

# Excelling in Proactive Security Management

An Innovative Approach

OSM

Whitepaper by

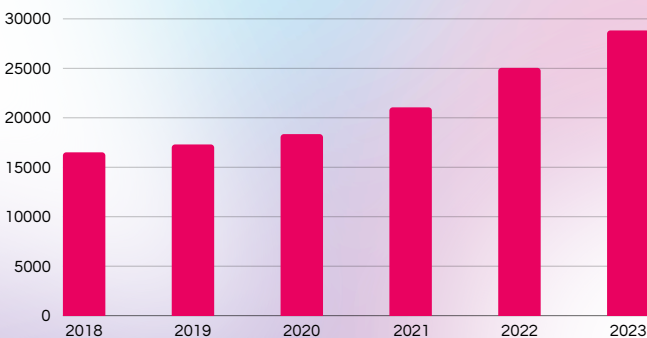
Offensive Security Manager

[ofsecman.io](https://www.ofsecman.io)

2024

# 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.

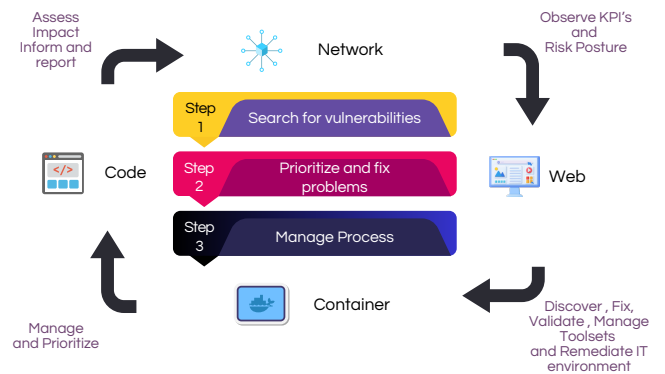


## Rapidly Increasing Risk

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 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

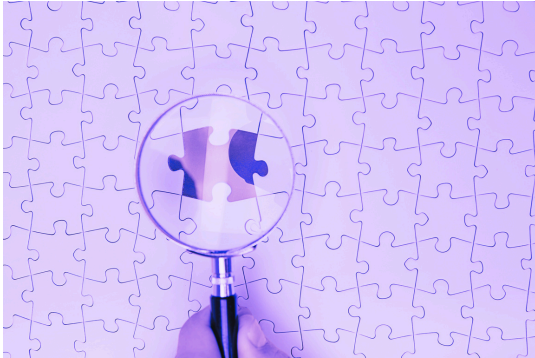
Underutilized analysis tools in network, web, container, and source code layers often result from the extensive time and expertise needed to understand, prioritize, and solve problems. Security teams must decipher complex issues and coordinate with infrastructure, development, and DevOps teams, leading 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 .

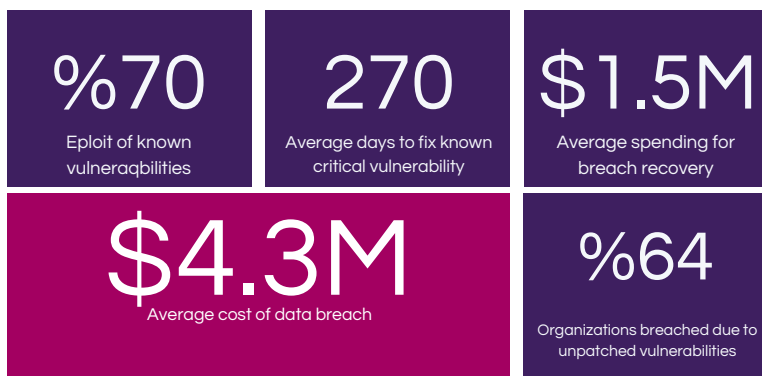


### Operational Challenges

- 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.

