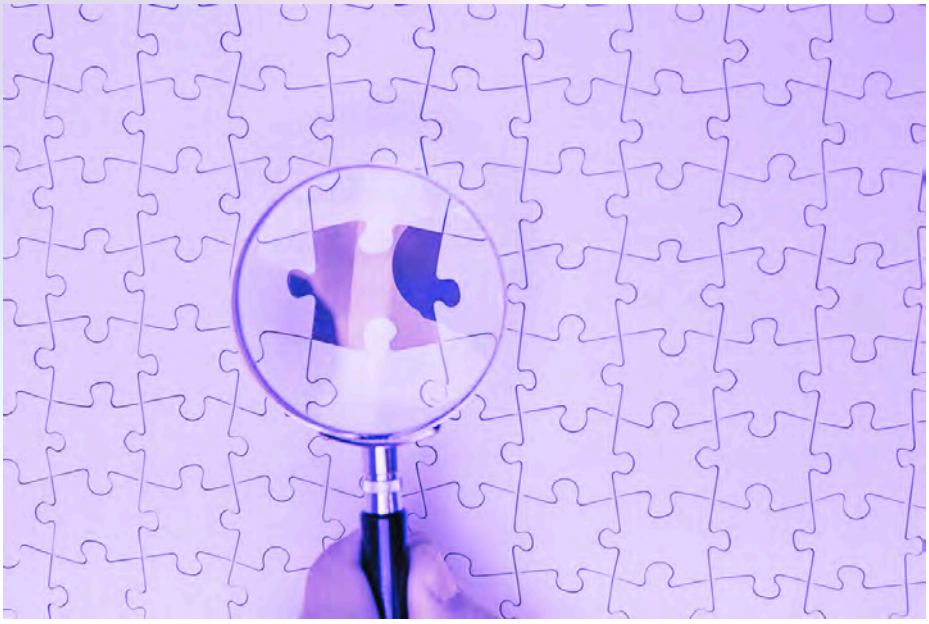
Underutilized tools, lack of resources and communication problems

Underutilized analysis tools in network, web, container, and source code layers often result from the extensive time and expertise needed to understand, prioritize, and solve problems. Security teams must decipher complex issues and coordinate with infrastructure, development, and DevOps teams, leading to delays. This highlights the need for integrated and automated solutions to streamline processes and enhance security.

Patching Delays

- Average time to patch a critical vulnerability is 270 days: Organizations take an average of nearly nine months to patch critical vulnerabilities, leaving systems exposed to potential exploits for extended periods .
- Only 20% of organizations patch critical vulnerabilities within 30 days: A small fraction of organizations can promptly address critical vulnerabilities, highlighting a significant gap in effective vulnerability management.

Resource Constraints



- 55% of organizations report a shortage of skilled cybersecurity professionals: The talent gap continues to be a major hurdle, with more than half of organizations struggling to find qualified security staff to manage and remediate vulnerabilities .

- 75% of security teams are overwhelmed by the volume of alerts: The sheer number of security alerts generated daily overwhelms most security teams, leading to alert fatigue and increased chances of missing critical threats .

Financial Impact

- The average cost of a data breach is $4.35 million: The financial repercussions of data breaches continue to rise, with the average cost reaching over four million dollars per incident .
- Organizations spend an average of $1.5 million annually on breach recovery: Beyond the immediate costs, recovering from a data breach incurs significant expenses, straining the financial resources of organizations .

Operational Challenges

60% of organizations report difficulty integrating security tools: Effective integration of various security tools remains a challenge, leading to fragmented security postures and increased vulnerability .

- 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 .

Data Breaches and Known Vulnerabilities

- 70% of data breaches in 2024 exploit known vulnerabilities: These breaches are linked to inadequately addressed issues.
- 64% of organizations have faced breaches from unpatched vulnerabilities: Despite awareness, many fail to implement timely patches, causing severe incidents.

%70 Eploit of known vulneraqbilities	270 Average days to fix known critical vulnerability	$1.5M Average spending for breach recovery
$4.3M Average cost of data breach		%64 Organizations breached due to unpatched vulnerabilities

OSM

Solving Challenges with OSM

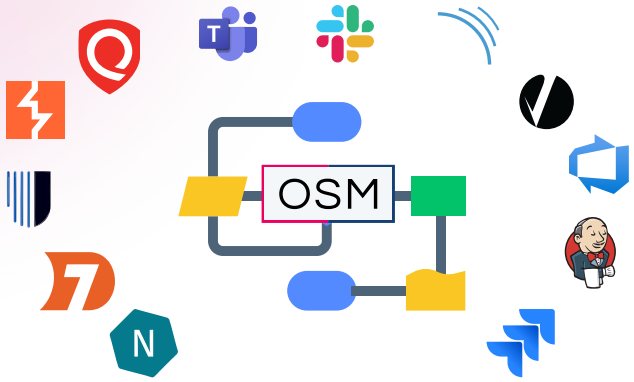
Offensive Security Manager (OSM) addresses the challenge of managing risks by effectively handling vast amounts of data from different layers—network, web, container, and source code. OSM enriches this data with advanced AI-driven insights and industry-specific knowledge, providing a comprehensive view of the security landscape. By consolidating and analyzing data from all layers, OSM delivers the critical information needed to understand and prioritize issues swiftly. This integration of enriched data and expert knowledge significantly shortens the time required to identify, analyze, and remediate vulnerabilities, streamlining the entire security management process.

