DATA SHEET

Securin

# Vulnerability Management as a Service (VMaaS)

## The Need for Vulnerability Management

Most organizations –mid to large enterprises, SLED, and government – have vulnerability management challenges:

- **Daunting Workloads:** Many organizations, including state governments, must manage millions of vulnerabilities across complex external web environments, shadow IT, and third-party services, often exceeding the resources available in-house to address the workload.
- **Conflicting Priorities:** Organizations use an estimated 60-75 tools in their security stack.[1] Since different tools provide different views and prioritization of risks, security teams have to spend time reconciling the outputs to prioritize how limited resources are spent.
- **Communications Challenges:** Security teams are often too overloaded to communicate consistently across the organization. If the security team has not informed all internal groups of critical issues, their credibility can be harmed when a compromise occurs.

Security teams need hands-on assistance from experts to help handle their workload, increase their efficiency, and enhance their credibility across the organization.

## Introducing Securin VMaaS

As an extension of the security team, Securin Vulnerability Management as a Service (VMaaS) provides expert, hands-on consulting that establishes a turnkey, successful and ongoing vulnerability management program. Leveraging Securin External Attack Surface Management (EASM), commercial scanners, and other tools, the VMaaS team establishes metrics for the organization's goals and drives improvements over time.

## Service Overview


**Securin VMaaS safeguards organizations from evolving cyber threats.**

1 SiliconANGLE, "Security budgets are growing, but so is vendor sprawl", April 27, 2024.

## Securin VMaaS Provides

### Expert Reviews

Securin experts review output from Securin EASM, security logs and other Securin tools to find known vulnerabilities and Indicators of Compromise (IoC) that may be threat actor-led and so are not yet detected or prioritized by the Cybersecurity and Infrastructure Security Agency (CISA).

### Improved Scanner Coverage

Securin's external penetration testing gives organizations an accurate picture of the risk associated with their externally facing assets. Our penetration testers identify all externally facing assets in scope and test their security controls to help determine how vulnerable they are to attackers.

### Security Trends

We identify and spotlight critical, emerging industry trends like Log4J, while offering proactive early warnings on issues observed across other Securin customers.

### Custom Reports

Securin provides custom reports that deliver actionable insights tailored to the specific needs of security teams, enabling them to prioritize critical threats, efficiently allocate resources, and ultimately enhance overall productivity in managing and mitigating security risks.

## Coordinated Management Plan

### Tailored Prioritization

A single list of tailored prioritization for vulnerability management is provided across organizations, even those with highly complex in-house, shadow IT, and 3rd party environments.

### Level Set Communication

The vulnerability management plan is communicated across all groups and departments in the organization, level setting access to recommended remediation information and status.

### Enhanced Credibility

VMaaS reporting enhances the organization's awareness and credibility in vulnerability management by providing tailored reports for specific groups or agencies, complete with visual dashboards. These reports can feature custom scoring models to compare groups and track progress over time.

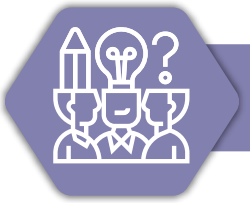
**Securin VMaaS provides hands-on, expert assistance that keeps security teams from being overwhelmed.**

# Methodology

Securin VMaaS ensures that the existing security practitioner team is kept informed, trained appropriately, and increasingly efficient over time. VMaaS leverages a methodology proven across industries and customers. It is phased to efficiently onboard and map into existing SecOps methodologies.

## PHASE 1 - Initial Onboarding & Platform Integration

Once the initial onboarding process is complete, the engagement begins. Securin's VMaaS team collaborates with the organization's security executives to initiate a knowledge transfer. This involves sharing critical details about the infrastructure, tools, dashboards, service-level agreements (SLAs), and key performance indicators (KPIs) to establish a solid execution framework.

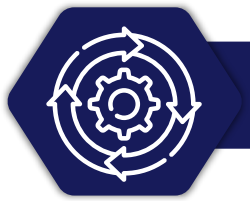


## PHASE 2 - Plan Assessment & Platform Enablement

After finalizing the execution framework, Securin's VMaaS experts determine the scope of coverage, scan frequencies, and processes. They also oversee platform enablement, which includes asset onboarding, grouping, asset criticality analysis, and scan ingestion.

## PHASE 3 - Threat Analysis & Reporting Remediation

Securin's VMaaS team assesses the threat, compares it with the organization's exposure data, and evaluates how susceptible the attack surface is to the threat. We further assist by prioritizing vulnerabilities based on exploitability, complexity, and weaponization. Our support includes providing remediation guidance, tracking remediation progress, and establishing a schedule for regular reporting throughout the engagement.



## PHASE 4 - Sustainability & Repeatability

Communications are established across the organization. The ongoing goal is to operate a sustainable, repeatable discipline that manages risks as they emerge, ideally at discovery. However, should a remediation not complete, it is highlighted at the next scan.

