ARMIS

ARMIS PLAYBOOK

Mastering Unified Vulnerability Management (UVM)

Vulnerabilities Abound What Are Organizations Dealing With?

Software Vulnerabilities

1. **Unpatched Software -** Outdated software that contains security flaws that attackers can exploit.
2. **Code Vulnerabilities -** Flaws in the code can lead to security breaches.
3. **Misconfiguration -** Incorrect settings or insecure configurations.
4. **Zero-Day Vulnerabilities -** Newly discovered vulnerabilities for which no patches or fixes are available.
5. **Third Party -** Software or services provided by third-party vendors often introduce additional risk due to lack of security oversight.

Human Vulnerabilities

1. **Social Engineering -** Exploiting human trust and gullibility to gain access (e.g., phishing, baiting).
2. **Weak Passwords –** Easily guessed, found or used credentials.
3. **Lack of Security Awareness -** Employees who are not trained in security best practices can unknowingly create vulnerabilities.

Network Vulnerabilities

1. **Weak Network Security -** Poorly configured devices can create entry points for attackers.
2. **Unprotected Services -** Services running on the network without proper security measures (e.g., open ports, weak authentication).
3. **Insider Threats -** Malicious or negligent actions by employees or insiders.

Physical Vulnerabilities

1. **Physical Security Breaches -** Unauthorized access to physical locations or equipment.
2. **Environmental Factors -** Extreme weather, natural disasters, or other environmental events can damage or compromise physical security.

Legacy Vulnerability Management Is Broken

Data Complexity and Fragmentation

Organizations face mounting difficulties due to the sheer volume of data originating from diverse security sources, including vulnerability scans, cloud infrastructure, application security (AppSec), and code repositories. This complexity is compounded as each tool assesses severity in isolation, often without the crucial context of asset importance or exposure. These disconnected data points inhibit a unified view of vulnerabilities, making prioritization more challenging and less effective.

Overwhelmed Remediation Teams

Remediation teams are increasingly overwhelmed as they receive numerous requests from various security sub-groups, often lacking a cohesive prioritization strategy. This misalignment results in inefficiencies, delayed remediation efforts, and the potential for high-risk vulnerabilities to linger unresolved. The absence of a clear, strategic process for remediation also exacerbates the division between identifying and fixing risks, creating organizational bottlenecks.

Lack of Holistic Risk Management

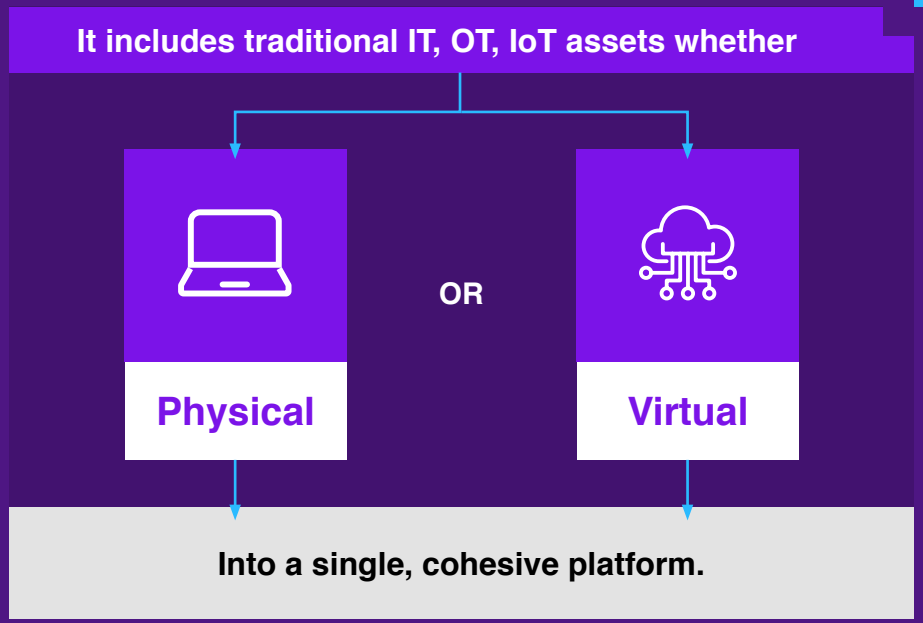
A cohesive approach to risk management remains elusive for many organizations. There is a growing gap between teams that identify vulnerabilities and those required to remediate them. This division prevents the seamless flow of information and collaboration needed for actionable risk reduction. Furthermore, without alignment on priorities, organizations struggle to address vulnerabilities that align with what threat actors are actively exploiting, leaving critical risks unaddressed.