Offensive Security Manager (OSM) evaluates every piece of information about assets and issues, using additional security context to prioritize effectively. By integrating data from various sources, OSM provides a comprehensive understanding of each asset's risk profile. It analyzes vulnerabilities, threat intelligence, and historical data to determine the severity and potential impact of issues. This enriched context allows OSM to prioritize threats accurately and highlight the most at-risk assets, ensuring that security teams focus their efforts on the most critical vulnerabilities, thereby enhancing overall security posture.

Offensive Security Manager (OSM) uses AI and gathered data to generate detailed, step-by-step remediation instructions. This guidance simplifies the resolution process, closing the knowledge gap and making it accessible to all team members. By providing clear, actionable insights, OSM reduces the time needed to address vulnerabilities, ensuring efficient threat mitigation.

Offensive Security Manager (OSM) enhances governance and workflows by facilitating collaboration between stakeholders according to Continuous Threat Exposure Management (CTEM) best practices. OSM integrates roles across IT, security, and business units, ensuring continuous assessment, prioritization, and remediation of threats. This unified approach enables real-time information sharing and coordinated responses, improving threat visibility and reducing mitigation time. OSM ensures all stakeholders are aligned and engaged in maintaining a secure IT infrastructure.

Offensive Security Manager (OSM) enhances visibility by integrating with existing security tools and systems. By consolidating data from networks, web applications, containers, and source code, OSM provides a comprehensive view of the security landscape. This unified approach ensures security teams have a clear, complete understanding of their security posture, enabling informed decision-making and effective risk management.



Offensive Security Manager (OSM) helps address patching delays by implementing SLAs, notifications, and escalations. OSM ensures timely patching by setting clear service level agreements (SLAs) that define the expected timelines for addressing vulnerabilities. Automated notifications keep security teams informed about pending patches and deadlines, while escalations trigger alerts to higher management if deadlines are missed. This structured approach ensures accountability and prompt action, significantly reducing patching delays and enhancing overall security posture.

Offensive Security Manager (OSM) provides continuous 24/7 coverage of all layers—network, web, container, and source code—ensuring real-time visibility into risks. Unlike infrequent scanning, OSM's CTEA (Continuous Threat Exposure Analysis) allows for immediate threat detection and assessment. This reduces exposure time, enabling proactive management and rapid response, maintaining a robust security posture.

Offensive Security Manager Value

The "Offensive Security Manager" (OSM) is an extensive cybersecurity management, automation and asset risk management solution, leveraging numerous systems to handle a vast array of security data, providing crucial functionality for offensive security operations , and enhancing the efficiency of offensive security testing with the application of AI . Offensive Security Manager will help you in any size of enterprises with :

Comprehensive Risk Management

Offensive Security Manager (OSM) offers comprehensive risk management by identifying and prioritizing risks across network, web, container, and source code layers. Using advanced AI and machine learning, OSM provides deep insights into potential threats, ensuring continuous monitoring and effective risk mitigation. Customers benefit from a robust, adaptable security posture.

Real-Time Visibility and Control

OSM offers real-time visibility and control over the entire security landscape by integrating with existing tools and systems. It consolidates data into a unified dashboard, enabling customers to monitor their IT environment in real-time and address risks promptly. This enhanced visibility ensures informed decision-making and comprehensive threat management.

Enhanced Operational Efficiency

OSM enhances operational efficiency by automating the identification and prioritization of risks, reducing manual efforts. Automated workflows, detailed guidance, and real-time notifications enable security teams to focus on critical tasks, minimizing human error and speeding up threat resolution. This leads to improved productivity and reduced costs for customers.

Proactive Security Measures

OSM empowers customers with proactive security measures, continuously monitoring and analyzing data to anticipate threats and vulnerabilities. This proactive approach helps prevent incidents before they occur, reducing the likelihood of breaches and minimizing potential damage. Customers benefit from a resilient security posture and greater peace of mind.

Improved Resource Utilization

OSM optimizes resource utilization by providing clear, actionable insights and step-by-step remediation instructions, making it easier for less experienced team members to handle complex tasks. This maximizes the efficiency of existing resources, allowing customers to maintain high security standards without additional hires.

Next Steps

OSM Offensive Security Manager

Schedule a demo:
https://www.ofsecman.io/schedule-demo

Our team will be assisting you to see full innovation of Offensive Security Manager .
please visit :
https:/www.ofsecman.io/about