**The VMaaS methodology is systematic, fits within a SecOps framework, and drives efficiencies.**

# Features

**Securin VMaaS capabilities are designed to accelerate every aspect of vulnerability management.**

| | |
|---|---|
| **End to End Risk-Based Approach** | Our team of security experts at Securin prioritizes your organization's vulnerabilities by taking a risk-based approach. Securin analyzes and investigates scan results to map the organization's vulnerabilities to known threats and risks. We assess each vulnerability based on its weaponization, exploit availability, along with risk associations with ransomware and advanced persistent threat (APT) groups. From there our analysts determine the criticality of each vulnerability by its impact on the business environment. We collaborate closely with security teams to create a speedy remediation plan to address high-impact vulnerabilities and risks. |
| **Dedicated Analyst** | Securin's dedicated analyst acts as an extension of the organization's security team to manage their vulnerabilities and improve security posture. Our analyst scans, analyzes, prioritizes threats, and provides ongoing reports to guide the team in securing their environment. |
| **Proactive Focus** | Securin takes a proactive approach to vulnerability management. Securin identifies 80% more KEVs around 35 days faster than CISA. |
| **Rapid Response Methodology** | Securin's rapid response strategy provides organizations with timely alerts and notifications tailored to their environment and tech stack. This personalized approach enables organizations to take immediate and precise action to protect their valuable assets. |
| **Remediation Efficiency** | Our analysts work closely with the security team and chart a rapid remediation plan to mitigate high-impact vulnerabilities and risks. |
| **Custom Reports** | We deliver actionable intelligence through custom reports that continuously optimize the organization's security posture. The reports provide accurate threat context for each vulnerability, providing the information needed to stay protected. |
| **Organization-wide Reporting** | We proactively deliver comprehensive reports and detailed debriefs across the entire organization on critical issues like Log4J. This not only alleviates the burden on the security team but also strengthens their credibility, ensuring that key stakeholders are well-informed and confident in their security posture. |
| **Flexible Cadences** | Securin enables organizations to set up flexible scanning cadences to meet their security and compliance needs while balancing operational and budgeting considerations. |

# Why Securin

Securin leverages a unique set of capabilities in VMaaS.

- **Actionable Insights to Reduce MTTR:** Securin's Rapid Response Methodology provides timely alerts and notifications tailored to the organization's environment and tech stack. As part of a continuous improvement cycle, we provide custom dashboards and scheduled reviews to track mean time to repair (MTTR), root causes, and blockers.
- **Relieve Overwhelmed Cybersecurity Teams:** Securin implements a turnkey, best practices Vulnerability Management program that leverages our process, people, and tools to streamline the organization's remediation efforts. This saves significant time and resources while improving program metrics. For example, a state government reduced ransomware-related exposures by up to 98% in just a 3-6 month period (case study).
- **Optimize Remediation Efforts:** Our risk-based approach to prioritization of vulnerabilities helps IT and security teams focus on the vulnerabilities that matter. Securin's patented Vulnerability Intelligence (VI) product provides organizations with all the information needed to remediate vulnerabilities. At an organization with multiple agencies, average remediation time for CISA KEVs was reduced by 40 days in a 6 month period.
- **Drive Operational Efficiencies Through Automation:** We work with existing scanners or our own to ingest data from multiple sources and identify vulnerabilities. Our experts streamline the entire vulnerability management process—from identification to resolution—by integrating with the organization's IT service management (ITSM) and optimizing ticket creation. For instance, a state government reduced overall issues by 71% within just 3 to 6 months (case study).
- **Prevent Risks and Potential Losses:** Leveraging Securin VI, Securin EASM, and our Risk-Based Vulnerability Management tool, our dedicated security analyst proactively prioritizes vulnerabilities before they can be weaponized. The analyst identifies critical vulnerabilities and highlights other emerging threats, such as Log4J, that are relevant to the organization's environment.

# Benefits

## Provides Critical Yet Rare Expertise

Ensures that your organization gets access to top tier vulnerability management consultants, filling a skills gap that is hard to maintain, much less develop, in-house.

## Same Toolset Across the Board

Unifies your vulnerability management efforts – whether in-house or via Securin's team of experts – with the same platform and tools to maximize efficiencies.

## Increases Credibility of Security Team

Level sets vulnerability management communications across all organizational groups while increasing credibility as a trusted, external set of experts.

### About Securin

At Securin, we empower teams and organizations to minimize their business risk with our comprehensive range of offensive cybersecurity solutions. These solutions are carefully crafted to be intuitive, adaptable, and scalable, catering to organizations of all sizes in today's ever-changing digital landscape. Securin's human-augmented intelligence approach to cybersecurity empowers organizations to thrive by proactively addressing emerging threats and uncertainties, ensuring their security.

Securin
securin.io

Follow Us On