Ineffective Prioritization Based on Threat Actor Activity

Current vulnerability management processes often fail to effectively prioritize risks based on real-world threat actor activity. Without incorporating actionable threat intelligence, teams miss the opportunity to focus on vulnerabilities actively being exploited in the wild. This misstep allows adversaries to capitalize on high-impact weaknesses despite the visibility of these vulnerabilities within the organization.

Introduction to Unified Vulnerability Management

Unified Vulnerability Management (UVM) is a comprehensive, integrated approach to identifying, assessing, contextualizing, prioritizing, and remediating vulnerabilities across an organization's entire attack surface.



Back of the Napkin Math

MTTR

Cybersecurity Threats (General): 1 to 5 hours (for initial response), but full resolution can take days or weeks.

Incident Response (SOC Teams): The median MTTR for security incidents is typically between 6 and 48 hours, depending on the severity.

Ransomware Attacks: 21 days on average for full remediation.

Vulnerability Patching: Critical vulnerabilities have an average MTTR of 60-150 days, depending on prioritization.

Cloud Security Breaches: 24 to 72 hours for initial containment, but weeks for full mitigation.

Cornerstones of Unified Vulnerability Management (UVM)

1. **Holistic Asset Coverage** – Identifies and manages vulnerabilities across IT, OT, IoT, cloud, and external attack surfaces.
2. **Risk-Based Prioritization** – Uses threat intelligence, exploitability data, and business context to rank vulnerabilities based on risk.
3. **Continuous Monitoring & Assessment** – Moves beyond periodic scanning to real-time or near-real-time assessment of vulnerabilities.
4. **Integration with Security & IT Workflows** – Connects with Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), IT Service Management (ITSM), and patch management solutions.
5. **Automated Remediation & Response** – Enables auto-patching, configuration changes, or compensating controls based on vulnerability severity.
6. **External Attack Surface Management (EASM) Integration** – Helps discover and secure internet-facing assets and shadow IT vulnerabilities.
7. **Compliance & Reporting** – Provides dashboards and reporting for regulatory frameworks like NIST, ISO 27001, and GDPR.

Key UVM Capabilities

UNIFY

Ingest data from existing sources, including Armis Centrix™, EDR, on premise, cloud services, code, and applications. Reduce the security findings volume with ML deduplication, and correlate all findings.

CONTEXTUALIZE

Assign context to findings including threat intelligence, likelihood of exploit, and asset attributes like environmental information and business impact.

PRIORITIZE

Automate prioritization based on business impact, adaptable risk severity and likelihood of the exploit. Focus on high-impact fixes that will resolve the largest number of security issues.

ASSIGN AND REMEDIATE

Leverage AI-driven predictive capabilities to determine who is most likely responsible for the asset and the remediation. Benefit from bidirectional integrations with existing workflows and enable self-service for risk resolution.

MONITOR AND REPORT

Track and demonstrate progress for both individuals tasks, as for overall risk trends in the organization.

This Is Not Your Father's RBVM

Overwhelmed Remediation Teams

	Traditional Vulnerability Management	Unified Vulnerability Management
1.	**SCOPE**	**SCOPE**
	IT-focused (endpoints, servers)	IT, OT, IoT, cloud, EAS
2.	**ASSESSMENT TYPE**	**ASSESSMENT TYPE**
	Periodic scanning	Continuous monitoring
3.	**PRIORITIZATION**	**PRIORITIZATION**
	CVSS-based	Risk-based (threat intel, exploitability, business impact)
4.	**REMEDIATION**	**REMEDIATION**
	Manual, ticket-based	Automated workflows & SOAR integration
5.	**COVERAGE**	**COVERAGE**
	Internal network	Internal + external attack surface

Strategic Adoption Phases

Developing a Playbook for Response

A well-crafted playbook for response is crucial for ensuring consistency and effectiveness in handling security incidents. This playbook should outline specific procedures for different types of threats, providing a step-by-step guide that staff can follow during an incident.

