Mandiant

JULY 20, 2023 ASM PRODUCT RELEASE ANNOUNCEMENTS

We're excited to announce the latest features and enhancements in Mandiant Advantage Attack Surface Management (MA-ASM).

WHAT'S NEW

Introducing Collection Workflows

Workflows will have predefined tasks that run based on use cases. Customers can choose their use case per Collection, offering greater visibility on Collection functionality, simpler set up, and enhanced control. Collection Workflows are expected to be released in Q3 2023.

- **External Discovery & Assessment**: Identify shadow IT or unknown assets and vulnerabilities.
- **Authenticated Cloud Discovery & Assessment**: Identify vulnerabilities across your cloud providers.
- **Code Repository Discovery & Assessment (Beta)**: Identify your company's known accounts for secrets and discover unknown rogue repositories.
- **Suspicious Domain Discovery (Beta)**: Identify unknown suspicious properties on the web including typosquats and punycode domains.
- **Third Party Monitoring**: Assess the external security posture of third-parties that have financial or operational impact to your organization.
- **Mobile App Discovery (Beta)**: Identify Android and iOS Apps tagged with your organization's brand keywords hosted in commonly used application marketplaces.
- **Web Application Discovery (Beta)**: Identify web application endpoints derived from URLs.

All new Collections will be configured through Workflows. Legacy Collections are expected to remain supported.

Operationalize Attack Surface Insights in Chronicle and Cortex XSOAR

Chronicle SOAR

Customers can use the API-based integration to retrieve Entities and Issues from MA-ASM to create cases and aid in enrichment playbooks within Chronicle SOAR.

Key Features

- Configure your MA-ASM and Chronicle SOAR and integration via API key.
- Set a minimum severity threshold on the issues presented to the team.
- Configure the issue confidence, bringing in potential, confirmed or both.
- Synchronize issue management between Chronicle SOAR and MA-ASM; reflect status changes and remediation progress in both products.
- Case enrichment and playbooks

Chronicle SOAR can reduce the time it takes to investigate incidents by solving multiple use cases, such as automatically fetching issues or using MA-ASM Entity details to collect additional insights about external assets. For more information, please refer to the **Chronicle SOAR documentation portal (https://cloud.google.com/chronicle/docs/soar/marketplace-integrations/mandiant-asm)**.

Cortex XSOAR

MA-ASM can enable comprehensive visibility of the extended enterprise, so security teams can proactively mitigate real-world threats. MA-ASM scans corporate assets and cloud resources daily and identifies application and service technologies. The module assesses exposure risks to the organization, assigns severity, and can create Incidents within

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.

Cortex XSOAR.

Key Features

- Configure your MA-ASM and Cortex XSOAR and integration via API key.
- Select a single project and multiple collections to feed issues into XSOAR.
- Set a minimum severity threshold on the issues presented to the team.
- Configure the issue confidence, bringing in potential, confirmed or both.
- Synchronize issue management between XSOAR and MA-ASM; reflect status changes and remediation progress in both products.

Go to the **Cortex XSOAR Marketplace (https://cortex.marketplace.pan.dev/marketplace/details/MandiantAdvantageAttackSurfaceManagement/)** to install MA-ASM to your XSOAR instance. For more information, please refer to **ASM Cortex XSOAR Integration documentation (https://docs.mandiant.com/home/asm-cortex-xsoar-integration)**.

CISA Known Exploited Vulnerability Checks

30 active checks for vulnerabilities on CISA's KEV are now available in the **MA-ASM Library (https://asm.advantage.mandiant.com/library)**. CVE-related issues now include a "KEV" tag to indicate if the vulnerability is on CISA's Known Vulnerability Catalog, and EPSS score.

- CVE-2023-21839 - Oracle WebLogic Server - Remote Code Execution
- CVE-2023-28432 - MinIO - Sensitive Information Disclosure
- CVE-2023-27351 - Papercut MF/NG - Authentication Bypass

For product questions, concerns or feedback, contact **Support (https://docs.mandiant.com/home/mandiant-support-cases)**.

MANDIANT PROPRIETARY AND CONFIDENTIAL, COPYRIGHT 2025.