Mandiant

ATTACK SURFACE MANAGEMENT

Mandiant Advantage Attack Surface Management End of Life Announcement

This document provides you with the formal timeline to guide all remaining Mandiant customers through the final phase of the transition to **Google Threat Intelligence (https://cloud.google.com/security/products/threat-intelligence)**. Our goal is to provide a seamless transition to the new Google Threat Intelligence offering, which serves as the next evolution of our threat intelligence capabilities.

This comprehensive offering builds upon and enhances the core intelligence features of your legacy Mandiant product by including Google's unique threat visibility, combined with a broader set of features. We've provided additional information below to guide you through this change.

Key changes

To ensure a clear path forward, we have listed the official End of Life (EOL) dates for the legacy Mandiant Advantage platform and its associated products. These products include:

- Mandiant Threat Intelligence Digital Threat Monitoring
- Mandiant Threat Intelligence Fusion
- Mandiant Threat Intelligence Security Operations
- Mandiant Advantage Attack Surface Management
- Mandiant Threat Intelligence Vulnerability

Platform and API EOL dates

- **January 20, 2027:** Access to the legacy Mandiant Advantage Threat Intelligence (MATI), the browser plugin, and the legacy MATI v2 and v3 APIs will be discontinued. You must be fully transitioned to the Google Threat Intelligence platform by this date.
- **April 1, 2027:** Access to the legacy MATI v4 API will be discontinued on this date to provide additional time to your development teams to migrate any existing integrations. All integrations must be moved to the native Google Threat Intelligence APIs before this date.

Action required before January 20, 2027

- **If you're already transitioning to Google Threat Intelligence:** Continue working with your Google Cloud account representative or partner to implement your existing transition plan.
- **If you haven't started transitioning to Google Threat Intelligence:** Contact your Google Cloud account representative immediately to begin planning your transition process and avoid any future disruption to your security operations.
- If you don't know who your Google Cloud account representative or partner is, send an email to **gti-transition-help@google.com ()** and we can assist you from there.

Contracts beyond EOL

If your contract extends beyond the EOL date, Google Threat Intelligence will be made available to you at no additional cost for the remainder of your current order term. Mandiant service will discontinue on the EOL date. Your admin will receive guidance by email in mid 2026 to inform of the transition process. You can transition today, if you prefer. Contact your Google Cloud account representative to begin this process.

Mandiant

The complimentary offer to transition to Google Threat Intelligence is for all current customers, not just for those with end dates beyond EOL. Contact your Google Cloud account representative or **gti-transition-help@google.com** () to proactively begin the transition ahead of this EOL process, or for any questions.

Help

We are committed to supporting this transition, and we look forward to bringing you the enhanced capabilities of Google Threat Intelligence.

If you have any questions or require assistance, contact **Google Cloud Support** (https://support.google.com/).

April 2, 2026 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2026.04.02

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Adjusted version check for CVE-2019-5513 - VMware Horizon - Information Leak

Vulnerability Checks

- Added Argo Workflows - Lack of Authentication
- Added CVE-2025-68645 - Zimbra Collaboration Suite - Local File Inclusion
- Added CVE-2026-23760 - SmarterTools SmarterMail - Authentication Bypass
- Added CVE-2026-24423 - SmarterTools SmarterMail - Remote Code Execution
- Added CVE-2023-6933 - Better Search Replace < 1.4.5 - PHP Object Injection
- Added CVE-2025-59718 / CVE-2025-59719 - Fortinet FortiOS - Authentication Bypass
- Added CVE-2026-21962 - Oracle WebLogic Server Proxy Plug-In - Unauthenticated Remote Code Execution
- Added CVE-2025-34026 - Versa Concerto Actuator Endpoint - Authentication Bypass
- Added CVE-2023-6549 - Citrix NetScaler ADC/Gateway - Out-of-Bounds Memory Read
- Added CVE-2025-49533 - Adobe Experience Manager Forms - Insecure Deserialization
- Added CVE-2025-40551 - SolarWinds Web Help Desk < 2026.1 - Deserialization RCE
- Added CVE-2025-31125 - Vite Development Server - Path Traversal
- Added CVE-2026-20045 - Cisco Unified Communications - Remote Code Execution
- Added CVE-2023-34990 - Fortinet FortiWLM - Directory Traversal
- Added CVE-2021-1472 - Cisco Small Business RV Series - OS Command Injection
- Added CVE-2025-13390 - Wordpress WP Directory Kit Plugin - Authentication Bypass
- Added CVE-2025-13342 - WordPress Frontend Admin Plugin - Privilege Escalation
- Added CVE-2025-64155 - Fortinet FortiSIEM - Unauthenticated RCE
- Added CVE-2026-24061 - GNU Inetutils telnetd - Authentication Bypass
- Added CVE-2021-43062 - Fortinet FortiMail - Reflected XSS
- Added CVE-2026-21858 - n8n Webhooks - Remote Code Execution
- Added CVE-2025-52691 - SmarterMail - Unrestricted File Upload

Technology Fingerprints

- Added Versa Concerto technology fingerprint
- Added WordPress "Better Search Replace" plugin technology fingerprint
- Added Cisco Unity Connection technology fingerprint
- Added Adobe Experience Manager (AEM) Forms technology fingerprint
- Added Argo Workflows technology fingerprint
- Added n8n technology fingerprint

- Added Cisco VPN Routers technology fingerprint

January 21, 2026 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2026.01.21

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2025-6174 - Qwizcards Reflected XSS
- Added CVE-2021-35042 - Django SQL Injection
- Added CVE-2023-6266 - WordPress Backup Migration Unauthorized Access
- Added CVE-2025-14611 - Gladinet CentreStack and Triofox Hardcoded Cryptographic Keys
- Added CVE-2025-20393 - Cisco Email Appliances Remote Code Execution
- Added CVE-2025-14847 - MongoDB Uninitialized Memory Read (MongoBleed)
- Added CVE-2017-10271 - Oracle WebLogic XMLDecoder Remote Code Execution
- Added CVE-2023-5914 - Citrix StoreFront XSS

Technology Fingerprints

- Added BackupBliss Backup Migration technology fingerprint
- Added Cisco Secure Email and Web Manager technology fingerprint
- Added Citrix StoreFront technology fingerprint
- Added Qwizcards Wordpress Plugin technology fingerprint

December 19, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.12.19

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Added fallback logic for Cymru resolution failures to prevent `net_name` fields from appearing as null.
- Fixed an issue where the Shodan Ranger task could include IPs outside of the range of the netblock.
- Corrected 2FA detection logic in the `enrich/uri` task; previously, `auth.2fa` was incorrectly defaulting to true.

Vulnerability Checks

- Adjusted severity for CVE-2025-55182 - React Server Components - Remote Code Execution to reflect its critical nature.
- Added CVE-2025-55183 - Next.js Server Actions - Source Code Disclosure
- Added CVE-2025-59287 - Windows Server WSUS Insecure Deserialization
- Added CVE-2025-66039 - FreePBX Authentication Bypass
- Added CVE-2025-61675 - FreePBX Authenticated SQL Injection
- Added CVE-2025-61678 - FreePBX Authenticated Arbitrary File Upload
- Added CVE-2025-32429 - XWiki Platform - SQL Injection
- Added CVE-2025-55749 - XWiki Platform Information Disclosure
- Added CVE-2025-34299 - Monsta FTP <= 2.11.2 - Unauthenticated Remote Code Execution
- Added CVE-2025-12101 - Citrix ADC/Gateway - Reflected XSS
- Added CVE-2025-8943 - Flowise < 3.0.1 - Remote Command Execution
- Added CVE-2025-6204 - Dassault Systems DELMIA Apriso Command Injection
- Added CVE-2024-20404 - Cisco Finesse Server-Side Request Forgery (SSRF)
- Added CVE-2025-5569 - IdeaCMS <= 1.7 - SQL Injection

Technology Fingerprints

- Expanded and consolidated React fingerprints to improve detection of modern Server Component deployments.

December 8, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.12.08

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2025-55182 - React Server Components - Remote Code Execution

December 3, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.12.03

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2025-0107 - Palo Alto Networks Expedition OS Command Injection
- Added CVE-2025-34031 - Moodle Jmol Filter Local File Inclusion
- Added CVE-2025-61757 - Oracle Access Management REST WebServices - Authentication Bypass
- Added CVE-2024-27348 - Apache HugeGraph - Remote Command Execution
- Added CVE-2025-52472 - XWiki Platform HQL Injection
- Added CVE-2025-62168 - Squid HTTP Authentication Credential Disclosure
- Added CVE-2025-64446 - FortiWeb - Authentication Bypass
- Added CVE-2025-10035 - GoAnywhere MFT - Insecure Deserialization / Auth Bypass
- Added CVE-2024-50498 - Wordpress Query Console Plugin - Remote Code Execution
- Added CVE-2025-58360 - GeoServer XML External Entity Injection

November 13, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.11.13

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2025-2748 - Kentico CMS - Unauthenticated Stored XSS
- Added CVE-2025-2746 and CVE-2025-2747 - Kentico CMS - Authentication bypass
- Added version check for CVE-2025-49844 - Redis - Remote Code Execution
- Added CVE-2025-24893 - XWiki Platform Remote Code Execution
- Added CVE-2025-12480 - Gladinet Triofox Authentication Bypass
- Added CVE-2025-11371 - Gladinet CentreStack Unauthenticated Local File Inclusion Vulnerability

Technology Fingerprints

- Added XWiki technology fingerprint
- Added Gladinet Centrestack technology fingerprint
- Added Generic Model Context Protocol technology fingerprint
- Fixed Imperva FlexProtect technology fingerprint
- Fixed Oracle E-Business Suite technology fingerprint
- Fixed Oracle Dynamic Monitoring Service technology fingerprint

October 28, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.10.28

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Fixed Github access token issue that was preventing Github Account retrieval

Vulnerability Checks

- Added CVE-2025-2611 - ICTBroadcast - Remote Code Execution
- Added CVE-2025-45854 - JEHC-BPM - Arbitrary code execution
- Added CVE-2025-5947 - Service Finder Bookings plugin Authentication Bypass
- Added CVE-2025-20362 - Cisco Adaptive Security Appliance Authentication Bypass
- Added CVE-2025-61882 - Oracle E-Business Suite Remote Code Execution

Technology Fingerprints

- Added ICTBroadcast technology fingerprint
- Added Service Finder Wordpress Plugin technology fingerprint
- Added Cisco generic SNMP technology fingerprint
- Added support for SNMP V3

October 10, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.10.09

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added Hoverfly (CVE-2025-54123)
- Added Oracle E-Business Suite (EBS) (CVE-2025-61882)
- Increased the scope of Wordpress User Info Leak vulnerability checks

Technology Fingerprints

- Added Hoverfly technology fingerprint
- Added jehc-bpm technology fingerprint
- Changed vendor name of MySQL to Oracle
- Expanded PHP technology fingerprint to identify when phpinfo() is present

September 30, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.09.30

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Fixes to reduce false positives on Insecure Pattern Detection
- Fixes for DNS teaser to Domains that have been added as seeds

Technology Fingerprints

- Increased overall reliability of technology fingerprints
- Improvements to MariaDB technology fingerprint
- Reduced false positives for Mysql technology fingerprint
- Added Cisco Identity Services Engine technology fingerprint
- Added Admin Panel technology fingerprint

Mandiant

May - September 2025 ASM Discovery Engine Releases

The following updates were made to the Attack Surface Management Discovery Engine after **May 19, 2025 ASM Discovery Engine Release (https://docs.mandiant.com/home/asm-engine-05192025)**:

Vulnerability Checks

- Added Cisco Identity Services Engine Unauthenticated RCE (CVE-2025-20281)
- Added Cisco IOS XE - Authentication Bypass (CVE-2025-20188)
- Added Citrix NetScaler ADC and Gateway Out-of-bounds Read (CVE-2025-5777)
- Added Craft CMS - Remote Code Execution (CVE-2025-32432)
- Added Fortinet FortiWeb Fabric Connector SQL Injection to RCE (CVE-2025-47812)
- Added Ivanti Endpoint Manager Mobile - Remote Code Execution (CVE-2025-4427/4428)
- Added Langflow AI - Remote Code Execution (CVE-2025-3248)
- Added Microsoft SharePoint Server Remote Code Execution (CVE-2025-53770)
- Added Palo Alto PAN-OS - Authentication Bypass (CVE-2025-0108)
- Added ThinkPHP 5.0.23 - Remote Code Execution (CVE-2018-20062)
- Added Wing FTP Server Unauthenticated RCE (CVE-2025-25257)

Technology Fingerprints

- Enhanced Cisco IOS XE technology fingerprint
- Enhanced Citrix Gateway technology fingerprint
- Added FlowiseAI Flowise technology fingerprint
- Added Fortinet FortiSIEM technology fingerprint
- Added GGML Llama.cpp technology fingerprint
- Added Hoverfly technology fingerprint

May 19, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.05.19

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added Advantive Veracore - SQL Injection (CVE-2025-25181)
- Added Apache Tomcat - Remote Code Execution (CVE-2025-24813)
- Added Next.js - Authentication Bypass (CVE-2025-29927)
- Added Kubernetes Ingress NGINX Controller - Remote Code Execution (CVE-2025-1974) (IngressNightmare)
- Added Vite - Arbitrary File Read (CVE-2025-30208)
- Added CrushFTP - Authentication Bypass (CVE-2025-2825)
- Added Fortinet FortiOS - Authentication Bypass (CVE-2024-55591)
- Added Oracle Peoplesoft - Arbitrary File Read (CVE-2023-22047)
- Added Apache CloudStack - Default Credentials
- Added Apache APISIX - Default Credentials
- Added Citrix Netscaler - Authentication Bypass (CVE-2024-6235)
- Added Apache DolphinScheduler - Default Credentials
- Added SAP NetWeaver - Remote Code Execution (CVE-2025-31324)
- Added SAP NetWeaver - Indicator of Compromise (CVE-2025-31324)
- Added Atlassian Jira - Authentication Bypass (CVE-2022-0540)
- Added Roxy-WI - Remote Code Execution (CVE-2022-31126)
- Added Roxy-WI - Remote Code Execution (CVE-2022-31137)

- Added Gradio - Arbitrary File Read (CVE-2023-51449)

Technology Fingerprints

- Added Advantive Veracode technology fingerprint
- Added Vite.js technology fingerprint
- Added Oracle PeopleSoft technology fingerprint
- Added Roxy-Wi technology fingerprint
- Added Gradio Instances technology fingerprint
- Enhanced Pan-OS fingerprints

April 15, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.04.15

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-12356 - BeyondTrust - Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability
- Added CVE-2024-53704 - SonicWall - SonicOS SSLVPN Improper Authentication Vulnerability
- Added CVE-2024-48248 - NAKIVO - NAKIVO Backup & Replication

Technology Fingerprints

- Added Nakivo Backup & Replication technology fingerprint
- Enhanced Moodle Detection & Versioning technology fingerprint
- Enhanced SonicWall SSL VPN technology fingerprint

February 26, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.02.26

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Citrix ADC Vulnerability updated with correct versions
- Added CVE-2021-27905 Apache Solr - Server-Side Request Forgery
- Added CVE-2022-26148 Grafana & Zabbix Integration - Credentials Disclosure

Technology Fingerprints

- Fixed False Positive on Citrix ADC Vulnerability

February 13, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.02.13

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2023-6021 - Ray API - Local File Inclusion
- Added CVE-2023-6020 - Ray - Arbitrary File Read
- Added CVE-2024-36412 - SuiteCRM - SQL Injection
- Added CVE-2024-23917 - JetBrains TeamCity 2023.11.3 - Authentication Bypass
- Added CVE-2024-50603 - Aviatrix Controller - Remote Code Execution

Technology Fingerprints

- Fixed false positive fingerprint for k8server
- Enchanced to capture additional variants of aviatrix controller HTTP title
- Added SuiteCRM technology fingerprint

January 22, 2025 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2025.01.22

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-56512 - Apache NiFi - Sensitive Information Disclosure
- Added CVE-2024-12856 - Four-Faith Industrial Router - Remote Code Execution
- Added CVE-2024-29895 - Cacti - Remote Code Execution
- Added CVE-2024-45507 - Apache OFBiz - Remote Code Execution

Technology Fingerprints

- Extended the existing set of signatures in order to successfully detect additional variants (firmwares) of Four-Faith Industrial Routers.