The playbook should be tailored to the unique aspects of the organization looking to adopt UVM, reflecting the specific technologies, processes, and personnel involved.

Key elements of a response playbook include:

- **Where we are today** and why legacy VM is no longer fit for purpose
- **Key elements for UVM** and the steps to develop your playbook
- **Strategic considerations** and implementation phase recommendations
- Translating your **strategy to action**
- **Checklist** to get operational

Did You Know

There were over

68,000 published

CVEs last year which is the most in any single year.

This does not include other vulnerabilities that have yet to be discovered, or other security issues that may cause a vuln such as an access or misconfiguration issue.

Strategic Considerations

Phase 1
Assessment & Strategic Planning

- Define Business Objectives & Risk Tolerance
- Map Your Attack Surface
- Establish Governance & Compliance Alignment

Phase 2
Technology Selection & Deployment

- Choose a Unified Vulnerability Management Platform
- Deploy & Integrate with Existing Security Stack

Phase 3
Continuous Discovery & Risk-Based Prioritization

- Enable Real-Time Asset & Vulnerability Visibility
- Threat Intelligence & Risk Contextualization
- Prioritize The Vulns That Matter

Phase 4
Automated Remediation & Risk Mitigation

- Establish Cyber Threat Exposure Management (CTEM) Practices
- Measure, Report & Optimize Performance

Phase 5
Continuous Exposure Management & Optimization

- Establish Cyber Threat Exposure Management (CTEM) Practices
- Measure, Report & Optimize Performance

Did You Know

60%

cyberattacks exploit known but unpatched vulnerabilities

Strategy Into Action

1

Assess & Plan

Why it Matters

Organizations must understand their risk landscape before implementing an effective UVM program. Without proper planning, efforts may be misaligned with business needs, compliance requirements, or existing security processes—leading to gaps in coverage, inefficiencies, and increased cyber risk.

Key Principles

- **Comprehensive Scope** - Cover all assets—IT, OT, IoT; virtual and cloud—to avoid blind spots.
- **Stakeholder Engagement** - Align security, operational, compliance, and executive teams for a unified approach.
- **Risk-Based Approach** - Prioritize actions based on business impact and threat exposure.
- **Regulatory Alignment** - Ensure compliance with industry regulations and security frameworks.

Strategic Steps

01. Define Scope & Objectives

- Identify assets across IT, OT, virtual, logical, and cloud environments.
- Establish clear KPIs e.g., reduced mean time to remediate (MTTR), increased risk visibility.

02. Stakeholder Alignment

- Identify key teams and decision-makers.
- Establish communication channels for ongoing collaboration.

03. Risk Assessment

- Evaluate current security maturity (gap analysis).
- Identify high-risk assets and business-critical systems.

04. Compliance & Regulatory Mapping

- Map existing processes to frameworks like NIST, CIS, and ISO 27001.
- Identify gaps in audit and reporting capabilities.

3 “Dig Deeper” Resources

- More About Armis
- White Paper: Modernizing Vuln Management to Reduce Risk
- 2024 GigaOm CVM Report

2

Asset Discovery & Inventory

Why it Matters

An organization cannot protect what it cannot see. Many security breaches occur because organizations are unaware of shadow IT, ephemeral or unmanaged devices, or misconfigured assets.

Key Principles

- **Real-Time Asset Visibility** - Continuous discovery is necessary to detect new, transient, or rogue devices.
- **Context Matters** - Asset classification should differentiate critical vs. non-essential systems.
- **Automation** - Manual asset tracking is not scalable—automated tools are required.

Strategic Steps

01. Automated Asset Discovery

- Deploy discovery tools for full visibility and contextual analysis.
- Integrate discovery tools with IT, OT, and IoT both physical and virtual.

02. Continuous Inventory Management

- Maintain an always-updated asset database.
- Use AI-driven analytics to detect and classify new assets dynamically.