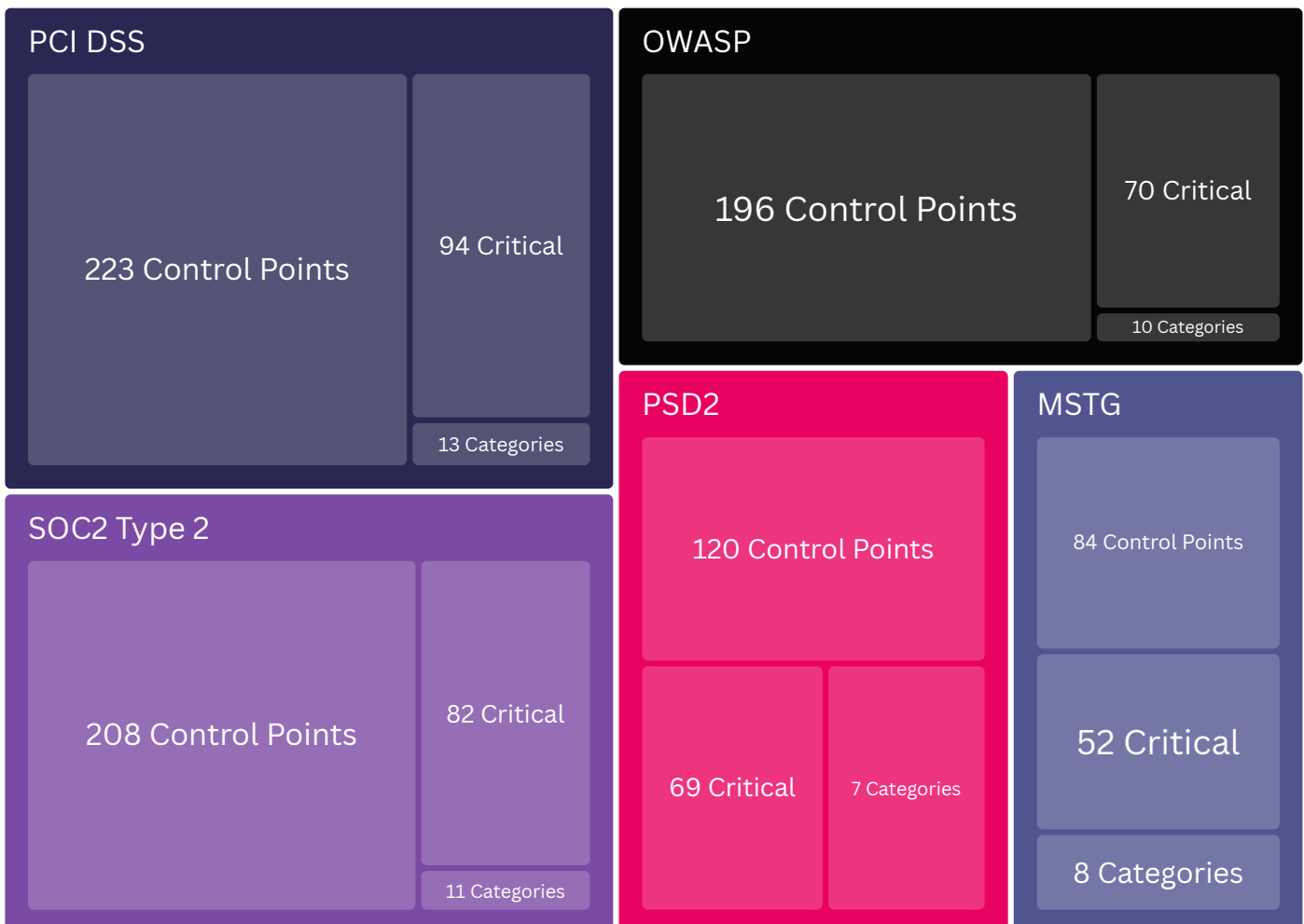


# Importance of Structured Offensive Testing for Industry Frameworks

When it comes to offensive security management, organizations must take a proactive approach in order to remain secure and compliant.