December 19, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.12.19

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-50623 - Cleo Harmony - Arbitrary File Read
- Added CVE-2024-32113 - Apache OFBiz Directory Traversal - Remote Code Execution
- Updated Proof of Concept reference for the Microsoft Internet Information Services - Tilde (Shortname Files) Misconfiguration

Technology Fingerprints

- Added Cleo Harmony technology fingerprint
- Added Hunk Companion Wordpress Plugin technology fingerprint

December 12, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.12.12

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-46938 - Sitecore Experience Platform - Arbitrary File Read
- Added CVE-2022-2130 - Microweber - Reflected Cross-Site Scripting
- Added CVE-2020-13405 - Microweber - Information Disclosure

November 26, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.11.26

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-0012 - Palo Alto PAN-OS - Authentication Bypass

- Added CVE-2024-9474 - Palo Alto PAN-OS - Remote Code Execution

November 20, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.11.20

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-8963 - Ivanti Endpoint Manager Cloud Services Appliance - Authentication Bypass

Technology Fingerprints

- Palo Alto Networks PAN OS Version Enhancements
- Jenkins Plugins Detection via Static Resource Analysis
- OpenJS Enhancement for jQuery detection and version information

November 13, 2024 ASM Discovery Engine Release - Scan Ranges Expanded

Mandiant Advantage Attack Surface Management (MA-ASM) has updated source IP scanning ranges.

See **ASM Scan Ranges** **(https://docs.mandiant.com/home/asm-scan-ranges)** for a comprehensive list of IP addresses to add to your allowlist.

November 11, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.11.11

This Attack Surface Management Discovery Engine release includes:

- Release of Enhanced Third-Party Supplemental Data Integration and Validation Framework

Vulnerability Checks

- Added CVE-2024-51568 - CyberPanel - Remote Code Execution
- Added CVE-2024-45216 - Apache Solr - Authentication Bypass

Technology Fingerprints

- Enhanced the Gitea technology fingerprints

October 31, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.10.31

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Fixed format of "Release Date" for CVE-2024-1709 to allow for accurate sorting.

Vulnerability Checks

- Added CVE-2019-14322 - Pallets Werkzeug - Arbitrary File Read
- Added CVE-2018-12613 - PhpMyAdmin - Local File Inclusion
- Added CVE-2017-12615 - Apache Tomcat - Remote Code Execution
- Added CVE-2024-51567 - CyberPanel - Remote Code Execution

Technology Fingerprints

- Added Teradata Viewpoint technology fingerprint

- Added BeyondTrust Remote Support and Privileged Remote Access technology fingerprints
- Added CyberPanel technology fingerprint
- Fingerprint Enhancement: Version information for multiple Veeam Backup Products
- Fingerprint Enhancement: Amazon EC2 detection

October 24, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.10.24

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Fixed woocommerce_cve_2021_32789 False Positive
- Added CVE-2019-10092 - Apache HTTP Server - HTML Injection
- Added CVE-2019-10098 - Apache HTTP Server - Open Redirect
- Added CVE-2012-1823 - PHP - Remote Code Execution

Technology Fingerprints

- Added Apache Tapestry Framework technology fingerprint
- Removed Microsoft X-MS-InvokeApp Header technology fingerprint

October 17, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.10.17

This Attack Surface Management Discovery Engine release includes:

- Updated "acceptable" strength ciphers to be classified as weak
- Added pagination to GCP Projects

Vulnerability Checks

- Modified several vulnerability checks for improved accuracy and performance
- Added CVE-2024-9463 - Palo Alto Expedition - Remote Code Execution
- Added CVE-2024-9465 - Palo Alto Expedition - SQL Injection
- Added CVE-2024-9014 - pgAdmin 4 - Sensitive Data Exposure

Technology Fingerprints

- Added PgAdmin technology fingerprint
- Added Snow Software technology fingerprint
- Added Fortinet FortiManager enhancement

October 14, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.10.14

This Attack Surface Management Discovery Engine release includes:

- When an email is used as a seed, discovered Entities are explicitly scoped in.

October 3, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.10.03

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Refreshed Meta HTTP Equiv to prevent redirect loop

Technology Fingerprints

- Fixed bug resulting in inaccurate version numbers of WooCommerce fingerprinting
- Protocol Addition: Apache Cassandra CQL Shell technology fingerprints
- Added SmartBear Swagger UI Detection technology fingerprints

October 2, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.10.02

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Disabled host discovery for port-scanner tool to aid in discovery of open ports on a host

September 20, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.09.20

This Attack Surface Management Discovery Engine release includes:

- Created a new port scan lightning task
- Added a retry mechanism for entity uploads which checks Cloud Storage to ensure file upload completion

Bug Fixes

- Added AWS Lambda fallback for S3 bucket checks to avoid throttling from direct calls
- Moved task queuing logic after database commit within the entity state machine to resolve "Invalid entity attempted" error

September 11, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.09.11

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-28987 - SolarWinds Web Help Desk - Hardcoded Credential
- Added CVE-2024-45195 - Apache OfBiz - Remote Code Execution
- Added CVE-2024-6893 - Journyx - XML External Entities Injection (XXE)
- Added CVE-2024-6670 - Progress WhatsUp Gold - SQL Injection

  ()

Technology Fingerprints

- Added SolarWinds Web Help Desk Detection
- Added Journyx Detection
- Fingerprint Enhancements for Progress Whatsup Gold
- Fixed bug resulting in inaccurate version numbers for dynamic WordPress fingerprinting

August 28, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.08.28

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-36104 - Apache OFBiz - Remote Code Execution
- Added CVE-2024-38856 - Apache OFBiz - Remote Code Execution
- Added CVE-2024-41107 - Apache CloudStack - Authentication Bypass
- Added CVE-2023-37679 - NextGen Healthcare Mirth Connect - Remote Code Execution
- Added CVE-2023-43208 - NextGen Healthcare Mirth Connect - Remote Code Execution
- Added CVE-2024-7928 - CVE-2024-7928 - FastAdmin < V1.3.4.20220530 - Path Traversal
- Added CVE-2024-7593 - Ivanti Virtual Traffic Manager - Authentication Bypass
- Added CVE-2024-28000 Version-Only Check - LiteSpeed Cache - Authentication Bypass

Technology Fingerprints

- Added Ivanti Virtual Traffic Manager detection
- Added Apache DolphinScheduler detection
- Added FastAdmin detection
- Fixed an issue where HTTP titles with 'Login' were bring incorrectly tagged as Salesforce
- Updated 'Litespeed-Cache' Wordpress Plugin to be detected using **active checks ()**

August 8, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.08.08

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-6922 - Automation Anywhere Automation 360 - Server-Side Request Forgery
- Added CVE-2022-34267 - RWS WorldServer - Authentication Bypass
- Added CVE-2024-37843 - Craft CMS - SQL Injection
- Added CVE-2024-25723 Version Check - ZenML - Authentication Bypass
- Added CVE-2024-38856 - Apache OFBiz - Remote Code Execution
- Added CVE-2024-36104 - Apache OFBiz - Remote Code Execution

Technology Fingerprints

- Added WorldServer Detection
- Added Automation Anywhere Detection
- Added ZenML Detection

July 23, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.07.23

This Attack Surface Management Discovery Engine release includes:

- Disabled unnecessary checks to speed up sslscan
- Re-enabled `uri_check_api_endpoint` task

Bug Fixes

- Fixed source of issue for Azure storage
- Temporarily disabled `microsoft_exchange_hafnium_compromised_webshell`
- Deprecated CPE Formats for Oracle Weblogic

Vulnerability Checks

- Added CVE-2024-5217 - ServiceNow - Template Injection (Database Credentials Dump)
- Added CVE-2024-4879 - ServiceNow - Template Injection
- Added CVE-2023-6380 - OpenCms - Open Redirect
- Added CVE-2023-6379 - OpenCms - Reflected Cross-Site Scripting
- Added CVE-2024-36401 - GeoServer - Remote Code Execution

Technology Fingerprints

- Added Cellopoint Secure Email Gateway technology fingerprints
- Added additional GeoServer technology fingerprints
- Added Jetty HTML Footer technology fingerprint

July 16, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.07.16

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-5910 - Palo Alto Expedition - Authentication Bypass

July 10, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.07.10

This Attack Surface Management Discovery Engine release includes:

- Added Dynamic Wordpress Plugin Fingerprinting Capability
- Disabled `uri_check_api_endpoint` in all Workflows

Bug Fixes

- Fixed Potential False Positive - Microsoft Exchange Hafnium Compromised Webshell
- Fixed bug where some Inferred CVEs were not linking to Mandiant Advantage Threat Intelligence (MATI)
- Fixed "undefined method nil" bug with the Azure integration that was preventing Entities from being fetched
- Fixed " `missing keyword: gcp_org_id` " bug with the Google Cloud integration that was preventing Entities from being fetched

Vulnerability Checks

- Added CVE-2024-6387 - Remote Unauthenticated Code Execution Vulnerability in OpenSSH Version Check
- Added CVE-2024-34102 - Adobe Commerce - XML External Entity Injection

Technology Fingerprints

- Added Oracle Solaris technology fingerprints

July 1, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.07.01

This Attack Surface Management Discovery Engine release includes:

- Support for Azure Entities via OCAI

Bug Fixes

- Fixed bug that allowed tasks to continue run or be requeued after a scan is completed
- Optimized redirect handling to block specific URLs

- Fixed TLS Handshake failures with a few legacy servers

Vulnerability Checks

- Fixed NameError: undefined local variable `our_version` for Prestashop CVE
- Added CVE-2024-31848 - CData API Server - Authentication Bypass
- Added CVE-2024-32399 - RaidenMAILD - Arbitrary File Read
- Added CVE-2024-28995 - SolarWinds Serv-U - Arbitrary File Read
- Added CVE-2024-31849 - CData Connect - Authentication Bypass
- Added CVE-2024-31850 - CData Arc - Authentication Bypass
- Added CVE-2024-31851 - CData Sync - Authentication Bypass

Technology Fingerprints

- Corrected CPE product name
- Updated fingerprinting timeouts and retries
- Updated product name and version for Palo Alto Pan OS
- Added CData Product technology fingerprints
- Added polyfill.js and polyfill.io technology fingerprints
- Added RaidenMAILD technology fingerprints
- Added FreeBSD Operating System technology fingerprints
- Added Oracle Linux Operating System technology fingerprints
- Added Prometheus Monitoring Tool technology fingerprints

June 25, 2024 ASM Discovery Engine Release - Scan Ranges Expanded

Mandiant Advantage Attack Surface Management (MA-ASM) has added an additional source IP scanning ranges:

- 34.19.127.192/28
- 34.19.116.48/28
- 34.19.127.208/28
- 34.19.127.176/28

For more information, see **ASM Scan Ranges** **(https://docs.mandiant.com/home/asm-scan-ranges)**.

June 20, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.06.20

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-23692 - Rejetto HTTP File Server (HFS) - Remote Code Execution

June 11, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.06.11

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-4358 - Telerik Report Server - Authentication Bypass
- Added CVE-2024-4577 - PHP - Remote Code Execution

May 30, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.05.30

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-4040 - CrushFTP - Server-Side Template Injection
- Added CVE-2024-3273 - D-Link Network Attached Storage - Remote Code Execution
- Added CVE-2024-4956 - Sonatype Nexus Repository Manager 3 - Arbitrary File Read
- Added CVE-2024-24919 - Check Point Security Gateway - Arbitrary File Read
- Enhanced multiple Active Checks to identify vulnerabilities accurately, while minimizing the impact on target assets:
  - Adobe Coldfusion Arbitrary Code Execution (CVE-2018-15961)
  - Cisco HyperFlex Unauthenticated Remote Code Execution(CVE-2021-1499)
  - Dynamicweb Logic Flaw Leading to Remote Code Execution (CVE-2022-25369)
  - F5 BIG-IP - Remote Code Execution (CVE-2023-46747)
  - F5 BIG-IP/BIG-IQ - Remote Code Execution (CVE-2021-22986)
  - Fortra FileCatalyst - Remote Code Execution (CVE-2024-25153)
  - Fortinet FortiNAC - Remote Code Execution (CVE-2022-39952)
  - Oracle E-Business Suite - Remote Code Execution (CVE-2022-21587)
  - SAP NetWeaver Privilege Escalation (CVE-2020-6287)
  - SysAid On-Premise - Remote Code Execution (CVE-2023-47246)
  - WSO2 - Remote Code Execution (CVE-2022-29464)
  - Zimbra Collaboration Suite - Remote Code Execution (CVE-2022-37042)

Technology Fingerprints

- Updated metadata for Konica Minolta Multifunction Printer

May 23, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.05.23

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-4040 - CrushFTP - Server-Side Template Injection
- Added CVE-2024-3273 - D-Link Network Attached Storage - Remote Code Execution
- Added CVE-2021-22986 - F5 BIG-IP/BIG-IQ - Remote Code Execution - Check Refactor

Technology Fingerprints

- Added Treasure Data Fluent Bit technology fingerprints

May 20, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.05.20

This Attack Surface Management Discovery Engine release includes:

- Enhancements to the iis_shortnames_misconfiguration task.

Bug Fixes

- Enhanced support for creating large sets of Entities from the Google Cloud integration.
- Fixed version extraction bug in Apache HTTP Server.

Mandiant

May 9, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.05.09

This Attack Surface Management Discovery Engine release includes:

- Provided vendor and product details in proof for Issues created due to fingerprints

Bug Fixes

- Fixed fingerprint tags causing Exposed SNMP Service false positives
- Corrected incomplete version extraction for Drupal fingerprints
- Corrected false positive Issues related to CVE-2021-38647
- Changed CVE-2024-21893 vulnerability check confidence to potential
- Adjusted protocol to bypass checks for Insecure Redirect Patterns if connection problems within the redirect chain result in incomplete data

Vulnerability Checks

- Remediated CVE-2023-29357 check that was not detecting SharePoint Issue

Technology Fingerprints

- Enhanced Nginx Default Page detection

May 1, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.05.01

This Attack Surface Management Discovery Engine release includes:

- Added support to scan non-common ports for HTTP services.

Bug Fixes

- Fixed a bug causing some issues with Microsoft Exchange Server Issue Detection.
- Fixed a bug causing detection of jQuery version 1.10 on a website with jQuery 3.7.0.
- Fixed a bug causing scans to fail to identify open ports.
- Fixed a bug causing incomplete version detection for backported packages and false positive results.
- Fixed a bug with the Google Cloud Inbound Integration not creating Domain or DNS Entities.

Vulnerability Checks

- Added CVE-2023-48023 - Anyscale Ray - Server Side Request Forgery
- Added detection of Exposed Ray Clusters.

Technology Fingerprints

- Added detection of Anyscale Ray HTTP Dashboard.

April 25, 2024 ASM Release

New Field for Issue Exports

A `Uid` field has been added to Issue Exports. If you depend on a specific column order in relation to Mandiant Advantage Attack Surface Management (MA-ASM) Exports, consider this as you review exported data moving forward.

See **Exporting Search Results** **(https://docs.mandiant.com/home/asm-export-search-results)** for a comprehensive list of fields associated with MA-ASM Issues, Entities, and Technologies Exports.