03. Contextual Asset Classification

- Categorize assets by business impact, network segmentation, and operational role.
- Map assets to critical applications and dependencies to understand attack paths.

3 “Dig Deeper” Resources

- White Paper: Overcoming the Cybersecurity Asset Management Challenge
- White Paper: The Age of Generative AI in Cyber Exposure Management
- Brochure: Armis Centrix™ for VIPR – Prioritization and Remediation – for Medical Device Security

3

Vulnerability Detection & Prioritization

Why it Matters

Not all vulnerabilities pose the same level of risk. Traditional approaches that focus on CVSS scores alone fail to address exploitability, asset criticality, and real-world attack potential.

Key Principles

- **Continuous Monitoring -** One-time scans are insufficient—vulnerability detection must be ongoing.
- **Threat Intelligence Integration -** Real-time exploit intelligence improves prioritization.
- **Risk-Based Decision-Making -** Focus remediation efforts on high-impact, high-exploitability vulnerabilities.
- **Attack Surface Correlation -** Combine external and internal risk perspectives.

Steps to Take

01. Continuous Assessment

- Deploy discovery technology that can provide comprehensive coverage.
- Extend deep situational awareness to virtual & cloud, environments managed and unmanaged assets.

02. Threat Intelligence Integration

- Use real-time feeds to identify active and early warning threats.
- Leverage AI-driven risk scoring to prioritize vulnerabilities based on real-world impact.

03. Risk-Based Prioritization

- Shift from CVSS-based prioritization to an early warning business impact + exploitability model.
- Identify attack vectors, paths and lateral movement opportunities.

04. Attack Surface Correlation

- Use AI-driven analytics to uncover hidden risks.
- Integrate with entire tech stack for a cooperative approach that leverage all of your security elements.

3 “Dig Deeper” Resources

- White Paper: Operationalizing Risk Prioritization for The Security Operations Center (SOC)
- Blog: Breaking Down CISA’s Top Routinely Exploited Vulnerabilities
- Solution Brief: Cyber Exposure Management – Platform Readiness Model

4

Remediation & Risk Reduction

Why it Matters

Many security programs struggle with remediation due to patching limitations, operational constraints, and lack of coordination between security and IT teams.

Key Principles

- **Automation -** Reduce manual remediation bottlenecks.
- **Alternative Mitigations -** Not all vulnerabilities can be patched—use compensating controls where necessary.
- **Integration with IT Workflows -** Ensure remediation efforts align with IT change management.
- **Incident Response Readiness -** Address vulnerabilities before they can be exploited.

Steps to Take

01. Automated Remediation & Patching

- Deploy patches based on business-criticality and risk exposure.
- Use patch automation tools to streamline fixes.

02. Compensating Controls

- Apply network segmentation, firewall rules, and application controls for high-risk vulnerabilities.

03. Workflow Integration

- Connect vulnerability management to ITSM platforms (ServiceNow, JIRA).
- Automate ticket creation and tracking.

04. Incident Response Alignment

- Correlate vulnerability data with threat detection systems.
- Implement automated containment for exploited vulnerabilities.

3 “Dig Deeper” Resources

- Report: ASM Organizational Trends and Challenges
- Brochure: Armis Centrix™ for VIPR – Prioritization and Remediation
- Brochure: Armis Centrix™ for VIPR – Prioritization and Remediation – for OT/IoT Security

5

Validation & Continuous Monitoring

Why it Matters

Patching alone doesn't guarantee security—organizations must validate fixes, detect new threats in real-time, and continuously refine their defenses.

Key Principles

- **Verification -** Ensure vulnerabilities are properly remediated.
- **Continuous Threat Monitoring -** Detect new attack vectors as they emerge.
- **Security Testing -** Red teaming and attack simulations improve defensive readiness.
- **Regulatory Compliance -** Automated reporting simplifies audits and governance.

Steps to Take

01. Validation Testing

- Implement automated verification checks to confirm patches are applied correctly.

02. Continuous Exposure Monitoring

- Deploy real-time monitoring for new vulnerabilities.

03. Attack Simulation & Red Teaming

- Conduct penetration testing and adversary simulations to assess resilience.

04. Automated Reporting & Compliance Audits

- Generate real-time dashboards for CISOs, auditors, and regulators.

