

OSM

OFFENSIVE SECURITY MANAGER

"Prevent Breaches Before
They Happen"

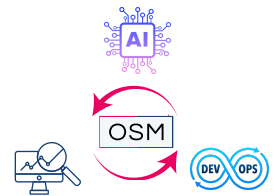
www.ofsecman.io



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 Artificial Intelligence.

AI-Assisted Automated Offensive Security Testing

OSM is an AI-assisted cyber security data orchestration platform with extensive automations for effective planning, control, and execution of offensive security operations. Integrating with Vulnerability Scanners, SIEM, SOAR, DevSecOps Tools and code analysis tools, enabling structured execution



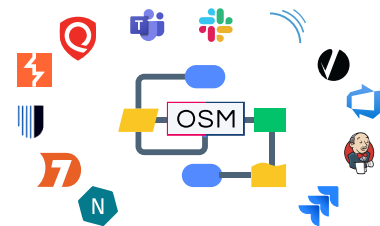
Industry Standard Offensive Testing Plan and Guidelines



OSM provides industry standard guidelines and detailed plans for PCI DSS, OWASP, PSD2 and more for managing offensive security testing activities.

Streamlined Automation, Workflow and Orchestration

OSM automates and consolidates scanning operations into a single interface, ensuring streamlined vulnerability assessment processes and effective with best resource utilization.



Threat Knowledge Enriched Real Time Asset Risk Management



Integration with asset management tools, threat intel feeds, ServiceNow, Service Desk Plus, etc., OSM provides complete visibility into the organization's assets. Realtime risks in SIEM, EDR, SOAR, and other associated technologies enrich risk, aiding the organization in prioritizing security measures.

OSM Offensive Security Manager

<https://www.ofsecman.io/about>

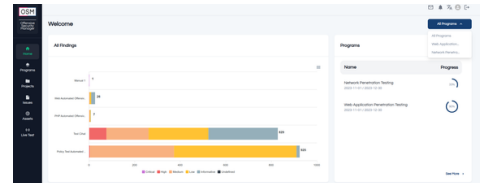


Offensive Security Manager



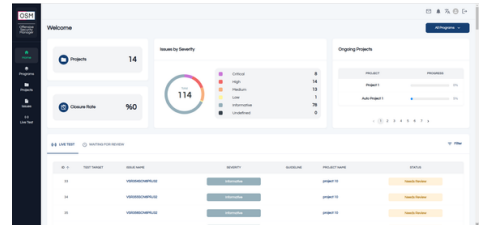
Offensive Security Governance

OSM's unique governance structure engages and creates harmony between Offensive Security team, Business Units , IT and Developments Teams for organizing everything in form of projects and programs



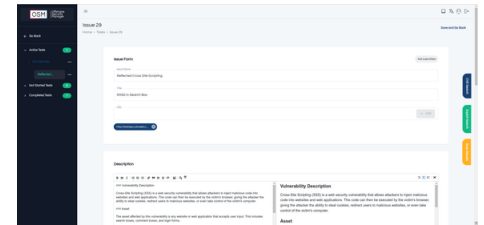
Ensuring Continuous , Compliant and Audit Ready Operation

OSM provides industry standard guidelines and detailed plans for PCI DSS, ISO 27001, PSD2 and more for managing offensive security testing activities.



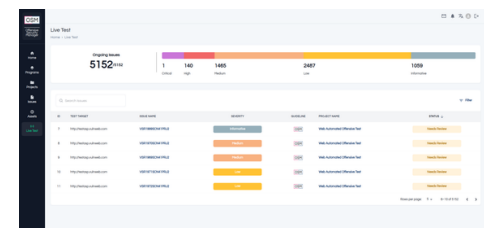
Extensive Visibility with AI Assisted Unified knowledge

OSM ensures maximum visibility and deduplication to create clear picture from any resource, from pentesters and scanners and other tools



Realtime Risk Management

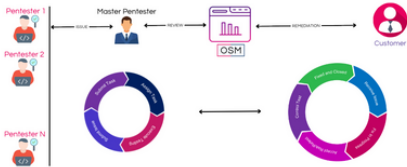
OSM ensures that organization correctly visualizes risk on any asset in real time enriched with all necessary information



OSM

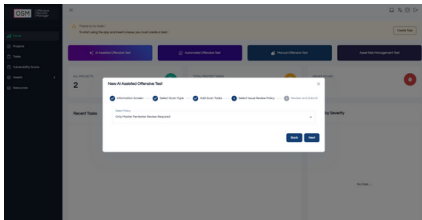
Offensive
Security
Manager

Zero False Positive Workflow



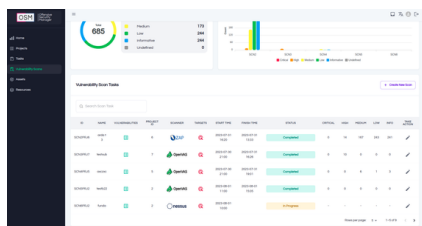
OSM's proven proprietary process workflow ensures multiple layers of control are completed before presenting to business units or customers. reducing false positives saving valuable time for resources

AI Enriched Semi or Fully Automated Offensive Security Testing



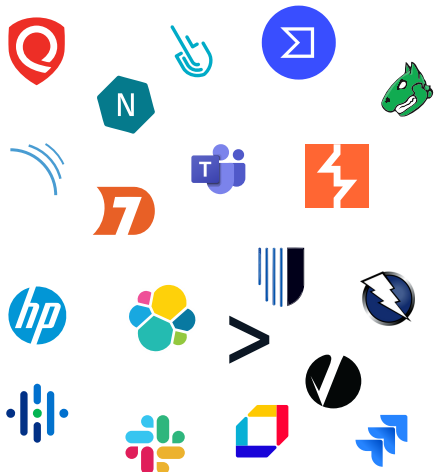
OSM's unique way of handling operations enables to fully or semi automate the testing process while collecting information and creating reports

Risk Correlation and Deduplication

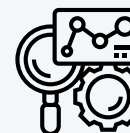


OSM ensures that organization correctly visualizes risk on any asset in real time enriched with all necessary information

Extensive Integrations



OSM orchestrates , gathers correlates and deduplicates all external security tools from Vulnerability Scanners to Active security tools(EDR, SIEM) in one place



The logo consists of the letters 'OSM' in a bold, black, sans-serif font, centered within a white rectangular box. The box has a thin, vibrant pink border on its top and left sides.

OSM

OFFENSIVE SECURITY MANAGER

"The Future of Offensive Security
Management "

www.ofsecman.io

2024