April 16, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.04.16

This Attack Surface Management Discovery Engine release includes:

- Fingerprinting functionality has been considerably enhanced to enable greater efficiency and accuracy around technology identification

Bug Fixes

- Fixed a bug causing some Issues to have no details
- Fixed a bug causing NetworkService and Uri Entities to be in scope when the related IpAddress Entity is out of scope
- Fixed a bug causing an invalid threat intelligence link to be added to some Issues in the proof

Vulnerability Checks

- Added CVE-2024-26198 - Microsoft Exchange Server - Remote Code Execution - Version Check
- Added CVE-2024-3400 - Active Vulnerability Check - Palo Alto GlobalProtect - Remote Code Execution

Technology Fingerprints

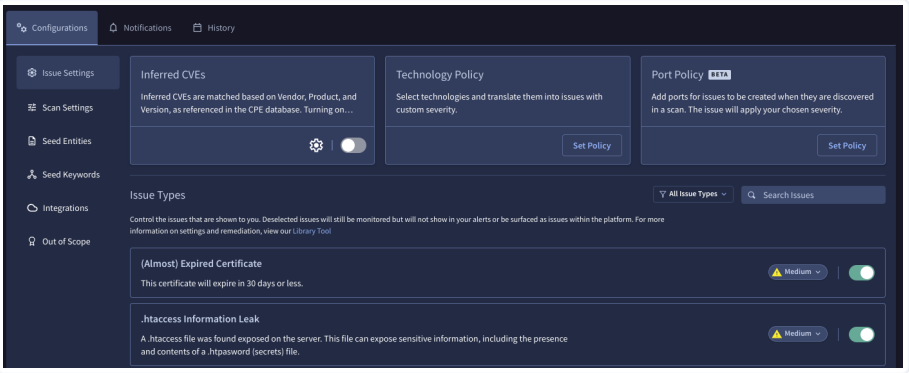
- Added WP Engine Advanced Custom Fields

April 15, 2024 ASM Release

Issue Settings

In Mandiant Advantage Attack Surface Management (MA-ASM), you can now use a wider variety of Issue Settings to curate what Issues you see for each individual Collection. For more detailed information, see the **Issue Settings (https://docs.mandiant.com/home/asm-issue-settings)** documentation.

> Technology Policy and Port Policy do not appear for all Collections. These option are gradually being released.



Issue Settings for a Collection

April 4, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.04.04

This Attack Surface Management Discovery Engine release includes:

- Implemented Issue configuration changes to support Mandiant Advantage Attack Surface Management (MA-ASM) platform feature. This includes the addition of Technology and Port violation policies.

Bug Fixes

- Fixed bug causing missing OpenSSH inferred Issues
- Fixed bug causing missing Node JS Error page detection
- Fixed bug causing missing Yandex Metrica - Cookies Match detection
- Fixed bug causing some scans to run multiple times and not complete
- Re-enabled Check Domain Registration Availability task for domain Entities
  ()

Vulnerability Checks

- Added CVE-2021-44529 - Ivanti - Endpoint Manager Cloud Service Appliance - Remote Code Execution Active Check
- Added CVE-2019-7256 - Linear eMerge - Remote Code Execution Active Check
- Added CVE-2024-21410 - Passive Vulnerability Check - Microsoft Exchange Server - Elevation of Privilege

Technology Fingerprints

- Added FortiClient Endpoint Management Server Detection

April 3, 2024 ASM Discovery Engine Release - Scan Ranges Expanded

Mandiant Advantage Attack Surface Management (MA-ASM) has added an additional source IP scanning range: 8.34.210.32/27

For more information, see **ASM Scan Ranges** **(https://docs.mandiant.com/home/asm-scan-ranges)**.

March 28, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.03.28

This Attack Surface Management Discovery Engine release includes:

- Added several Kubernetes Checks Enhancements, including:
  - Added etcd instance Issue
  - Added Kubernetes API exposure Issue
  - Added etc publicly accessible keys Issue
  - Fixed confusing Kubernetes sensitive content exposure Issue

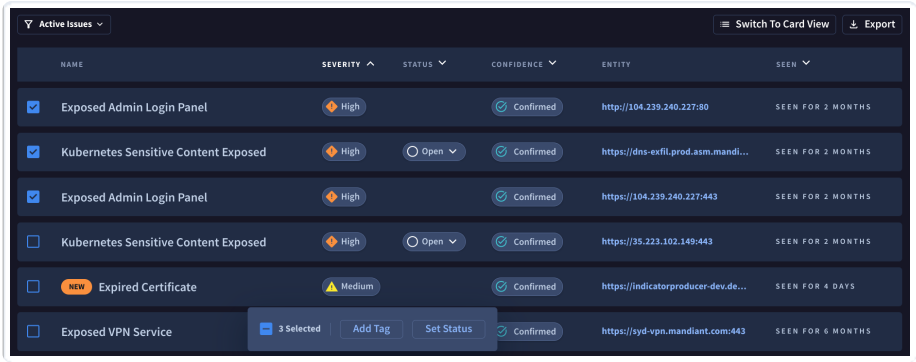
Technology Fingerprints

- Enhanced Kubernetes fingerprints, added version detection and etcd detection

March 28, 2024 ASM Release

Bulk Select

In Mandiant Advantage Attack Surface Management (MA-ASM), you can now use the bulk select feature to apply a variety of actions to multiple Issues or Entities at the same time. For more detailed information, see the **Bulk Select** **(https://docs.mandiant.com/home/asm-bulk-select)** documentation.



A list of six Active Issues in Table View. Three of the Issues are selected for modification.

March 21, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.03.21

This Attack Surface Management Discovery Engine release includes:

- Added links for all fingerprints to DefaultPage Issue remediation.
- Added Exposed Database Service (MSSQL) Issue.

Bug Fixes

- Fixed bug causing some web spidering tasks to fail.
- Addressed confusing inferred Issue names and descriptions.

Vulnerability Checks

- Added CVE-2024-25153 Active Vulnerability Check - Forta FileCatalyst - Remote Code Execution.
- Added CVE-2023-34993 Active Vulnerability Check - Fortinet Wireless LAN Manager - Remote Code Execution.
- Added Active Vulnerability Check - Fortinet Wireless LAN Manager - Sensitive Information Disclosure.

Technology Fingerprints

- Enhanced detection methods for:
  - Okta
  - ServiceNow
- Added new detection coverage for:
  - Fortinet Wireless LAN Manager
  - Fortra FileCatalyst
  - Slack
  - Splunk
  - Tanium

March 14, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.03.14

This Attack Surface Management Discovery Engine release includes:

- Added current task count to scan history tab for active scans.

Vulnerability Checks

- Added CVE-2024-27198 - JetBrains TeamCity - Authentication Bypass Active Check.
- Added CVE-2024-27199 - JetBrains TeamCity - Authentication Bypass Active Check.
- Fixed bug with CVE-2019-18818 - Strapi CMS Active Check.
- Fixed bug with CVE-2023-46747 - F5 BIG-IP Active Check.
- Updated metadata for CVE-2024-22024 - Ivanti Connect Secure Active Check.

March 7, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.03.07

This Attack Surface Management Discovery Engine release includes:

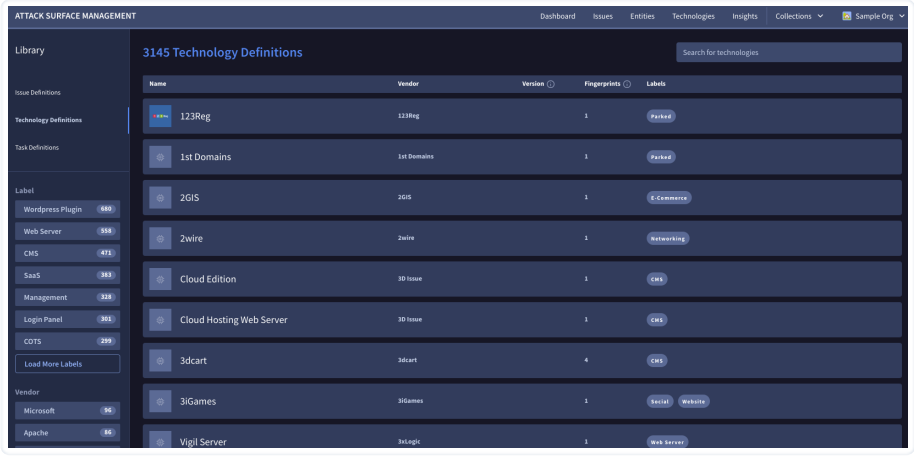
Bug Fixes

- Revised proof for Telerik Crypto Weakness (CVE-2017-9248). This now includes the response body used for vulnerability evaluation.
- Fixed broken MATI URIs provided in Issue descriptions.
- Fixed Featured Video Plus Dynamic Version Extraction.
- Fixed missing http and https open ports in IpAddress Entity.
- Included a version check for Ivanti Connect Secure (for unpatched versions).

March 7, 2024 ASM Release

Enhanced Technology Definitions

The Mandiant Advantage Attack Surface Management (MA-ASM) Library now displays a streamlined list of fingerprinted technologies, eliminates duplicates, includes fingerprint counts, and offers updated documentation for better understanding and usability.



For more detailed information, see the **Technology Library (https://docs.mandiant.com/home/asm-technologies#library)** documentation.

February 28, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.02.28

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Corrected function used for creating DNS Entities.

February 22, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.02.22

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Fixed an issue where reverse WHOIS was not finding domains based on UniqueKeyword
- Fixed an issue with incorrect keyword parsing in the Code Repository Discovery & Assessment Scan Workflow

Vulnerability Checks

- Added CVE-2023-35368 - Microsoft Exchange Server - Remote Code Execution Vulnerability Check
- Added CVE-2023-35388 - Microsoft Exchange Server - Remote Code Execution Vulnerability Check
- Added CVE-2023-38182 - Microsoft Exchange Server Remote Code Execution Vulnerability Check
- Added CVE-2023-38181 - Microsoft Exchange Server Spoofing Vulnerability Check
- Added CVE-2023-36777 - Microsoft Exchange Server Information Disclosure Vulnerability Check
- Added CVE-2023-36757 - Microsoft Exchange Server Spoofing Vulnerability Check
- Added CVE-2023-36744 - Microsoft Exchange Server Remote Code Execution Vulnerability Check
- Added CVE-2023-36745 - Microsoft Exchange Server Remote Code Execution Vulnerability Check
- Added CVE-2023-36756 - Microsoft Exchange Server Remote Code Execution Vulnerability Check
- Added CVE-2024-22024 - IVANTI Connect Secure Active Check
- Added CVE-2021-30497 - Ivanti Avalanche - Arbitrary File Read Vulerability Check
- Added CVE-2023-38185 - Microsoft Exchange Server Remote Code Execution Vulnerability Check
- Added CVE-2024-1709 - ScreenConnect - Authentication Bypass Vulnerability Check
- Enhanced CVE-2023-46805 Vulnerability Check

Technology Fingerprints

- Updates to ScreenConnect Fingerprint
- General fingerprint enhancements to vendor names for accuracy/consistency

February 20, 2024 ASM Release

AWS Inbound Integration Updated

As a best practice, AWS recommends requiring an external ID when creating a role to be used by a third party. To account for this, Mandiant Advantage Attack Surface Management (MA-ASM) now provides an **AWS External ID** to be used when integrating MA-ASM and AWS.

While existing AWS integrations will not be affected, requiring an external ID is more secure.

For more detailed information on how to use this external ID, see the **ASM AWS Integration**

(https://docs.mandiant.com/home/asm-aws-integration) documentation.

February 15, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.02.15

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Use AWS Lambda as backup to check s3 bucket existence
- Fixed release date and enhanced description/remediation for leaked secrets Issue
- Citrix Product CPE cleanup
- Only hide an Entity if connection reset is the only fingerprint
- Fixed Godaddy integration errors
- Fixed generic fingerprints to remove unnecessary follow-on http calls

Vulnerability Checks

- Added CVE-2024-22024 Vulnerability Check - (Ivanti Connect Secure - XML External Entity Injection)

Technology Fingerprints

- Microsoft Exchange fingerprint enhancements
- Added Ivanti Avalanche Detection Technology Fingerprint
- Improved the following twelve fingerprints:
  - Adobe CRXDE Lite
  - Apache Hadoop
  - Connect Box
  - Connectwise
  - Draytek
  - Entrust IdentityGuard
  - Hadoop Yarn
  - HiveManager
  - Honeywell Tuxedo
  - Idera
  - Keenetic
  - One Identity Password Manager

February 8, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.02.08

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2024-0204 Vulnerability Check - (GoAnywhere MFT - Authentication Bypass)
- Added CVE-2024-21893 Vulnerability Check - (Ivanti Connect Secure - Server-Side Request Forgery)

Technology Fingerprints

Added or improved fingerprints for the following 13 vendors:

- Apache Flink
- Canon Remote UI
- Cisco Docsis
- Cisco Finesse

- Cisco Web
- Citrix SD-WAN
- Codesys WebVisu
- frp
- Somfy
- SonarQube
- Synnefo
- Traefik
- Zenario

February 1, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v2024.02.01

This Attack Surface Management Discovery Engine release includes:

- Added Secrets Exposed check to detect and report leaked secrets (API Keys, Client Secrets, S3 Bucket Names, Access Keys) in web pages.
- IP addresses are now resolved and stored for AppEndpoint Entities.
- Added CVE-2023-36847 Identifier to Juniper JunOS RCE Chain (CVE-2023-36844/36845/36846)

Bug Fixes

- Fixed bug causing false positives when port scanning certain Entities.
- Fixed bug causing GoDaddy integration to return no Entities.
- Fixed bug where Entities created through cloud integrations did not have the cloud_seed attribute.
- Fixed bug preventing scans from completing due to malformed URI Entity name.
- Fixed bug causing two Issues to be created for the same Entity under certain conditions.

Vulnerability Checks

- Added CVE-2024-23897 Vulnerability Check - (Jenkins - Arbitrary File Read)

January 23, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.43.0

This Attack Surface Management Discovery Engine release includes:

- DNS TLD enumeration now covers the complete list of IANA TLDs.
- Added or improved the remediation for exposed database issues.

Bug Fixes

- Individual IP addresses in a out-of-scope netblock are now enumerated and scoped out.
- Fixed a bug where a check didn't run because the Issue name and the task name were not the same.

Technology Fingerprints

- Added Ivanti Connect Secure technology fingerprints

Vulnerability Checks

- Added CVE-2023-22527 Vulnerability Check - (Atlassian Confluence Remote Code Execution)
- Added CVE-2023-46805 Vulnerability Check - (Ivanti Authentication Bypass)
- Added CVE-2024-21887 Vulnerability Check - (Ivanti Connect Secure - Remote Code Execution)

January 12, 2024 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.42.0

This Attack Surface Management Discovery Engine release includes:

Updates to Apache Tomcat Manager detection.

Bug Fixes

- Resolved issue where DnsRecord Entities were incorrectly being hidden when TLD resolved wildcards.

Vulnerability Checks

- Added CVE-2023-3368 Vulnerability Check - (Chamilo - Remote Code Execution)
- Added CVE-2023-49070 Vulnerability Check - (Apache OFBiz - Remote Code Execution)
- Added CVE-2021-29200 Vulnerability Check - (Apache OFBiz - Remote Code Execution)
- Added CVE-2023-51467 Vulnerability Check - (Apache OFBiz - Remote Code Execution)
- Added CVE-2023-43177 Vulnerability Check - (CrushFTP - Remote Code Execution)

December 15, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.41.0

This Attack Surface Management Discovery Engine release includes:

A WebAccount Entity type is now available.

Bug Fixes

- Resolved a bug causing AWS S3 subdomain takeover false positives.
- Resolved a bug causing wayback search tasks to respond with inconsistent results.
- Resolved a bug causing false positives with CVE-2018-7600.

Vulnerability Checks

- Added CVE-2019-18818 Active Check (Strapi CMS)
- Added CVE-2019-19609 Version Check - (Strapi CMS - Remote Code Execution)
- Added CVE-2023-49103 Active Vulnerability Check - (ownCloud - Sensitive Information Disclosure)

Technology Fingerprints

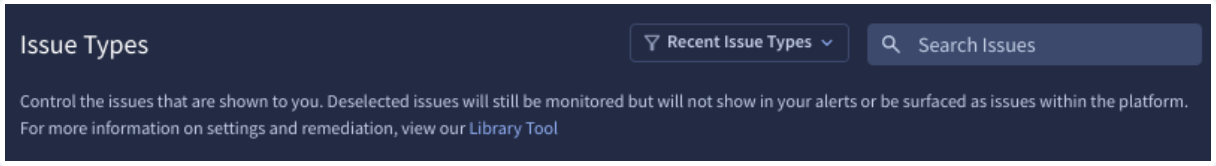
- Updates to Strapi CMS fingerprints

December 15, 2023 ASM Release

Disable specific Issue types before initial Collection Scans

This feature lets you create Collections without running them automatically. This provides you with the opportunity to decide what Issue types to disable before running the initial Collection scan. For more information, see the **Create a Collection documentation (https://docs.mandiant.com/home/asm-create-a-collection)**.

Collections Settings (https://docs.mandiant.com/home/asm-customize-collections) have been updated to aid in navigation. New filters and search options provide easier methods to find Issues when configuring **Issue Settings (https://docs.mandiant.com/home/asm-issue-settings)**.