3 "Dig Deeper" Resources

- Blog: The Year Vulnerability Management Moves to the C-Suite
- Brochure: Armis Centrix™ for VIPR Pro – Prioritization and Remediation – Financial Services
- Brochure: Armis Centrix™ for VIPR Pro – Prioritization and Remediation – for Education

6

Optimization & AI-Driven Automation

Why it Matters

Threat actors evolve rapidly. Organizations need AI-driven automation to keep up with emerging risks, evolving vulnerabilities, and increasing attack complexity.

Key Principles

- **Dynamic Risk Scoring** - AI-driven risk prioritization based on threat context.
- **Automated Response** - Security teams must act fast; Automation enables instant containment.
- **Predictive Threat Hunting -** Use AI to identify and mitigate risks before they are exploited.

Steps to Take

01. Adaptive Risk Scoring

- Use AI and machine learning to dynamically adjust risk assessments.

02. Automated Playbooks

- Leverage SOAR/SIEM and ticketing workflows.

03. Proactive Threat Hunting

- Deploy predictive analytics and early warning technology to uncover emerging threats.

04. Cross-Platform Integration

- Ensure a unified vulnerability management program across IT, OT, IoT, logical, virtual, and cloud.

3 “Dig Deeper” Resources

- The State of Cyberwarfare Report
- Solution Brief: Armis Centrix™ for VIPR Pro – Prioritization and Remediation
- Transform Vulnerability Management: Bridging Identifying Risk and Fixing Risk

Operational Outcomes

01.

Identification, de-duplication and contextualization of vulnerability, cloud, code and application security findings, providing a centralized view across tools into risk priorities

02.

Operational efficiency gains through grouped findings with a common fix

03.

Automated ownership assignment via predictive AI and global asset-based rules, with ongoing asset coverage tracking

04.

Automate ticket assignment with actionable guidance, scale with bulk ticketing and route through existing workflows using organizational, asset ownership rules

05.

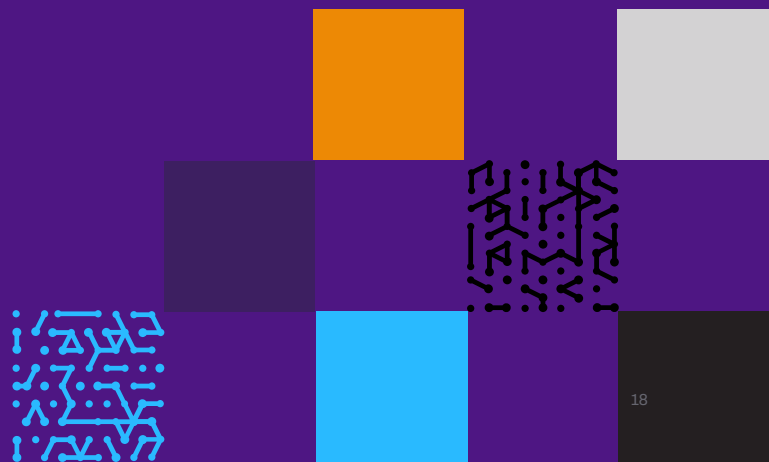
Focus on high-impact fixes via root cause analysis

06.