One of the biggest hurdles in the path to effective offensive security management is the existing skill gap. Penetration testers, or 'pentesters' for short, are expected to be well-versed in numerous standards. These include PCI DSS, OWASP, HIPAA, and GDPR. This extensive knowledge requirement, along with the best practices of offensive security testing, creates a significant learning curve that can be quite challenging to overcome.

It's akin to learning the intricate steps of a complex dance while simultaneously trying to understand the diverse rhythms of multiple music genres. Yet, as daunting as it seems, this formidable task is not insurmountable. With the right resources, guidance, and a dash of tenacity, any dedicated pentester can conquer the mountain of offensive security management challenges.



# Testing with well defined industry controls

Any dedicated pentester can conquer the mountain of offensive security management challenges with the right resources, guidance, and tenacity. On this high-stakes stage, knowledge of key standards such as PCI DSS, OWASP, HIPAA, and GDPR is not an option; it is a necessity. This arsenal of regulations and guidelines is not just a checklist to follow but a roadmap to navigate the intricate terrain of data security and privacy. However, this terrain is ever-evolving, making it even more crucial for pentesters to update their skills and knowledge continuously.

Consistent, well-defined offensive security testing controls are the unsung heroes of a robust cybersecurity program. They're like the secret agents of the digital world, quietly working behind the scenes to identify and neutralize threats before they can do harm



Offensive testing methodologies are not as efficient as they seem to be. The lack of standardized testing controls renders them ineffective, painting a misleading picture of security.

Diving into some startling statistics that may prompt you to think twice about the effectiveness of your offensive security testing controls. According to a recent survey, did you know that over 70% of organizations have no well-defined offensive security controls in place. It's time to rethink your strategies and bring those stats down. You may be saying, "But we do security testing." Statistics show that current offensive security testing methods are largely ineffective and often misleading.

Existing offensive security testing might make you feel secure, but it doesn't necessarily safeguard your precious data. Just because you're checking boxes on a compliance form is not enough anymore. So, what's the solution? It's simple - we need well-defined offensive security management and testing controls.

A crucial puzzle piece is missing - a well-defined security management system. Without this, any security testing - offensive or not - is like a car without a GPS, likely to get lost and miss the mark. This requires a well-defined offensive security management and testing control system.

Several recent studies have shown that our current systems are inadequate. Now, you might be wondering, "How could this be?" It's because the effectiveness of offensive security testing is often misunderstood, leading us down a false path of security. It's high time we recognized this issue.

You need to re-evaluate and redefine our offensive security management and testing controls.





# Detailed Offensive Testing Guidelines

## Importance of guidelines for offensive security teams

In the evolving digital landscape, the significance of offensive security cannot be overstated. With cyber threats growing in sophistication and frequency, a proactive security approach is necessary, not a luxury. Enter the world of offensive security testing, a pivotal component of an organization's cybersecurity strategy.

Detailed offensive testing guidelines are essential to ensure that pen testers do not inadvertently cause harm to the target environment.

- InfoSec Institute

The role of penetration testers in this scenario is paramount. However, the right skill set and adherence to detailed offensive security guidelines are essential to ensure their efforts are not in vain.

Unfortunately, many pen testers lack the necessary skills and guidelines to perform their duties effectively. This gap in proficiency can lead to disastrous results for the organizations they protect.

So, how can we bridge this gap? How can organizations equip their pen testers with the right toolset and guidelines? Let's delve into the significance and elements of comprehensive offensive testing guidelines. Offensive testing guidelines are more than just instructions for pen testers. They serve as a roadmap, providing a clear path to uncovering vulnerabilities while staying within ethical and legal boundaries. The absence of these guidelines can result in incomplete testing, overlooked weaknesses, and potential legal issues. Moreover, these guidelines are essential in addressing the skill gap in penetration testing. With rapid technological advancement, the landscape of threats is complex and constantly evolving. Even the most thorough penetration tester may fall short without the right skillset. In-depth offensive testing guidelines ensure that penetration testers are well-equipped to navigate this landscape. They provide a structured approach to testing, enabling testers to identify and exploit vulnerabilities effectively. Additionally, they help the testers maintain an ethical stance, ensuring respect for privacy and adherence to the law.