December 6, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.40.0

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2023-41265/41266 Active Vulnerability Check - (Qlik Sense - Authentication Bypass)

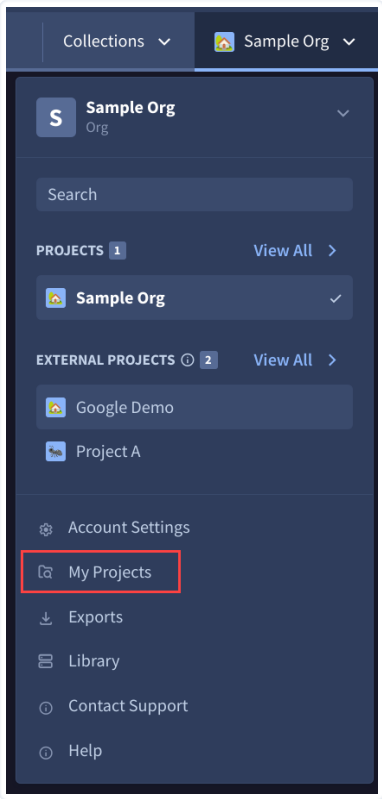
Technology Fingerprints

- Added Qlik Sense technology fingerprints

December 5, 2023 ASM Release

Organization and Project management updates

- The organization switcher is now part of the **Projects and Settings** menu. See the **organization switcher documentation (https://docs.mandiant.com/home/asm-organization-switcher)** for more information.
- Projects are now available on the **My Projects** dashboard which is accessible from the **Projects and Settings** menu. See the **Project documentation (https://docs.mandiant.com/home/asm-projects)** for more information.



December 4, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.39.0

This Attack Surface Management Discovery Engine release includes:

- Resolved a bug causing false positive subdomain takeover Issues

November 29, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.38.0

This Attack Surface Management Discovery Engine release includes:

- Enhanced typosquat detection to add support for TLDs in domain permutations

Bug Fixes

- Updated Citrix NetScaler checks including misspellings in the content length headers
- Fixed duplicate Issues due to generic checks
- Updated to only run SSL checks if an Entity is not hidden

Vulnerability Checks

- Added CVE-2023-36844/36845/36846 Active Vulnerability Check - (Juniper J-Web - Remote Code Execution)
- Added CVE-2023-35813 Active Vulnerability Check - (Sitecore - Remote Code Execution)
- Added CVE-2023-29357 Active Vulnerability Check - (Microsoft SharePoint Server - Authentication Bypass)
- Added CVE-2023-47246 Active Vulnerability Check - (SysAid On-Premise - Remote Code Execution)
- Added Vulnerability Check for Hashicorp Consul KV Exposed Secrets

Technology Fingerprints

- Added new Storage Bucket technology fingerprints
- Added SysAid Help Desk Software Detection technology fingerprint

November 16, 2023 ASM Release

Entity categories

Entities types are now organized by category. For information about Entity type categorization, see the **Entity Types documentation (https://docs.mandiant.com/home/asm-entities#entity-types)**.

November 15, 2023 ASM Release

Scan Rate terminology update

The scan rate term "ad-hoc" has been updated to "on demand."

The **Collection Scan Rate documentation (https://docs.mandiant.com/home/asm-collection-scan-rate)** reflects this update.

November 15, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.37.0

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Updates to PHP Detection

Checks

- Enhanced Heartbleed check
- Added CVE-2023-24488 Vulnerability Check (Citrix NetScaler ADC/Gateway - Reflected Cross-Site Scripting)
- Added CVE-2006-3392 Vulnerability Check (Webmin/Usermin - Arbitrary File Read)Resolved a bug causing false positive Insecure Redirect Pattern Issues

November 10, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.36.0

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Resolved a bug causing false positive Insecure Redirect Pattern Issues

Vulnerability Checks

- Added CVE-2023-46604 Vulnerability Check (Apache ActiveMQ - Remote Code Execution)

November 9, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.35.0

This Attack Surface Management Discovery Engine release includes:

Bug Fixes

- Revolved a bug related to scope on Entity zone records
- Resolved a bug causing hidden Entities to be included in open ports for IP address Entities

Checks

- Added CVE-2023-23752 Vulnerability Check (Joomla Sensitive Information Leak)
- Added CVE-2023-23333 Vulnerability Check (SolarView Compact Remote Code Execution)
- Added CVE-2023-1671 Vulnerability Check (Sophos Web Appliance Remote Code Execution)
- Added CVE-2023-22518 Vulnerability Check (Atlassian Confluence authentication bypass)
- Added CVE-2023-32235 Vulnerability Check (Ghost CMS Path Traversal)
- Added CVE-2023-34960 Vulnerability Check (Chamilo LMS command injection)
- Added CVE-2023-29919 Vulnerability Check (SolarView Compact - Arbitrary File Read)
- Added CVE-2023-46747 Vulnerability Check (F5 BIG-IP remote code execution)
- Added Active Check (ServiceNow Sensitive Data Exposure via Widget Misconfiguration)

Technology Fingerprints

- Added Sophos Web Appliance Detection Technology Fingerprint
- Added support for Point-to-Point Tunneling Protocol (PPTP) negotiation during technology fingerprinting process
- Added additional detection fingerprints for F5 Big IP Configuration Utility

November 2, 2023 ASM Release

Adjustable Scan Rates

Customers can now set their own scan rates for Collections. For more information on how to change the scan rate for a Collection, see the **Collection Scan Rate documentation** **(https://docs.mandiant.com/home/asm-collection-scan-rate)**.

November 1, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.34.0

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- Added CVE-2023-4568 Vulnerability Check (PaperCut NG Unauthenticated XMLRPC Functionality)
- Added CVE-2023-40779 Vulnerability Check (IceWarp Mail Server Deep Castle 2 Open Redirect)
- Added Apache Hadoop YARN Remote Code Execution Vulnerability Check
- Added CVE-2023-39598 Vulnerability Check (IceWarp Email Client Cross Site Scripting)
- Added CVE-2023-37728 Vulnerability Check (IceWarp Webmail Server Reflected Cross Site Scripting)

- Added CVE-2023-38646 Vulnerability Check (Metabase Remote Code Execution)
- Added CVE-2023-39361 Vulnerability Check (Cacti SQL Injection)
- Added CVE-2023-0126 Vulnerability Check (SonicWall Arbitrary File Read)
- Added CVE-2023-20198 Vulnerability Check (Cisco IOS XE Software Web UI Privilege Escalation)

November 1, 2023 ASM Release

DNS Made Easy integration

For more information, visit the **ASM DNS Made Easy Integration documentation** **(https://docs.mandiant.com/home/asm-dns-made-easy-integration)**.

October 30, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.33.0

This Attack Surface Management Discovery Engine release includes:

- Revolved a bug causing duplicate Issues for the same Entity.
- Resolved a bug causing some network services to skip the enrichment process.
- Resolved a bug causing some ports to not be shown for IP address Entities.
- Resolved a bug causing duplicate MySQL Fingerprints.

Vulnerability Checks

- Added CVE-2023-20198 Indicator of Compromise Check (Cisco IOS XE Privilege Escalation)
- Added CVE-2023-4966 Vulnerability Check (Citrix NetScaler ADC/Gateway Sensitive Information Disclosure)
- Added CVE-2023-5244 Vulnerability Check (Microweber Reflected Cross-Site Scripting)
- Added CVE-2023-4714 Vulnerability Check (Playtube Sensitive Information Leak)
- Added CVE-2023-4451 Vulnerability Check (Agentejo Cockpit Reflected Cross-Site Scripting)

Technology Fingerprints

- Enhanced Microweber technology fingerprint

October 19, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.32.0

This Attack Surface Management Discovery Engine release includes:

- Revolved a bug causing duplicate Issues for the same Entity.

Technology Fingerprints

- Updates to Citrix Netscaler Gateway and ADC fingerprints
- Update fingerprints for Cisco IOS XE

October 11, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.31.0

This Attack Surface Management Discovery Engine release includes:

- Improved remediation for IIS Shortnames Misconfiguration
- Added nodejs remediation for Insecure Cookie (Missing 'HttpOnly' Attribute) Issue

Vulnerability Checks

- Added CVE-2023-40044 vulnerability check (Progress WS_FTP Server remote code execution)
- Added CVE-2023-33246 vulnerability check (Apache RocketMQ remote code ececution)
- Added CVE-2023-22515 vulnerability check (Atlassian Confluence broken access control)

Technology Fingerprints

- Improved Progress technology fingerprints
- Improved Atlassian Confluence technology fingerprints

September 29, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.30.0

This Attack Surface Management Discovery Engine release includes:

Vulnerability Checks

- **Improved vulnerability check for CVE-2022-22536 (SAP NetWeaver)**
  Severity adjusted, remediation added, refactored check logic, more information added to proof, and added testing coverage.
- **Added vulnerability check for CVE-2023-42793 (JetBrains TeamCity authentication bypass)**
  A critical authentication bypass that affects on-premises instances of JetBrains TeamCity, a CI/CD server.
- **Added vulnerability check for CVE-2023-36845 (Juniper J-Web remote code execution)**
  A vulnerability in J-Web of Juniper Networks Junos OS on EX and SRX Series enables unauthenticated attackers to remotely execute code.

Technology Fingerprints

- **Improved fingerprint check scope and logic**
  Enhanced technology identification via HTTP.
- **Improved technology fingerprint for JetBrains TeamCity**
  Enhanced existing fingerprint logic and added favicon matching.
- **Improved technology fingerprinting for Juniper devices**
  Added SNMP fingerprint, and added additional fingerprint checks to detect SRX devices based on the form header and title.
- **Improved fingerprint coverage for Shelly IoT**
  Added Shelly Plus Plug S, Shelly Plus 1, Shelly Uni, Shelly 1L, Shelly Motion 1, and Shelly RGBW2 fingerprint patterns.

September 25, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.29.0

This Attack Surface Management Discovery Engine release includes:

- **Improved Wordpress Exposed API Issue**
  Reworded the description, added remediation, and added additional references.
- **Improved Exposed Admin Panel Issues**
  Added path in which the fingerprint was discovered to the Issue proof. Created unique Issues for each technology where several fingerprints are discovered.
- **SAP - Memory Pipes Desynchronization (CVE-2022-22536) Active Check temporarily disabled**
  There are active and passive variants of this check. The majority of the findings are passive so the active check has been disabled until it is refactored to work with the new socket helper.
- **Issue reference updates**
  Updated URI reference in description for "Updated Suspicious Web Resource Requested", "Vulnerable Citrix Netscaler (CVE-2019-19781)", "Vulnerable Tomcat - Deserialization in Filestore (CVE-2020-9484)", "Tomcat PersistManager Deserialization RCE (CVE-2020-8494)" and "Jupyter Exposed UI Detection" Issues.

Vulnerability Checks

- **Improved VMWare Workspace One vulnerability check (CVE-2022-22972)**
  Added remediation and tests. Improved check for consistency and reliability of detection.
- **Added Acmailer command injection vulnerability check (CVE-2021-20617)**
- **Added Apache CouchDB vulnerability check (CVE-2022-24706)**
- **Added Tenda AC11 Command Injection vulnerability check (CVE-2021-31755)**
- **Added VMware Aria Operations for Logs remote code execution vulnerability check (CVE-2023-20864)**

Technology Fingerprints

- **Improved fingerprint coverage**
  Added support for compressed responses while fingerprinting technologies via HTTP.
- **Added support for "Configuration Management" technology tag**
- **Improved Tenable fingerprint check**
  Made changes to eliminate false positives when evaluating HTTP response body.
- **Added Puppet technology fingerprints**
  Enables detection of "Puppet" as a vendor, and "Puppet Enterprise", "Puppetboard", "Puppet Dashboard", "PuppetDB" products.
- **Added Pi-Hole technology fingerprints**
  Enables detection of "Pi-Hole" as a vendor/product.
- **Added AVM technology fingerprints**
  Enables detection of "AVM" as a vendor and "FRITZ!Box", "FRITZ!Repeater" as products.
- **Added Shelly IoT technology fingerprints**
  Enables detection of "Shelly" as a vendor, and 1, Plus 1PM, 1 PM, 2.5, EM, Dimmer 2, Pro 1, Duo, 2 Pro, 3EM, PlugS, 4PM as products.
- **Improved Progress MoveIT technology fingerprint**
  Adds cookie-based detection.

September 12, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.28.0

This Attack Surface Management Discovery Engine release includes:

- **Added Third party Workflow to production**
- **Added support for variable cache TTL**
  Previous cache time was hardcoded to 14 days for all data sources. Now 24 hours, 48 hours, 1 week, and 2 weeks are supported.
- **Added Open SMTP Relay check**
- **Added Adobe Coldfusion access control bypass (CVE-2023-38205) vulnerability check**
- **Added Tenda AC11 fingerprint check**
  Mandiant Advantage Threat Intelligence (MATI) rates Tenda router vulnerabilities high. Mandiant Advantage Attack Surface Management (MA-ASM) does not yet have a vuln check.
- **Entity fingerprint logic enhancements**
  Added result verification for Entity identity checks. Also added additional logging to help debug fingerprint failures.
- **Added category to Issue details**
  Category is now present for inferred CVEs.
- **Modified MATI cache TTL**
  Modified MATI caching from 14 days to 7 days so that the IC-score pulled from MATI will refresh faster.
- **Added UniqueKeyword to Code Repository and Assessment Workflow**
- **Fixed Out of Scope bug**
- **Fixed EC2 entity detail bug**
  IpAddress Entities (for public IPs) are now correctly created from EC2 instance details.
- **Fixed typo in Azure Storage Account issue**

Mandiant

September 11, 2023 ASM Release

Introducing Scan History

Scan History lets you visualize changes to an Entity over time. You can compare two scans and see what's changed about an Entity.

For more information, visit the **Scan History documentation** **(https://docs.mandiant.com/home/asm-scan-history)**.

September 7, 2023 ASM Release

Third Party Monitoring Workflow

This new Workflow helps you monitor your supply chain.

For more information, visit the **Scan Workflow templates documentation** **(https://docs.mandiant.com/home/asm-collections-and-workflows#template)**.

September 6, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.27.0

This Attack Surface Management Discovery Engine release includes:

- **Fix for check run logic**
  Addresses the missing Bluekeep check detail.
- **CloudPanel remote code execution (CVE-2023-35885) vulnerability check added**
- **Ivanti Mobileiron remote code execution (CVE-2023-38035) vulnerability check added**
- **Openfire path traversal auth bypass (CVE-2023-32315) vulnerability check added**
- **Pega API fingerprint check added**
  Proactive fingerprint coverage expansion.
- **MobileIron fingerprint enhancements**
  Better, more accurate fingerprint coverage.
- **Openfire fingerprint added**
  New technology fingerprint added, and enables the CVE-2023-32315 check.
- **Cloudpanel fingerprint added**
  New technology fingerprint added, and enables the CVE-2023-35885 check.

August 30, 2023 ASM Discovery Engine Release

Attack Surface Management Discovery Engine release v1.26.0

This Attack Surface Management Discovery Engine release includes:

- **Core base image updated to include support for legacy SSL negotiation**
  Addresses a Citrix Netscaller identification issue.
- **Fixed description typo in Threat Investigation workflow description**
- **Additional properties added to support Third Party workflow**
- **Citrix ShareFile StorageZones Controller RCE (CVE-2023-24489) Vulnerability Check**
- **CVE-2022-26134 ID typo fix**
- **Exposed database coverage now includes CouchDB**
  Port 5984 is now scanned.
- **Exposed Erlang Port Mapper Daemon Issue added**

Port 4369 is now scanned.

- **Enrich URI early termination bug fix**
- **Ident check return bug fix**
  Addresses Bluekeep false negatives.

August 1, 2023 ASM Release

Introducing Collection Workflows

Workflows is a new feature released on August 1, 2023. Workflows 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.

- **External Discovery & Assessment**: Identify shadow IT or unknown assets and vulnerabilities.
- **Authenticated Cloud Discovery & Assessment**: Identify issues across your externally facing cloud assets through 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.
- **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.

For more information, visit the **Create a Collection documentation (https://docs.mandiant.com/home/asm-create-a-collection)**.

July 31, 2023 ASM Release

Corrected response on API errors

Some API requests have been incorrectly returning a 500 Internal Server error. This has been corrected to return a 404 Page Not Found error, when applicable.