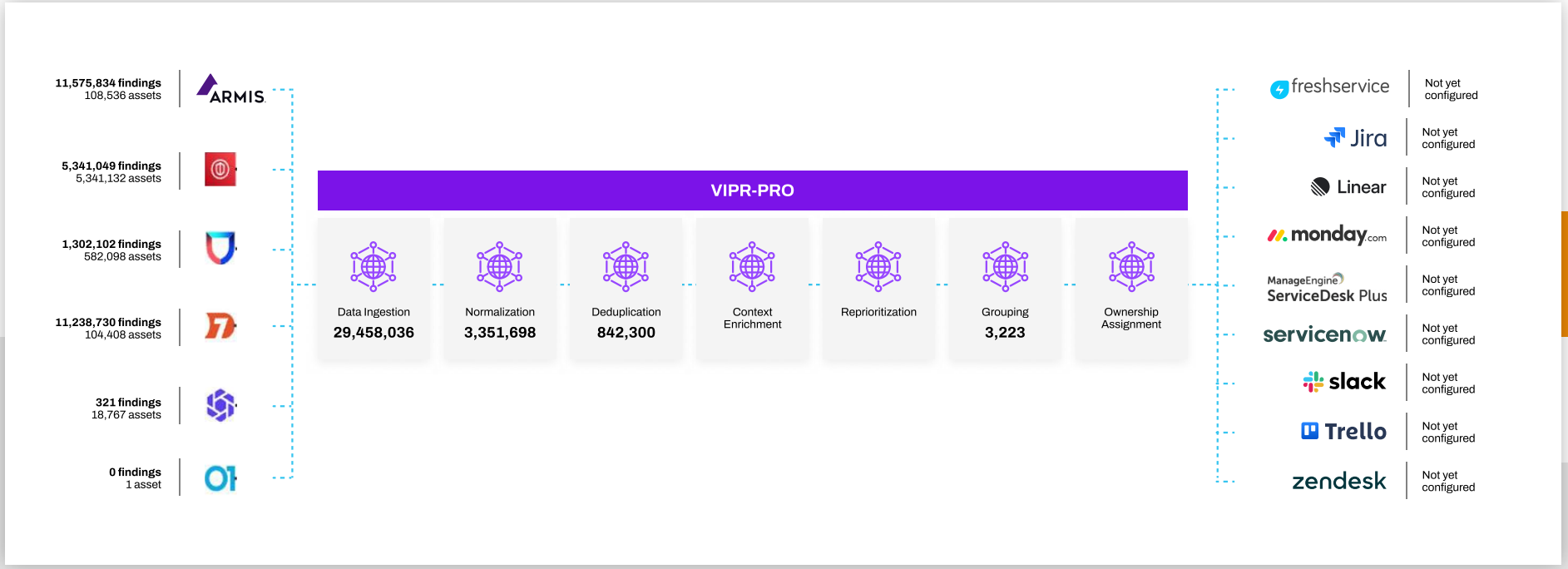
Holistic, end-to-end asset ownership, including application-tier insight into security findings, asset linkings, code pipeline and owner

07.

Shift to programmatic and formalized security strategy across the business



Key Business Outcomes



50-1 backlog reduction with alert consolidation and ML deduplication.