The absence of detailed guidelines can lead to mistakes that can be costly. These errors can range from missing critical vulnerabilities to accidentally causing damage to the system under test. Furthermore, testers may unintentionally cross legal or ethical boundaries without a clear framework to guide testing, resulting in serious repercussions. Therefore, the importance of comprehensive offensive testing guidelines cannot be overstated. They enhance the effectiveness and efficiency of penetration testing and foster an ethical and legal approach to uncovering and addressing system vulnerabilities. With these guidelines in place, testers are better equipped to face the ever-evolving threats of the digital realm. A well-defined, detailed offensive testing guideline serves as a training manual, enhancing the skills of testers, thereby ensuring all vulnerabilities, patched or unpatched, are identified and addressed.





# Ensuring Offensive Security Tester's Success

A penetration test is only as good as the tester performing it.

- Kevin Mitnick

Inadequate offensive testing can also lead to false positives or negatives, wasting time and resources. False positives can lead to unnecessary remediation efforts, while false negatives can leave vulnerabilities unaddressed. Additionally, inadequate offensive testing can result in compliance failures. Many industries have regulations and standards that require regular security testing, and failure to comply can result in fines or legal action. Finally, inadequate offensive testing can lead to a false sense of security. Organizations may believe they are secure when they are not, leading to a lack of preparedness for attacks.

In the intricate world of cybersecurity, the importance of comprehensive offensive security guidelines cannot be overstated. In the hands of a skilled penetration tester, these guidelines transform into a robust shield, safeguarding the cyber world from unsolicited intruders. However, a lack of proper skill sets might render them ineffective. A relentless rise in cyber threats marks the current digital era. Strong defensive strategies are now a necessity, not a luxury. But what happens when the defenders aren't equipped with the right weapons?



Reflecting on this timeless wisdom, we realize how crucial offensive testing is in the cyber landscape. Such testing, often referred to as penetration testing or 'pen testing,' probes for vulnerabilities in a system, much like an adversary would. But a pen tester without a detailed guide is like an archer without a target. That's where offensive security guidelines come into play. They serve as a roadmap for pen testers, directing their every move. Despite the importance of these guidelines, there is a significant gap in the skillset required for effective penetration testing. The complex nature of cyber threats demands a comprehensive knowledge base, honed skills, and continuous learning - aspects that are often lacking.

# Offensive Security Manager Closes Knowledge Gap

So, how can we bridge this gap? What role do offensive security guidelines play in effective penetration testing? Let's delve deeper to find out. Offensive security guidelines serve as a roadmap for penetration testers, providing detailed procedures to conduct thorough and effective tests. These comprehensive guidelines ensure that no stone is left unturned during testing. Rigorous adherence to these guidelines reduces the chances of missing critical vulnerabilities that malicious elements could exploit. However, these guidelines necessitate a certain level of skill and expertise on the part of the penetration tester.

Without the requisite knowledge, a tester might fail to correctly interpret and apply the guidelines, leading to flawed testing and inaccurate results. Therefore, it's crucial that the tester possesses an adequate skillset for penetration testing. Unfortunately, there is a palpable lack of such skillset in the industry. Many aspiring testers cannot acquire the necessary skills for various reasons. This leads to a significant dearth of qualified testers who can properly adhere to offensive security guidelines. This predicament underscores the need for robust training and skill development programs for penetration testers. Such initiatives should equip testers with the practical know-how to apply security guidelines effectively.

They should also promote understanding the importance of following these guidelines in the letter. In conclusion, offensive security guidelines are essential tools for conducting effective penetration tests. However, their usefulness is rendered moot without testers possessing the necessary skillset. Hence, concerted efforts toward skill development are crucial in ensuring the effectiveness of these guidelines. Offensive security testing, a critical practice in today's cyber-centric world, requires comprehensive guidelines to ensure its effectiveness.

The absence of these guidelines can lead to inconsistencies, inaccuracies, and inefficiencies in penetration testing practices. However, guidelines alone are not enough - the skillset of the testers plays a pivotal role too. Even the most comprehensive guidelines can fall short without a thorough understanding of the theoretical and practical aspects of penetration testing. Therefore, for organizations seeking to conduct effective offensive security testing, investments in skill training and development of their personnel are as important as establishing guidelines. Combining properly trained testers and detailed guidelines can yield more accurate and valuable testing outcomes. It's important to remember that offensive security testing doesn't just identify vulnerabilities. It is also a proactive approach to improving an organization's overall security posture. Consequently, the importance of having competent testers and well-structured guidelines cannot be overstated.

"A successful penetration test requires a well-defined scope, clear objectives, and a thorough understanding of the target environment.

- NIST"

In conclusion, the effectiveness of offensive security testing hinges on two main factors: comprehensive guidelines for conducting tests and a skilled team of testers. None of these elements can exist in a vacuum. They must be developed and improved in tandem to realize the full benefits of offensive security testing.



## Reaping the Rewards of Comprehensive Offensive Security Guidelines

With "Offensive Security Manager," your business can confidently navigate the complexities of cybersecurity. This dynamic software product provides a roadmap for security measures and equips your team with the knowledge necessary to mitigate risks and prevent potential threats.

1. Ensure compliance with industry best practice guidelines.
2. Equip your team with the necessary knowledge to mitigate potential risks.
3. Achieve a robust and reliable security posture.

## Compliance with Industry Best Practice Guidelines

Adherence to industry best practice guidelines in offensive testing is paramount. These guidelines, often established by cybersecurity experts and regulatory bodies, provide a framework for conducting penetration testing systematically, ethically, and legally. Non-compliance could result in the inadvertent disruption of services, violation of privacy laws, and damage to system integrity. Therefore, penetration testers must familiarize themselves with these guidelines and ensure their testing procedures align with them.



## Equipping Your Team with Necessary Knowledge

Offensive testing is not merely about discovering vulnerabilities but also about understanding them in depth and devising effective strategies to mitigate them. This requires a comprehensive knowledge of cyber threats, attack vectors, and defensive measures. A lack of sufficient knowledge can lead to inefficient testing, overlooked vulnerabilities, and ill-devised mitigation strategies. Hence, investing in continuous learning and training for your team is critical to keep them abreast of the latest threats and countermeasures in the ever-evolving cybersecurity landscape.

## Achieving a Robust and Reliable Security Posture

Offensive testing is crucial in achieving a robust and reliable security posture. Through systematic penetration testing, organizations can identify and address their security weaknesses before malicious actors do. However, achieving a strong security posture requires more than just identifying vulnerabilities. It requires strong security policies, proactive threat hunting, regular audits, continuous monitoring, and timely response to security incidents. Therefore, offensive testing should be a part of an organization's broader cybersecurity strategy, not an isolated activity. When conducted correctly, offensive testing can significantly improve an organization's security posture. However, it is a specialized field that requires a specific set of skills. A lack of knowledge and expertise in penetration testing can lead to inaccurate results and false positives, giving a false sense of security. Organizations must engage skilled penetration testers who follow detailed offensive testing guidelines. These guidelines provide a structured approach to conducting penetration tests, ensuring a thorough and accurate assessment of the organization's security posture.

# Statistics Tell The Truth

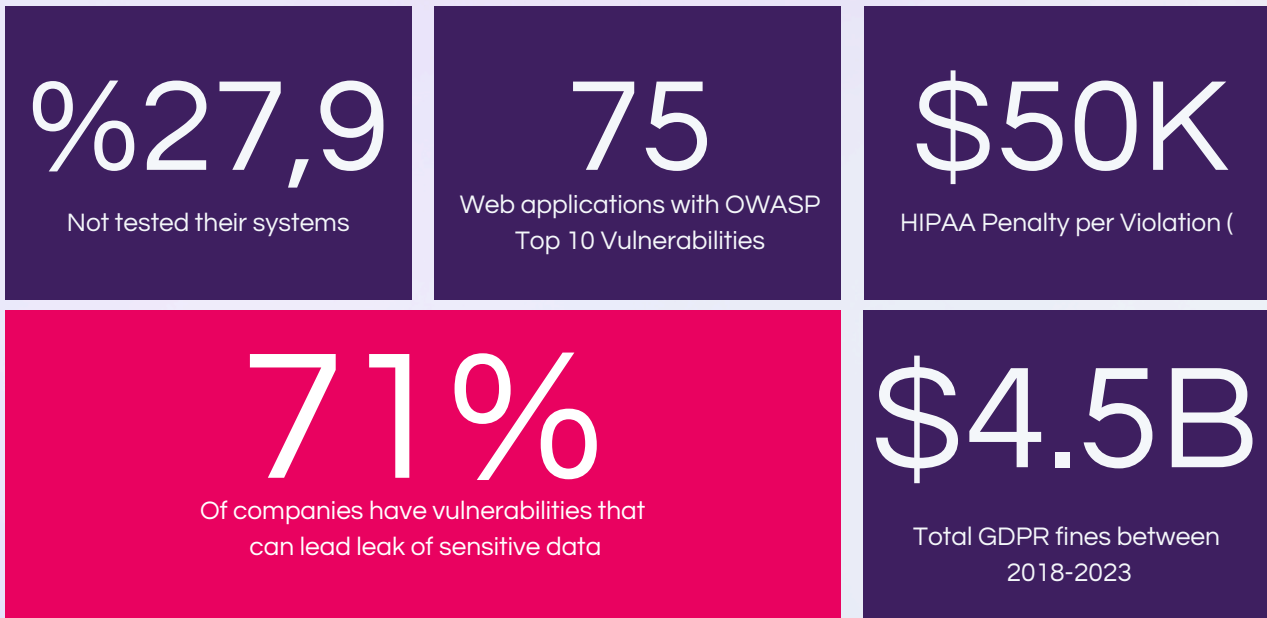
Let's delve deeper into the nitty-gritty of PCI DSS, OWASP, GDPR, and HIPAA penetration testing requirements, peppered with some intriguing statistics to paint a fuller picture of the current cybersecurity scenario. For the uninitiated, PCI DSS, or the Payment Card Industry Data Security Standard, is a security standard that businesses must comply with if they handle credit card transactions. Companies should conduct penetration testing quarterly or after any system changes to meet these standards. According to Verizon's 2020 Payment Security Report, a whopping 27.9% of organizations failed to test security systems and processes in 2019 effectively. Let's pivot to OWASP (Open Web Application Security Project), a non-profit organization acclaimed for its work in web application security. It's worthwhile for businesses to align with the OWASP Testing Guide, which recommends penetration testing to identify known and unknown vulnerabilities.



An alarming statistic from Positive Technologies reveals that 82% of web applications tested in 2019 had vulnerabilities listed in the OWASP Top 10. Moving on to GDPR (General Data Protection Regulation), a regulation that protects user data in the European Union. Under GDPR, organizations must conduct penetration testing to ensure the robustness of their security measures. A 2019 survey from IT Governance revealed that 56% of businesses were not fully compliant with GDPR requirements. Lastly, let's discuss HIPAA (Health Insurance Portability and Accountability Act), a U.S. legislation that provides data privacy and security provisions for safeguarding medical information.

**"Regular penetration testing is essential for HIPAA compliance as well. The 2019 Verizon Breach Investigation Report found that 53% of healthcare organizations suffered a data breach, highlighting the crucial importance of penetration testing."**

Penetration testing is a requirement of the Payment Card Industry Data Security Standard (PCI DSS), a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. A 2017 Verizon report noted that only 55.4% of organizations were fully compliant with PCI DSS at the time of data breaches. This underscores the role of penetration testing in maintaining compliance and protecting consumer data. Moving on to the Open Web Application Security Project (OWASP), it's a non-profit organization dedicated to improving software security. OWASP recommends penetration testing as a part of its Top 10 list of web application security risks. In fact, the 2017 Acunetix Web Application Vulnerability Report found that 33% of tested websites were vulnerable to at least one OWASP Top 10 risk, validating the need for thorough penetration testing. Let's move on to the General Data Protection Regulation (GDPR), a regulation in EU law on data protection and privacy. It mandates organizations to conduct regular penetration tests to identify vulnerabilities and fix them.







# 360° Real-Time Integrated Risk Management

Real-time risk management is the most critical aspect because any vulnerability can be exploited anytime- even if might have been exploited in the past. Amid a penetration test, a critical vulnerability disclosure might suddenly require immediate action by all relevant team members.

Penetration testing identifies potential weak points. While the process goes on, there are three things you should be taking care of, Offensive testing shall be interactive and immediate .

The goal is not to eliminate all risks - that's a utopian dream. Rather, it's about managing them effectively in real-time to keep your system's integrity intact.

Let's start by breaking down what this looks like in practice: Penetration testing, colloquially known as pen-testing, is a simulated cyber-attack against a computer system designed to exploit potential vulnerabilities. We can promptly identify and address possible security threats with real-time risk management during the process. It's like having a safety net while walking a tightrope. It's not just about finding vulnerabilities, it goes beyond that. Real-time risk management during penetration testing is about assessing the impact of those vulnerabilities and strategizing in real time. It's like playing a game of chess, where you're constantly evaluating your moves and your opponent's potential responses. As you navigate through the complex labyrinth of your system's security, you're not just looking for holes to patch. You're also identifying risk factors and assessing their potential impact on your overall security posture. It's a meticulous process that requires precision, sharp insight, and quick decision-making. While it's a faux cyber-attack, the insights garnered are real and valuable. With real-time risk management, you're always one step ahead, ensuring that even in the face of potential threats, you're well-equipped to respond swiftly and effectively. So, the next time you plan for a penetration test - it's not just about the test itself. It's about real-time risk management that goes hand in hand with it.

Integration with Jira, Azure Devops, Slack, MS teams during penetration testing is essential for real-time risk management. These tools facilitate immediate communication and response, enabling teams to rapidly identify, assess, and mitigate potential threats



# Asset Risk Visibility

Let's face it: in this digital era, the security landscape has become a vast, challenging territory. With countless assets at stake, every single vulnerability is a potential gateway for cybercriminals. In this high-stakes game, visibility is key;

**“Knowing your vulnerability is the first step towards safeguarding your assets. Ignorance is no longer bliss, it's a risk you can't afford.”**

Think about your business as a fortress with high walls. A strong defense is crucial, but what about the cracks and crevices that aren't immediately visible? That's where the concept of asset risk and vulnerability exposure comes into play.

Now, let's dive into the world of offensive security. Here, the stakes are higher, the threats more sophisticated, and the need for visibility more vital than ever. Imagine going into battle blindfolded - a frightening thought, isn't it? That's exactly how it feels to operate in offensive security without a clear view of asset risk and vulnerability exposure. It's like navigating through a minefield with no map, unaware of where the next danger might lurk. Visibility in this realm is not just significant; it's pivotal. Ignoring it can lead to disastrous consequences, including system breaches and data theft.

Having a comprehensive understanding of asset risk and vulnerability exposure, therefore, greatly enhances the security posture of an organization. This understanding, in turn, plays a crucial role in the development and implementation of effective offensive security strategies. These strategies, designed to actively seek out and mitigate potential threats, rely heavily on the ability to accurately identify and assess asset risk and vulnerability exposure. In the ever-evolving cyber landscape, a proactive approach to security is no longer a luxury, but a necessity.

The visibility of asset risk and vulnerability exposure empowers businesses to stay one step ahead of potential threats, ensuring their security measures are as robust and effective as possible. Thus, placing a high priority on the visibility of asset risk and vulnerability exposure during offensive security operations is not just beneficial, it's essential. It provides the foundation for successful security management, contributing significantly to the overall security and resilience of the organization. In conclusion, achieving a high level of visibility in asset risk and vulnerability exposure is crucial in today's digital age. It's a key enabler of offensive security - a proactive, forward-thinking approach that seeks to outsmart cyber threats before they even happen. So, let's not underestimate the power of visibility. Instead, let's embrace it, invest in it, and watch it strengthen our security infrastructure.



# 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:

## **AI Assisted Effective Planning, Control and Automation**

OSM acts as a framework for the effective planning, control, automation execution, and monitoring of offensive security operations. By integrating with various vulnerability scanners, SIEM, SOAR, Devsecops Tools and code analysis tools, it enables a systematic and structured execution of these operations by leveraging AI.

## **Orchestrated Automation Workflow**

OSM consolidates scanning operations from tools like Nessus, Rapid7, and OpenVAS into a single interface, ensuring streamlined vulnerability assessment processes and effective resource utilization.

## **Unified Reporting**

OSM collates findings from different sources into a unified report, providing a clear and comprehensive view of an organization's security posture. It integrates with tools like Azure DevOps and Microsoft Teams for streamlined reporting and communication.

## **Industry Standard Offensive Testing Plan and Guidelines**

OSM provides best practice guidelines and detailed plans for PCI DSS, OWASP, PSD2 and more for managing offensive security testing activities. These guidelines ensure that all activities are performed in compliance with industry standards and best practices, enabling teams to effectively and efficiently manage their offensive security operations.

## **Real Time Asset Risk Management**

Through integration with asset management tools like ServiceNow and ManageEngine Service Desk Plus, OSM provides full visibility into an organization's assets. It assesses and ranks these assets based on the vulnerabilities and risks coming from SIEM, EDR, SOAR technologies associated with them, aiding the organization in prioritizing security measures.





# Offensive Security Manager Value

## **Data-Enriched Testing with Extensive Integrations**

OSM integrates with a multitude of security tools, allowing it to gather and utilize vast amounts of data for offensive security testing. This data-driven approach enhances the effectiveness and precision of security testing, ensuring a comprehensive evaluation of an organization's cybersecurity posture.

## **Automated Scanning and Efficiency**

OSM's automation capabilities ensure consistent vulnerability assessments. Scans can be scheduled or initiated in response to specific triggers. OSM also leverages AI tools like ChatGPT to enhance the efficiency of offensive security testing.

## **Resource Management, Reporting, and Monitoring**

OSM provides robust resource management capabilities, helping organizations optimize the use of their security assets. It also facilitates thorough reporting and real-time monitoring of performance metrics, ensuring organizations have up-to-date insights into their security stance.

## **Education**

OSM is a potent educational resource, utilizing data from numerous security tools to inform and educate teams about potential vulnerabilities and threats. It helps offensive security teams understand and effectively mitigate potential risks.





# Offensive Security Manager Value

## **Extensive Real-Time Visibility**

OSM gives extensive visibility into offensive security operations and the security posture of assets. This clear oversight allows organizations to easily identify and address vulnerabilities, thereby enhancing their overall cybersecurity strategy

“As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace.”

- Newton Lee, Counterterrorism and Cybersecurity: Total Information Awareness

## **Correlation, De-duplication, and Security Posture Improvement**

OSM provides a comprehensive understanding of potential threats by identifying and eliminating duplicate findings, and correlating results from different scanners. It integrates with security management tools like Splunk, Qradar, and Elastic for enhanced analysis capabilities.

## **Efficiency and Quality Assurance**

OSM's embedded information management methodology ensures the highest quality results for offensive security testing activities in the shortest amount of time, improving efficiency and lowering false positives.

# Next Steps



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>