July 26, 2023 ASM Release

Chronicle SIEM integration

Customers can automatically send assets and security issues identified by MA-ASM to Chronicle SIEM. MA-ASM Entities and Issues can be correlated with other telemetry events, streamlining detection and automating the tasks of security analysts.

Key Features

- Control the ingest period.
- Set a minimum severity threshold on the Issues presented to the team.
- MA-ASM Entities and Issues populate within the Chronicle event timeline.

For more information, visit the **Chronicle SIEM integration documentation (https://docs.mandiant.com/home/asm-googlesecops-siem-integration)**.

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 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/customer-support)**.

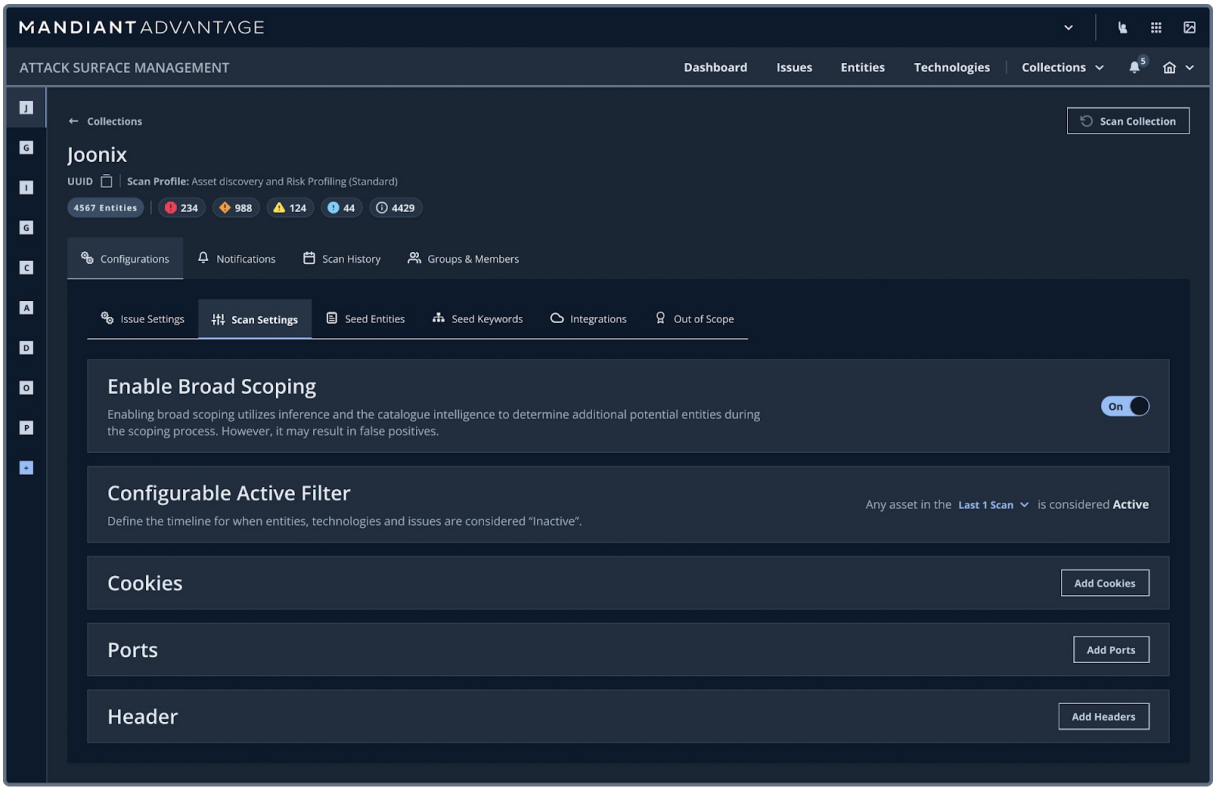
March 28, 2023 ASM Product Release Announcements

We're excited to announce the latest features and enhancements in Mandiant Attack Surface Management.

WHAT'S NEW

Collection Configuration and Scan Changes

Paid customers now have control over the scope of Collection entity discovery with new configuration and scan settings.



Strict Scoping

On March 30th, Strict Scoping will be the new default for Collection scans. Strict Scoping will narrow the discovery and enumeration process to the entities related to the designated Seeds. Upon the completion of scans after March 30th, entities discovered during previous scans will be moved to the 'Inactive' tab on the Entities search page.

Customers can opt into Broad Scoping:

- Broad Scoping utilizes inference and the global intelligence repository to identify additional potential entities during the scoping process. However, it may result in false positives.
- To opt into Broad Scoping, go to **Collection Settings** > **Scan Settings** and toggle **Enable Broad Scoping** to **On**.

Configurable Cookies, Ports, and Header

New Scan Settings enable Attack Surface Management to definitively scope assets that belong to your organization. Custom input types include:

- Cookies
- Ports
- Headers

Configurable 'Active' Filter

Define the timeline for when entities, technologies, and issues are considered 'Inactive'. Go to Collection Scan Settings and choose the quantity of scans between first and last seen.

Expanded Scanning Capabilities

New scanning capabilities allow for new issue creation for:

- Domain Expiration Notification
- Broken Link Detected

Export Enhancements

Entity, technology, and issue CSV exports contain an expanded set of fields, including Issue proof and remediation.

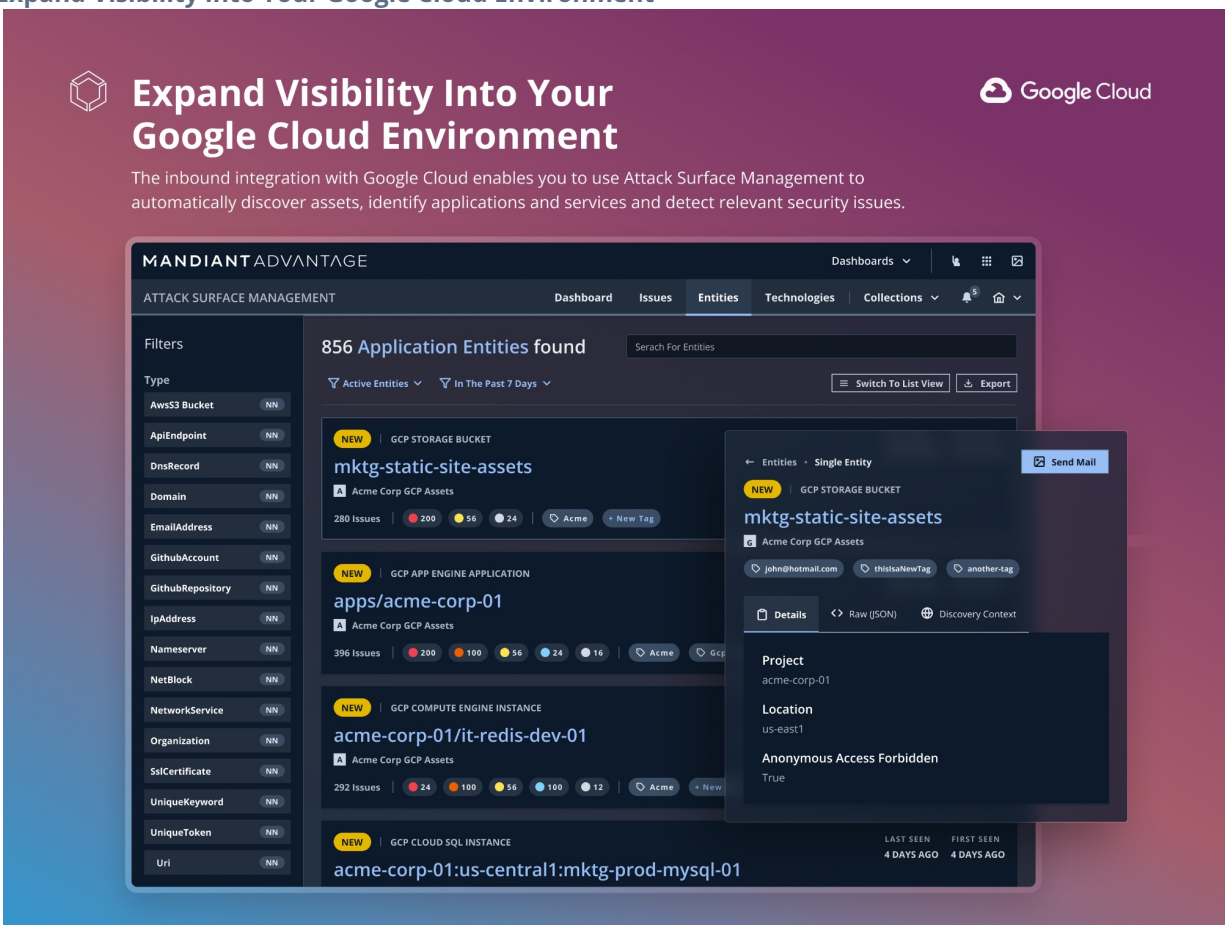
ENHANCEMENTS

- New checks and technology fingerprints are available in the library.
- An API enhancement increased the query limit from 10K to **infinite**. Users can now use the `page_token` to view the next page of results. See **API documentation** (https://docs.mandiant.com/home/asm-api) for details.
- Entity searches now include Search Summaries on the right panel.
- All entity pages now display the related Seed for additional context.
- Mandiant Advantage Splunk App version 1.5 is now available

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

December 14, 2022 ASM Release

Expand Visibility into Your Google Cloud Environment



The Mandiant Advantage Attack Surface Management for Google Cloud is now available.

Head straight to the **integration guide** (https://docs.mandiant.com/home/asm-gcp-integration) now.

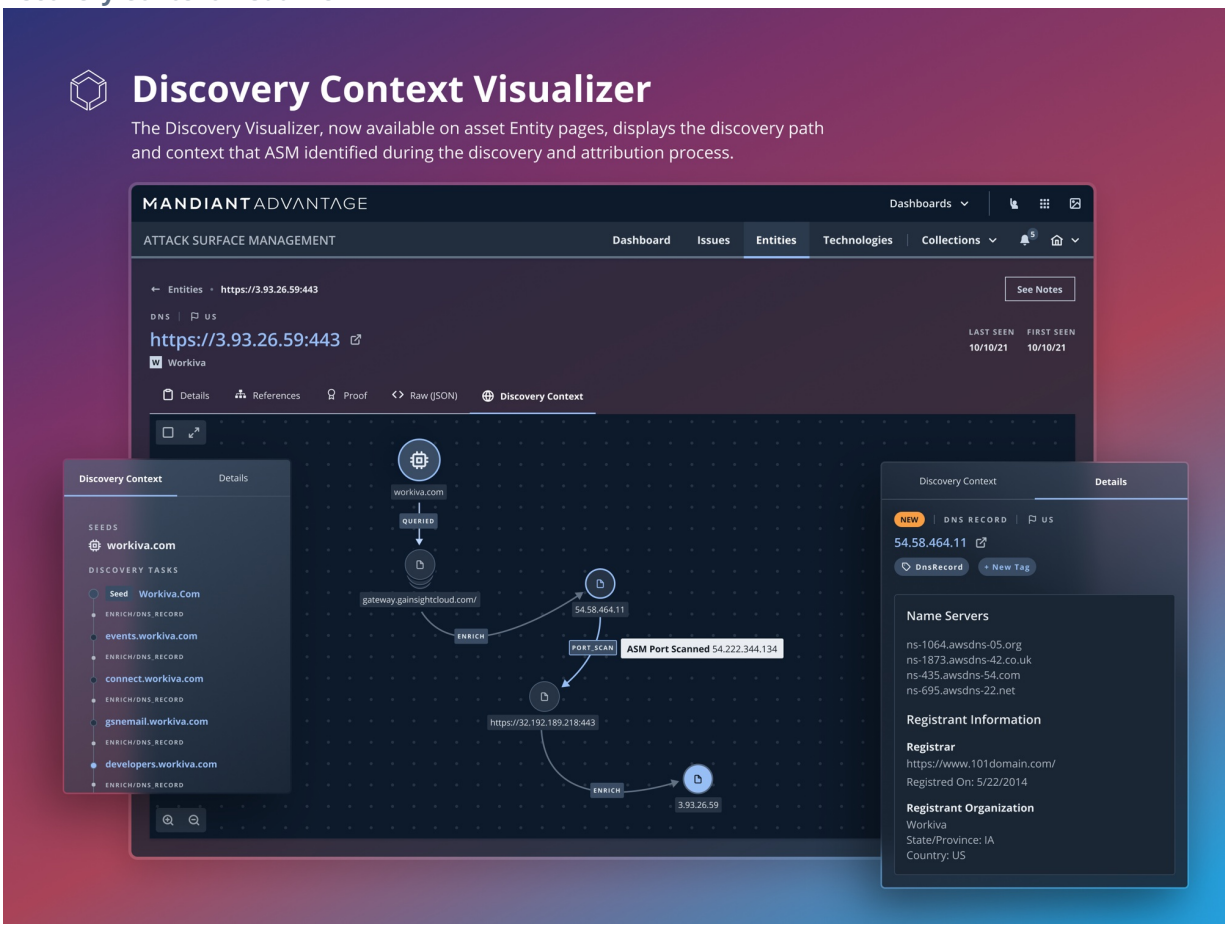
The inbound integration with Google Cloud enables you to use Attack Surface Management to automatically discover assets, identify applications and services and detect relevant security issues. Discoverable asset types include:

- APIs via API Gateway
- Applications
- Cloud Functions
- Cloud SQL Instances
- Compute
- Storage
- DNS

The integration complements the available integrations with Azure, AWS, GitHub, Akamai, Cloudflare, and GoDaddy, delivering extended visibility across hybrid or multi-cloud environments.

November 16, 2022 ASM Release

Discovery Context Visualizer



Why does this asset belong to me?

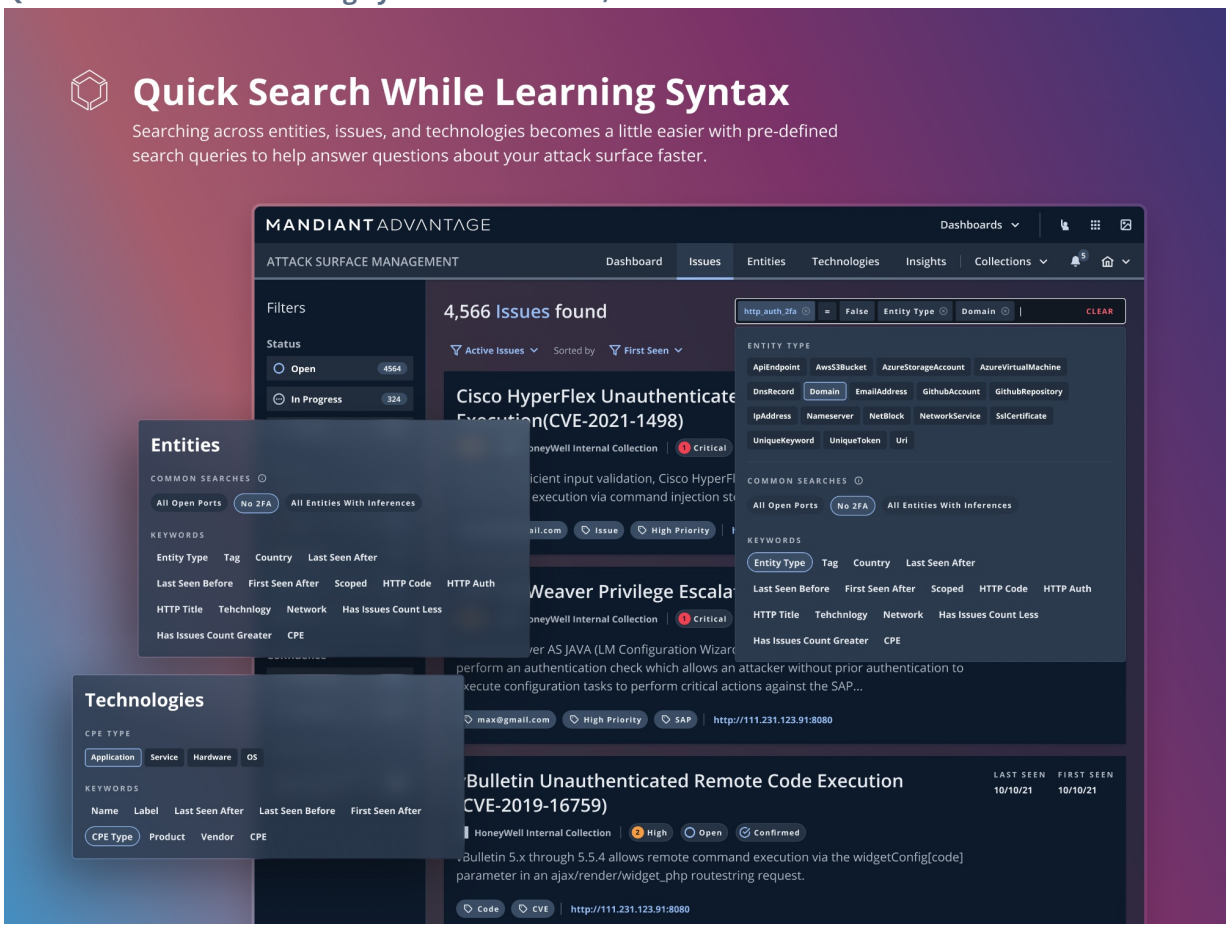
Attack Surface Management (ASM) collection engines perform unique discovery tasks for each type of discoverable asset. These tasks gather information and help ASM determine if the asset belongs to your organization and the security posture of those external assets.

Determining asset attribution to your organization occurs when ASM maps discovered assets to Global Intelligence to assess ownership and whether it is shared, infrastructure, or owned by a third party.

The Discovery Visualizer, now available on asset Entity pages, displays the discovery path and context that ASM identified during the discovery and attribution process.

October 2022 ASM Releases

Quick Search While Learning Syntax - October 20, 2022



Searching across entities, issues, and technologies becomes a little easier with pre-defined search queries to help answer questions about your attack surface faster. Leverage the quick searches available within the search bar to answer your questions while you learn the syntax.

Common Questions

- What are the critical confirmed issues in my attack surface?
- What are the CVEs discovered in my attack surface (potential or confirmed) in the last week?
- Are we running the vulnerable version of the technology with a recently disclosed 0-day?

Manage Remediation with ServiceNow Vulnerability Response - October 13, 2022

The Mandiant Advantage Attack Surface Management App for ServiceNow Vulnerability Response is now available.

Seamless Issue Remediation

ServiceNow Vulnerability Response uses the ASM API to pull issues into your remediation workflows. The integration allows you to do the following:

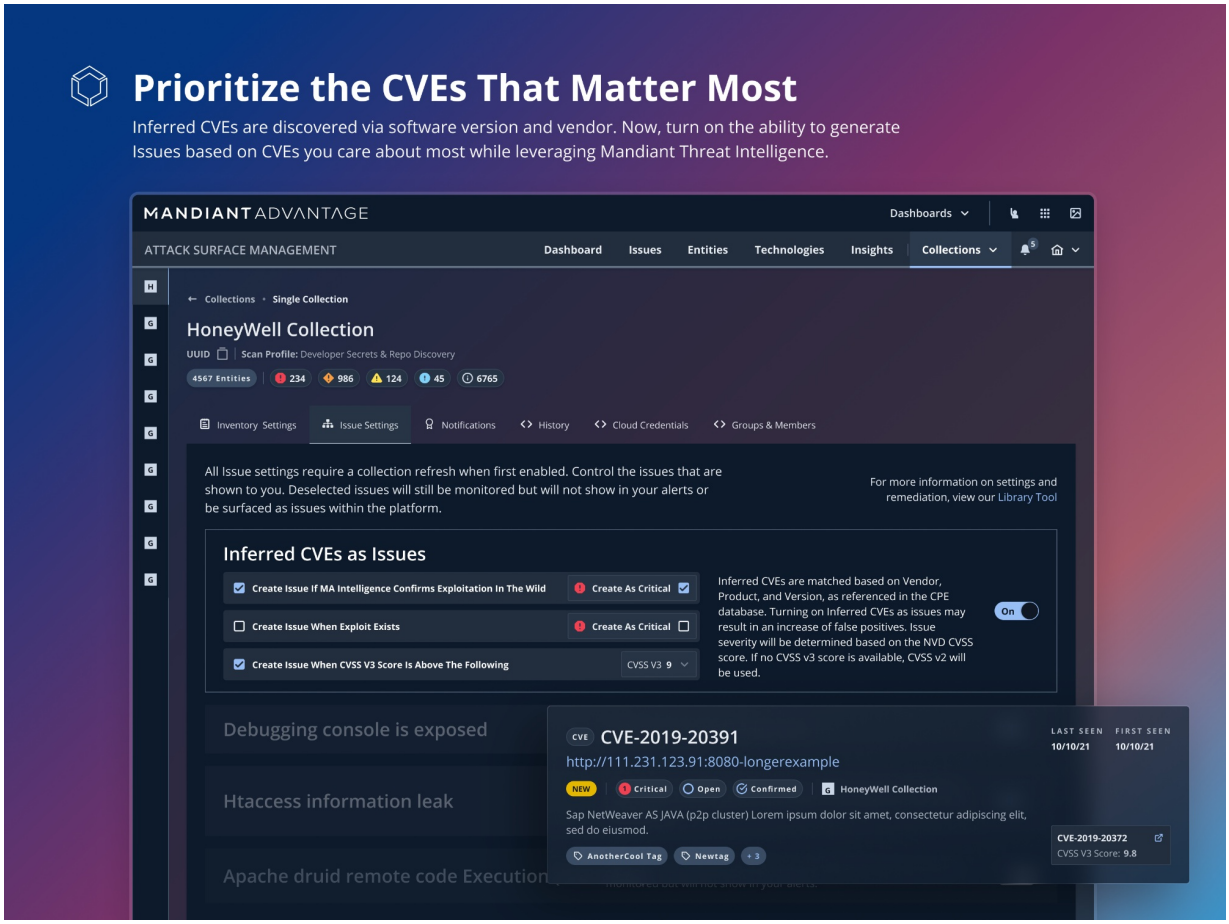
- Pull issues from multiple collections within a single project
- Set a minimum severity threshold on the issues presented to the team

- Configure the issue confidence, bringing in potential, confirmed, or both
- Synchronize issue management between ServiceNow and Attack Surface Management; reflect status changes and remediation progress in both products.

Add the App to your ServiceNow instance today

(https://store.servicenow.com/sn_appstore_store.do#!/store/application/1ce124b4976951104b4edf14a253aff5/1.0.0).

Prioritize the CVEs That Matter Most - October 11, 2022



Generate Issues from Inferred CVEs

Inferred CVEs are discovered via software version and vendor. Now, turn on the ability to generate Issues based on CVEs you care about most while leveraging Mandiant Threat Intelligence.

Head to **Collection Settings** **(https://asm.advantage.mandiant.com/collections)** to configure when inferred CVEs generate issues based on the following:

- Active exploitation seen in the wild
- A public exploit code is available
- Align Issue severity to CVSS v3 score

Exchange Server Zero(0)-Day Vulnerabilities - October 3, 2022

Microsoft recently reported two zero-day vulnerabilities (assigned vulnerability IDs: CVE-2022-41040, CVE-2022-41082) affecting Exchange Server 2013/2016/2019. The vulnerabilities require authentication to execute and are unlikely to be leveraged in a mass exploitation event. Furthermore, though an adversary has allegedly leveraged this vulnerability, no

exploit code has been observed in the wild, limiting access and impact. Mandiant has not observed this activity affecting any customer environments at this time.

Mandiant recommends that organizations apply the **Microsoft suggested workarounds** (https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/)to any on-premises Exchange servers publicly exposed to the internet.

Locate the Exchange Servers Publicly Exposed on the Internet
Follow the link to find your **Microsoft Exchange Servers** (https://asm.advantage.mandiant.com/technologies?table_view=false&search_string=last_seen_after%3Alast_refresh%20%22Microsoft%20Exchange%22) or search for "Microsoft Exchange" in the Technologies page search bar.

We are actively monitoring and will provide a check when more details emerge.

Curate Attack Surface Insights with Custom Dashboards - October 3, 2022

We're excited to announce Custom Dashboards, a new way to curate and customize information from the Mandiant Advantage modules.

Within a single dashboard, you can combine insights from Attack Surface Management with relevant data from Threat Intelligence.

Watch a **recorded demo** (https://videos.mandiant.com/watch/Jg9eS8T98TrmKyScWDU5fe?) for more information.

Mandiant

September 2022 ASM Releases

API Functionality and Documentation Updates - September 15, 2022

The expanded ASM V1 API delivers more control over Projects, Collections, and Seeds. Take advantage of the new functionality; visit the **API Documentation** **(https://docs.mandiant.com/home/asm-api)** for more information.

Projects:

- Add, view, and delete

Collections:

- Add, refresh, and delete
- View associated integrations and history
- Archive and unarchive

Seeds:

- Add, view, and remove

Issues:

- Set status

Integrations:

- Add integrations
- Associate integrations to Collections

Searching for Answers - Where's the Tech? - September 8, 2022

Use the search function on the Entities page to answer questions about the breadth of technology used across the attack surface.

1. **Which entities rely on plugins, servers and frameworks?**
   Use the **Technology Label** to identify categories of technology identified around the ecosystem. Examples:
   - **Web Servers** **(https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology_labels%3Aweb_server)** - copy & paste **technology_labels:web_server**
   - **Web Frameworks** **(https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology_labels%3Aweb_framework)** - copy & paste **technology_labels:web_framework**
   - **Websites** **(https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology_labels%3Awebsite)**- copy & paste **technology_labels:website**
   - **Cache** **(https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology_labels%3Acache)** - copy & paste **technology_labels:cache**
   - **Wordpress Plugins** **(https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology_labels%3Awordpress_plugin)**- copy & paste **technology_labels:wordpress_plugin**
   - **Login Panels** **(https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology_labels%3Alogin_panel)** - copy & paste **technology_labels:login_panel**

2. **What is the impact of _____ application or service?**
   Use the **technology:vendor** query in the Entities search bar to identify the entities with a specific application or service. Examples:
   - **Apache** (https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology%3Aapache) - copy & paste **technology:apache**
   - **Nginx** (https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology%3Anginx) - copy & paste **technology:nginx**
   - **Cloudflare** (https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology%3Acloudflare) - copy & paste **technology:cloudflare**
   - **Heroku** (https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology%3Aheroku) - copy & paste **technology:heroku**
   - **Drupal** (https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology%3Adrupal)- copy & paste **technology:drupal**

Visit the **Technology Library** (https://asm.advantage.mandiant.com/library/technologies?search=&field=&value=) for the full list of vendors, labels, and more.

Searching for Answers - Meta Pixel Edition - September 1, 2022

A fingerprint for the Meta Pixel has been added to the **Technologies Library** (https://asm.advantage.mandiant.com/library/technologies?search=&field=&value=) to help customers identify if and where the pixel is used to track website visitor behavior or collect data. The fingerprint allows Attack Surface Management to determine when website pages have the pixel statically embedded. Currently, only the top-level URL or landing page is tested for the existence of this technology.

The default setup for the Meta Pixel collects user IP addresses, referring URLs, page views, button clicks, field names on forms, and more. Enabling Advanced Match or altering the default settings expands the data collection scope, increasing the risk of inadvertently sharing PII or PHI, in the case of healthcare organizations, with Meta.

Recommendation: Identify where the Meta Pixel is embedded, assess the classification of data collected, and restrict the pixel deployment to must-have website pages.

Use the search function on the Entities and Technologies pages to identify where a Meta Pixel is used around the attack surface. Currently, no Issue will be created.

Which Entities have the Meta Pixel?

- **Check out which Entities have the Meta Pixel** (https://asm.advantage.mandiant.com/entities?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20technology%3AMeta). Or,
- Copy & paste **technology:Meta** in the Entities search bar.

Does our organization use the Meta Pixel anywhere?

- **Find the pixel on the Technologies page** (https://asm.advantage.mandiant.com/technologies?table_view=false&search_string=last_seen_after%3Alast_refresh%20%20cpe%3A%22cpe%3A2.3%3Aa%3Ameta%3Apixel%3A%3A%2
  Or,
- Copy & paste **vendor:Meta** in the Technologies search bar.

August 2022 ASM Release

Mandiant

Integrate with Splunk through the Mandiant Advantage App - August 31, 2022

We're excited to announce the addition of Attack Surface Management (ASM) to the Mandiant Advantage App for Splunk.

Easy Entity and Issue Management

With customizable data pulls, Splunk customers can easily manage Entities and Issues directly within the Splunk Enterprise interface. The App uses the ASM API to provide control over the scope of data pulled:

- Project and Collection
- Issue Severity
- Timeframe (All time or Daily)
- Schedule an API query (Hourly or Daily)

Visit **Splunkbase (https://splunkbase.splunk.com/app/6128/#/overview)** to add the Mandiant Advantage App to your Splunk Enterprise Security instance. The step-by-step App configuration directions are available on the **Documentation Site (https://docs.mandiant.com/home/mandiant-advantage-for-splunk)**.

Mandiant Advantage Threat Intelligence, Digital Threat Monitoring, and Security Validation are also available through the App.

The legacy Intrigue Splunk integration will be deprecated by the end of November.

New Insights Reports - August 17, 2022

We're excited to announce two new **Insights Reports (https://asm.advantage.mandiant.com/insights)**:

1. Entities with the Most Inferred CVEs - Inferred CVEs are mapped based on the vendor, version, and technology fingerprints, where we have not actively tested for the vulnerability. Customers can quickly assess and prioritize investigating entities with inferred CVEs.
2. Top Prevalent Technology Labels - Identify the applications and services most used in your ecosystem.

We will continue to expand the reporting capabilities and welcome all customer feedback.

Even more visibility with our Akamai DNS Edge integration! - August 4, 2022

Akamai DNS Edge is the latest integration to date. By integrating with Akamai, we'll take your DNS associated with Akamai and give you even more visibility of your attack surface through our automated discovery engine.

Similar integrations are also available for Cloudflare and GoDaddy.

If you're a Project Owner, find and configure all your integrations **here (https://docs.mandiant.com/home/asm-integrations)**.

UX Enhancements - August 1, 2022

URI Entity Updates

- URI details are easier to view on the entity page
- Assess URI details without leaving the **Entities page (https://asm.advantage.mandiant.com/entities?table_view=true&search_string=%20type%3AUri%20last_seen_after%3Alast_refresh)** with the new table view pop-out. Click on the URI title to view.

Dozens of New Technology Fingerprints

FastApi, Flask, Sinatra, and more. See the **Technology Definitions Library (https://asm.advantage.mandiant.com/library/technologies?search=&field=&value=)** for more information.

July 2022 ASM Release

Auto-Discover DNS Records - GoDaddy Integration - July 28, 2022

Expand the scope of your Collection by auto-discovering Entities behind GoDaddy.

The new integration continuously ingests DNS records to improve attack surface visibility in situations where the GoDaddy account manages a substantial amount of DNS records.

You can find the new integration **here (https://asm.advantage.mandiant.com/account/settings/project/integrations)**.

Latest Checks - Atlassian Confluence, WSO2, and More - July 22, 2022

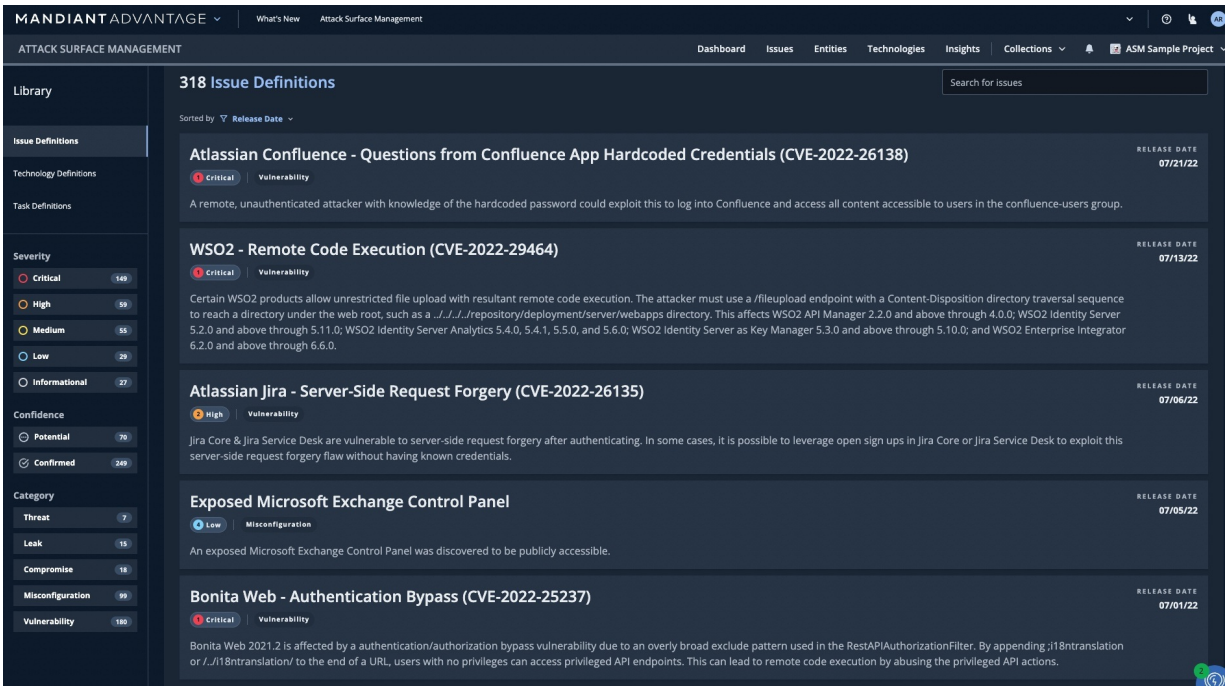
Checks are continuously added to the **Library (https://asm.advantage.mandiant.com/library/issues?search=&field=&value=)** to keep our customers informed about the latest vulnerabilities, misconfiguration, and exposures that impact external assets.

Notable Check:

 Atlassian Confluence - Questions from Confluence App Hardcoded Credentials (CVE-2022-26138)

See the latest:

- WSO2 - Remote Code Execution (CVE-2022-29464)
- Atlassian Jira - Server-Side Request Forgery (CVE-2022-26135)
- Exposed Microsoft Exchange Control Panel
- Bonita Web - Authentication Bypass (CVE-2022-25237)



Searching for Answers - 2FA Edition - July 15, 2022

Use the search function on the Entities page to answer questions about your external security posture.

1. **What application endpoints in my primary domain don't allow 2FA?**
   - **Check out your application endpoints not protected by 2FA (https://asm.advantage.mandiant.com/entities?table_view=false&search_string=%20http_auth_2fa%3Afalse%20last_seen_after%3Alast_refresh).** Or,
   - Copy & paste **http_auth_2fa:false** in the Entities search bar.

2. **What application endpoints in my primary domain allow 2FA?**
   - **Check out your application endpoints protected by 2FA (https://asm.advantage.mandiant.com/entities?table_view=false&search_string=%20http_auth_2fa%3Atrue%20last_seen_after%3Alast_refresh).** Or,
   - Copy & paste **http_auth_2fa:true** in the Entities search bar.

Reporting Insights Beta - July 7, 2022

Our initial round of Reporting Insights has been released for paid customers. Navigate over to the Insights tab to view them.

Reporting Insights Available:

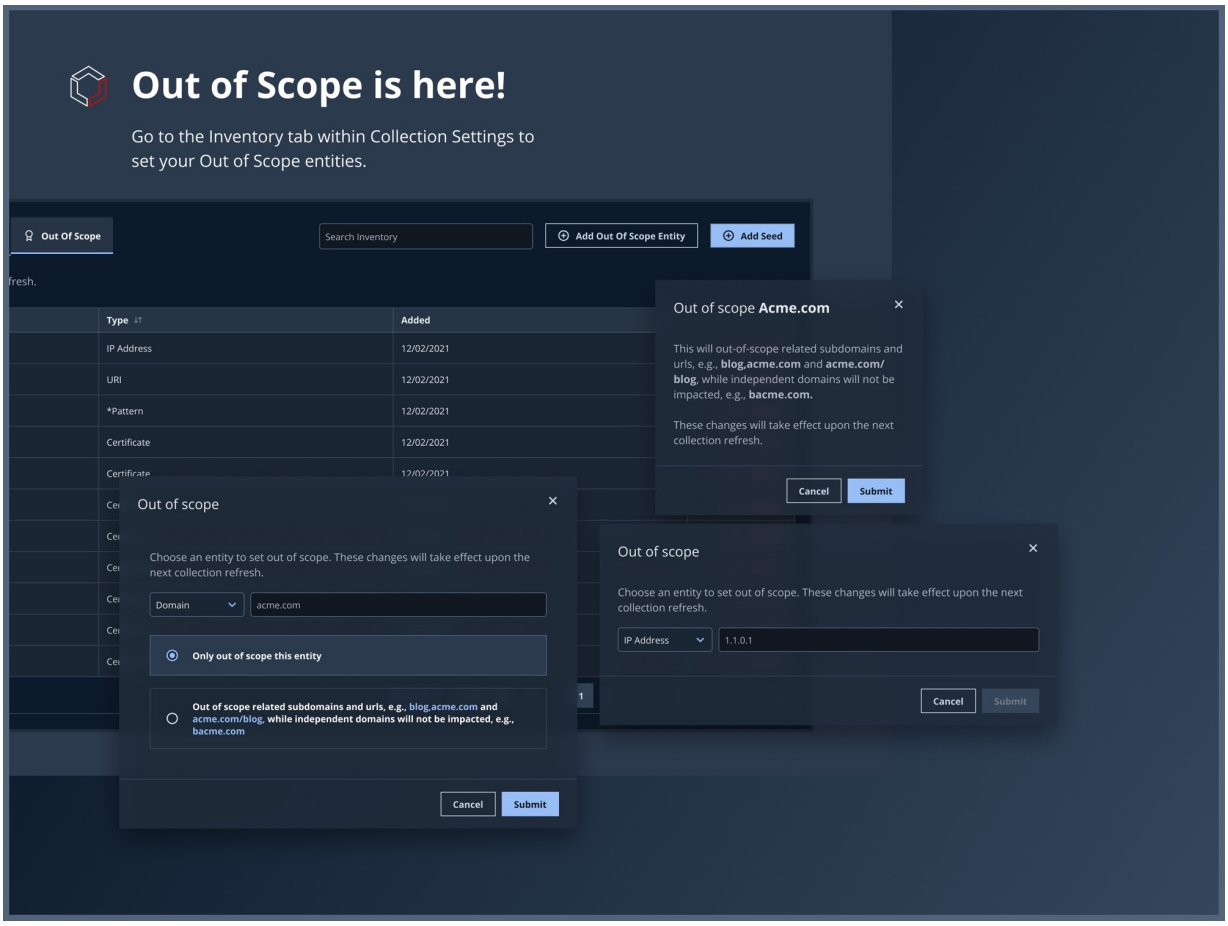
- Top 10 Most Severe Issues
- Top 10 Critical or High Issue Types by Prevalence
- Entities with the Most Issues

You can generate a formatted PDF of this information as well.

New charts and reports will be released on an ongoing basis. We know this is a priority for our customers and will make it a priority for us. All feedback, suggestions, and comments are welcome!

Much more to come.

Take Control of Collections with Out of Scope - July 5, 2022



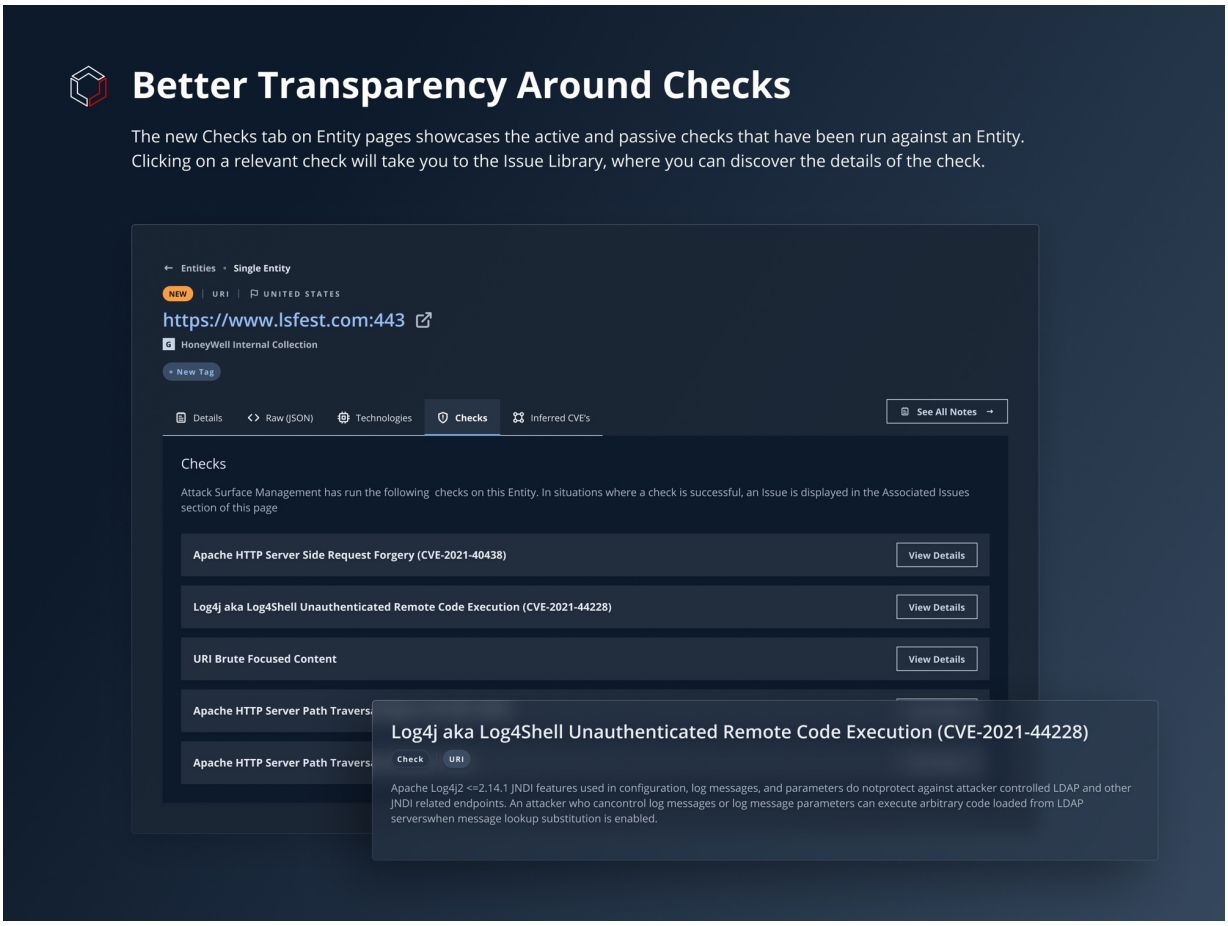
Take control of your entities when creating a Collection! You can now add out-of-scope Entities like domains, URLs, subdomains, IP addresses, and more to a Collection to ensure ASM does not scan them.

Navigate to your **Collection Settings -> Inventory -> Out of Scope.** If you see an Entity you'd like to scope out in your Entities view; you can set it out of scope directly on the page.

June 2022 ASM Release

Better Transparency Around Checks - June 30, 2022

The new Checks tab on Entity pages showcases the active and passive checks that have been run against an Entity. Clicking on a relevant check will take you to the Issue Library, where you can discover the details of the check.



Documentation Has a New Home - June 29, 2022

ICYMI: We launched a new **Mandiant Advantage Documentation Site (https://docs.mandiant.com/home/attack-surface-management)**! The new centralized location gives you a one-stop location for all Mandiant Advantage documentation.

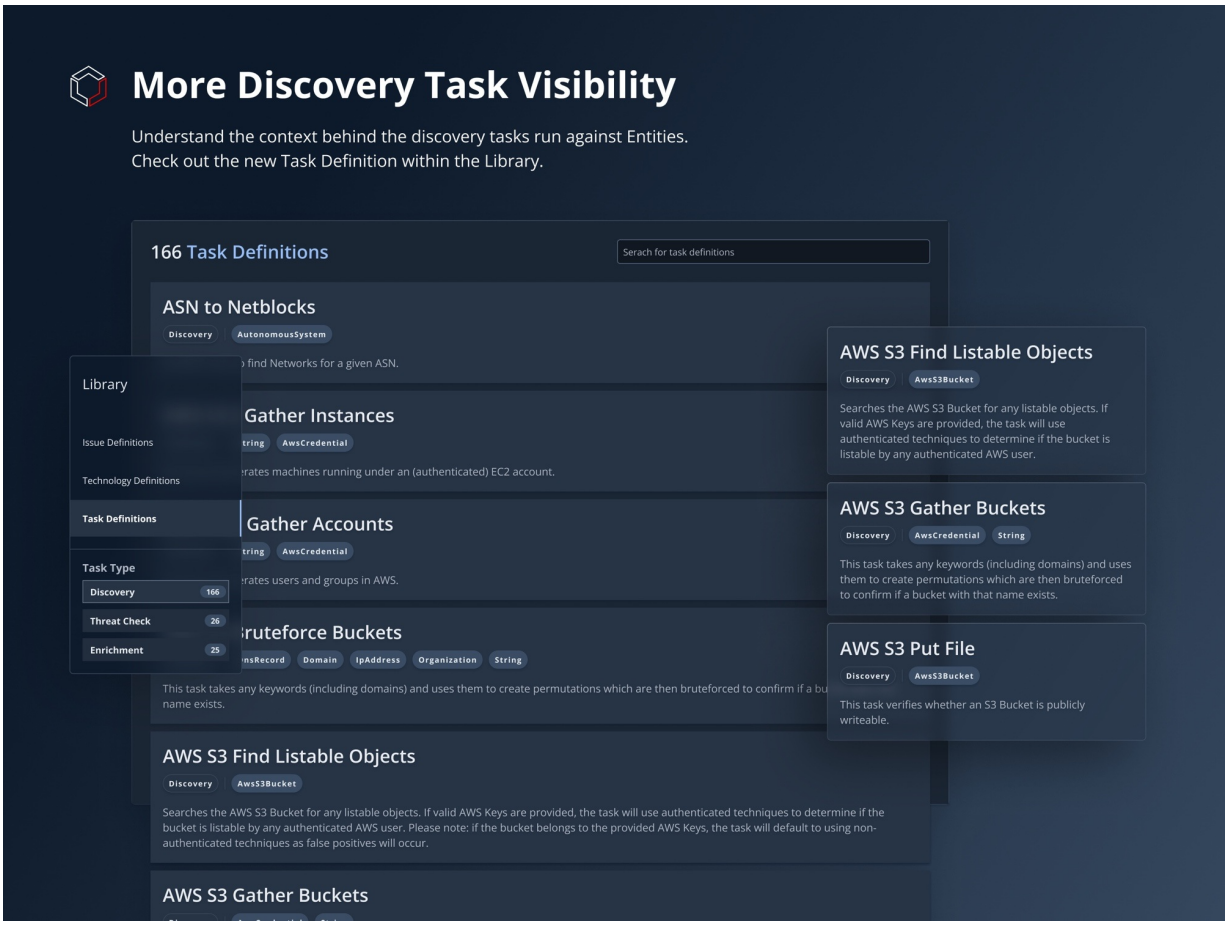
Azure Integration! - June 23, 2022

Use the token-based integration to auto-discover public Virtual Machine instances, storage accounts (blobs), and public DNS zones within your Azure accounts. Learn how to set up the integration **here (https://docs.mandiant.com/home/asm-azure-integration)**.

More Discovery Task Visibility - June 20, 2022

Understand the context behind the discovery tasks run against Entities. Check out the new Task Definition tab within the **Library (https://asm.advantage.mandiant.com/library/tasks)**.

Each definition is tagged with the associated Entities it runs against.



Expanded GitHub Integrations! - June 16, 2022

Adding GitHub accounts and repositories as Seeds within ASM just got easier. The new token-based integration creates Entity records for GitHub Accounts and Repositories, automatically populating them as Seeds into your Collection. Learn how to add GitHub to your Integrations page **here (https://docs.mandiant.com/home/asm-github-integration)**. After adding the integration, you can pull the GitHub Seeds into a Collection.

Enhanced SSL Issues - June 14, 2022

ASM now generates Misconfiguration Issues when deprecated SSL/TLS protocols or weak SSL/TLS ciphers are identified. These misconfigurations are common but are often overlooked, so we've made it easier for you to identify and prioritize them.

New Active Check for Atlassian Confluence (CVE-2022-26134) - June 4, 2022

Atlassian Confluence (CVE-2022-26134)

On June 2, 2022, information was publicly disclosed that malicious actors are exploiting vulnerability CVE-2022-26134, affecting Atlassian Confluence Server, prior to a patch becoming available.

Active Check

We're using a benign active check that will confirm if your Atlassian Confluence Server is vulnerable to CVE-2022-26134. The vulnerability check will send a payload that, when evaluated by a vulnerable target, will force the target to invoke a DNS Lookup, thus confirming successful (benign) exploitation. This active check will automatically run upon the next Collection Refresh. Mandiant recommends Confluence users put in place mitigations and detections as quickly as feasibly possible.

Recent UX Enhancements - June 3, 2022

Keep sharing feedback with the ASM product team; we're listening and continuously making improvements.

- Integrations are easier to add on the Collections page.
- The last refresh date is available on the Collections list, letting you know when each Collection was updated.
- Typosquats and CVEs can be copied with one click.
- Guiding tooltips are enhanced throughout the product.
- Minor visibility enhancements to the dashboard.

May 2022 ASM Release

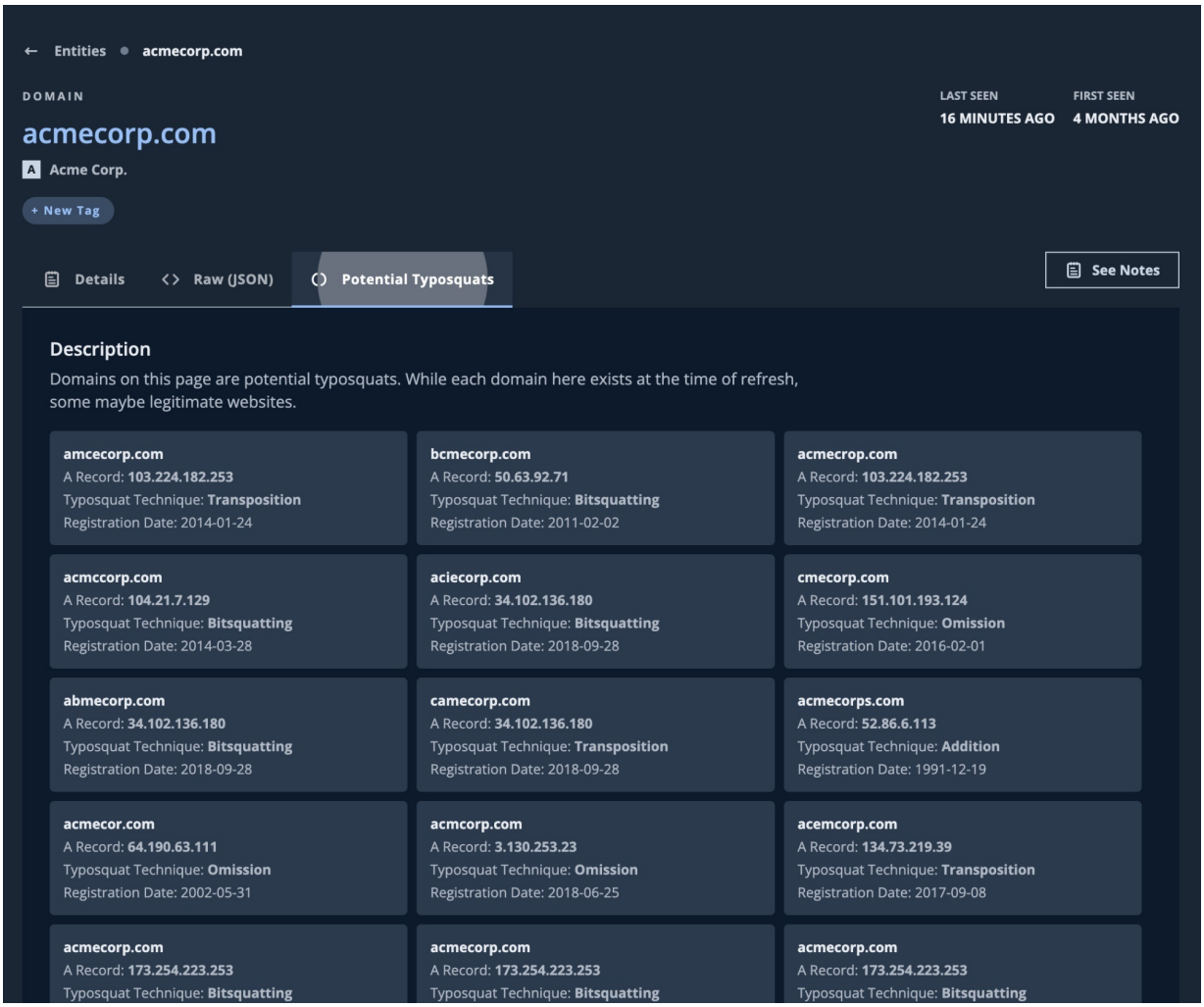
Cloudflare Integration! - May 3, 2022

- Pull in more data directly into your ASM account with better seeds.
- Our Cloudflare integration is designed to pull all DNS Records from zones where the Cloudflare API Key is authorized. The records pulled downstream are then created as entities based on their respective type.
- For example, A and AAAA records will create IP Address entities, and the associated name/label will create DNS Record entities.
- The new integration increases the quality of seeds in situations where the Cloudflare account manages a substantial amount of records.

April 2022 ASM Release

Better oversight on typosquats! - April 14, 2022

We pulled out Potential Typosquats into a separate tab within Domain Entity pages for easier access. No need to sort through the JSON to get an overview of suspicious domains.

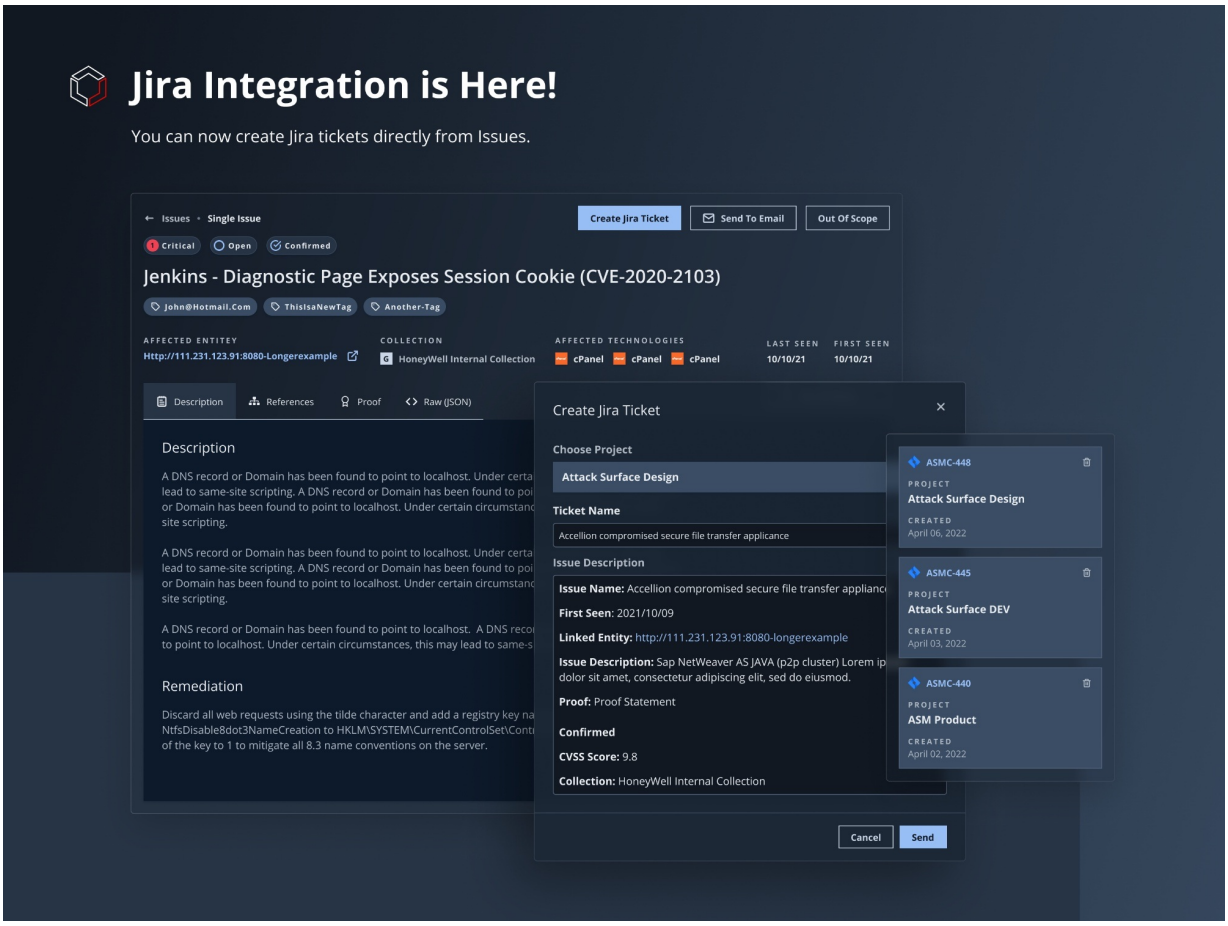


Jira Integration is Here! - April 13, 2022

You can now create Jira tickets directly from Issues. No copy & paste necessary; Issue details are pre-populated within the Jira ticket.

How it Works:

1. Enable the integration
2. View an Issue and click the Create Jira Ticket button
3. Choose a Jira Project
4. Send to Jira

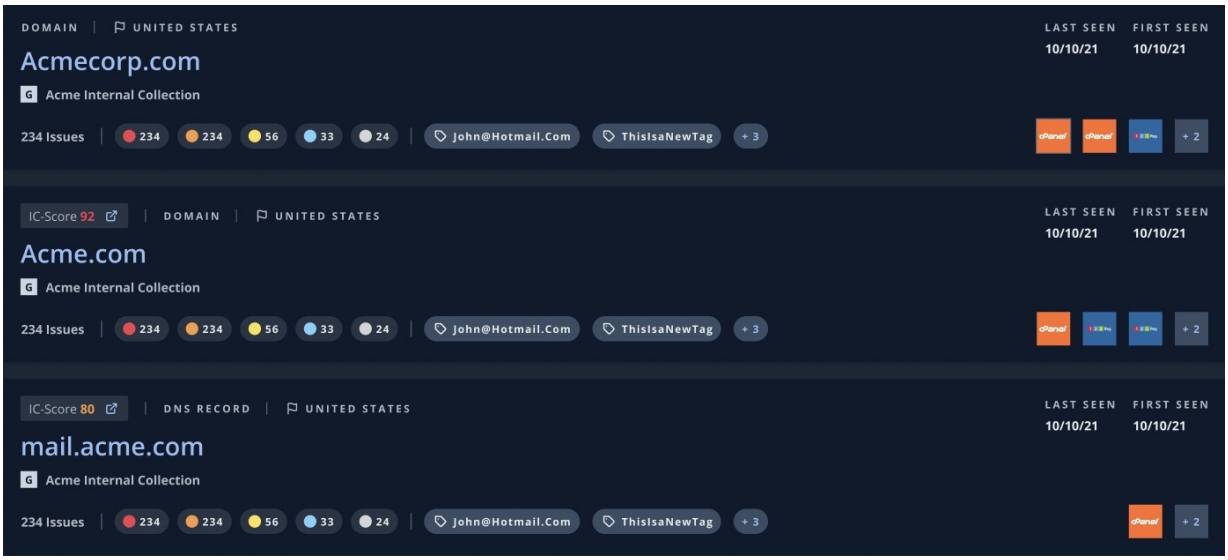


UX Updates & Enhancements - April 12, 2022

We heard your feedback and will continue to make incremental changes; please continue to share your feedback.

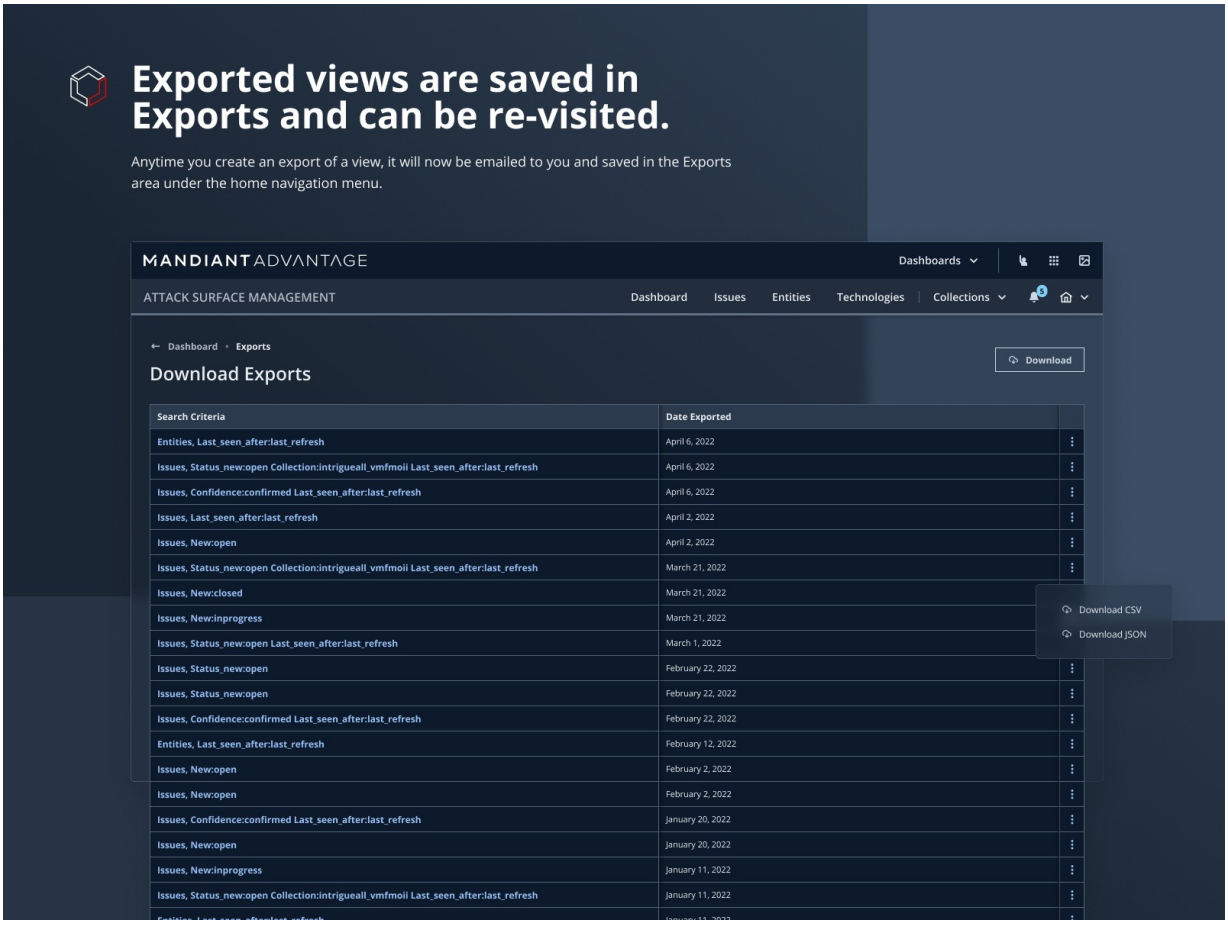
Updates:

1. The **Entities page (https://asm.advantage.mandiant.com/entities?table_view=true&search_string=type%3AUri%20last_seen_after%3Alast_refresh)** now includes technology cards on the respective entity.
2. Copy raw JSON to your clipboard with one click on Issues and Entities.
3. New team members can be invited directly to a Collection and are automatically invited to the Project.



Exported views are saved in Exports and can be re-visited - April 6, 2022

Anytime you create an export of a view, it will now be emailed to you and saved in the Exports area under the home navigation menu.



Sort your issues by Name - April 5, 2022

Now you can group issues that share the same name, consolidating issues into more consumable views.