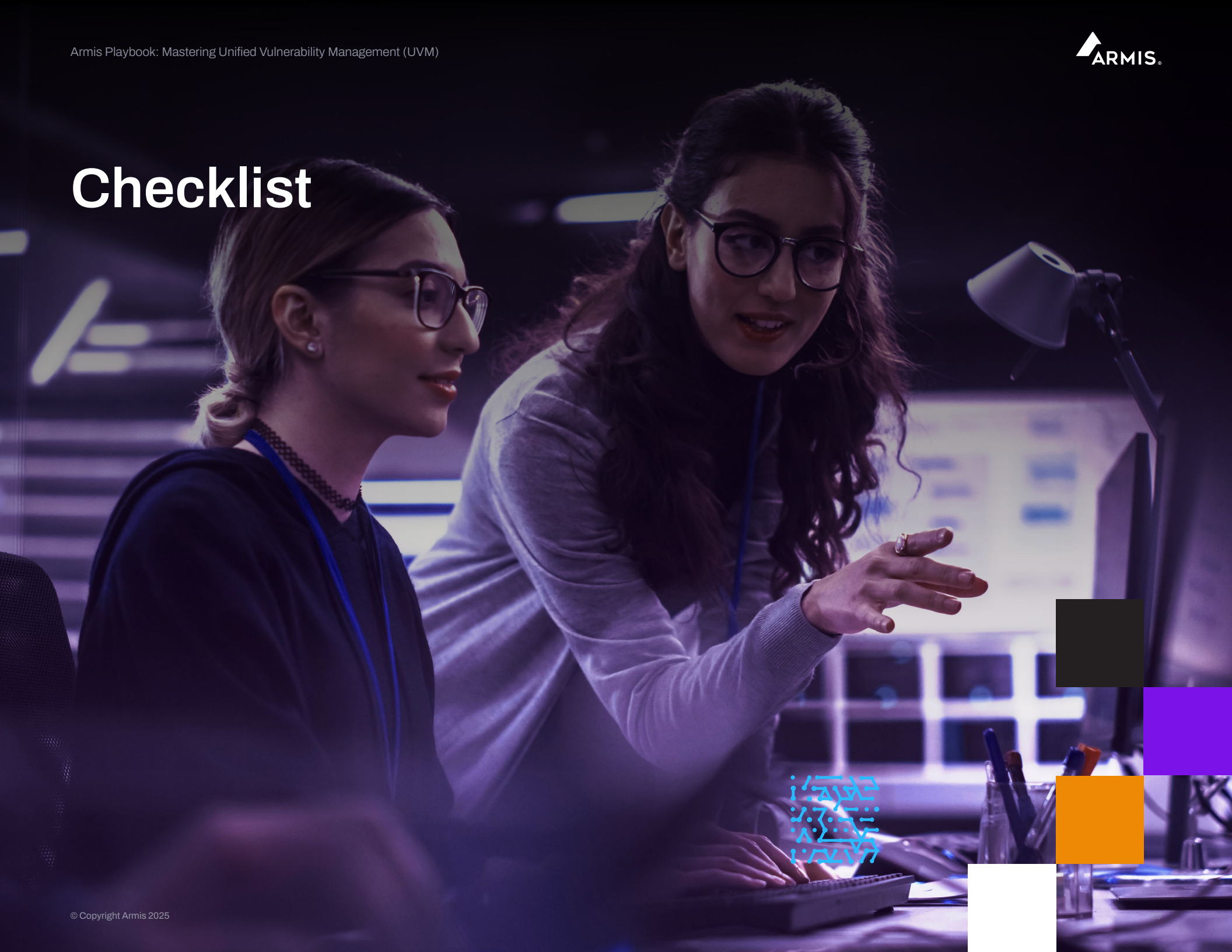
90% improved MTTR for prioritized findings.

80% time savings by automating assessment.

90% Remediation task efficiency improvement through ownership assignment and ticket automation.

7x increase the number of closed findings on an annualized basis.

Checklist



Category	Checklist Item
Assessment & Planning	01. Define the scope by identifying all assets (IT, OT, IoT; logical, virtual to cloud). 02. Set key objectives and success metrics (e.g., MTTR reduction, improved risk visibility). 03. Engage key stakeholders: Security, IT, OT, compliance, executive teams. 04. Conduct a risk assessment to evaluate current vulnerability management maturity. Align with compliance regulatory frameworks (NIST, CIS, ISO 27001, etc.).
Asset Discovery & Inventory	01. Deploy automated asset discovery tools for full visibility and context. 02. Maintain a real-time inventory of devices, applications, and cloud workloads. 03. Classify assets based on business criticality, risk exposure, and dependencies. 04. Ensure visibility into shadow IT, ephemeral and unmanaged devices.
Vulnerability Detection & Prioritization	01. Implement continuous discovery across all environments. 02. Integrate real-time threat intelligence to assess exploitability. 03. Shift to risk-based prioritization (business impact + exploitability, not just CVSS). 04. Correlate and collaborate with the entire tech stack.

Category	Checklist Item
Remediation & Risk Reduction	01. Deploy automated remediation & patching based on prioritization. 02. Apply compensating controls (segmentation, firewall rules, etc.) when patching isn't feasible. 03. Integrate with ITSM platforms (ServiceNow, Jira) for workflow automation. 04. Align vulnerability management with incident response processes.
Validation & Continuous Monitoring	01. Conduct validation testing to ensure vulnerabilities are properly remediated. 02. Deploy real-time monitoring for new vulnerabilities and attack surface changes. 03. Perform attack simulations and red teaming to test security effectiveness. 04. Automate reporting for CISOs, auditors, and regulators.
Optimization & AI-Driven Automation	01. Implement AI-driven adaptive risk scoring to refine prioritization. 02. Leverage SOAR /SIEM playbooks for faster response. 03. Use predictive analytics and early warning and proactive threat hunting to identify emerging risks. 04. Ensure cross-platform integration to unify vulnerability management across all devices and the entire digital footprint.

ARMIS.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo