Hacking, Computer Hacking and Security Testing

- Microsoft Defender EASM

Sanna Diana Tomren

Accenture | LinkedIn: Sanna Diana Tomren

MVP Dagen

Hacking, Computer Hacking and Security Testing

- Definere hacking
- Computer hacking
- Sikkerhetstesting
- Fysisk og digital sikkerhetstesting
- Microsoft Teknologi

Takk til våre sponsorer

Microsoft
audiocodes
glasspaper
POINT:TAKEN
EPOS
aztek
Evidi
KPMG
CloudWay
spirhed
Noroff
School of technology
and digital media
blinQ
amesto
Fortytwo
SparebankenVest
IT styring
INNOFACTOR

Takk til vår by-sponsor

Sanna Diana Tomren

Associate Manager, Accenture

- Cloud Security Lead
- Kunnskapsdeler
- Microsoft MVP 2022 – Security
- Microsoft Security User Group Founder and organizer

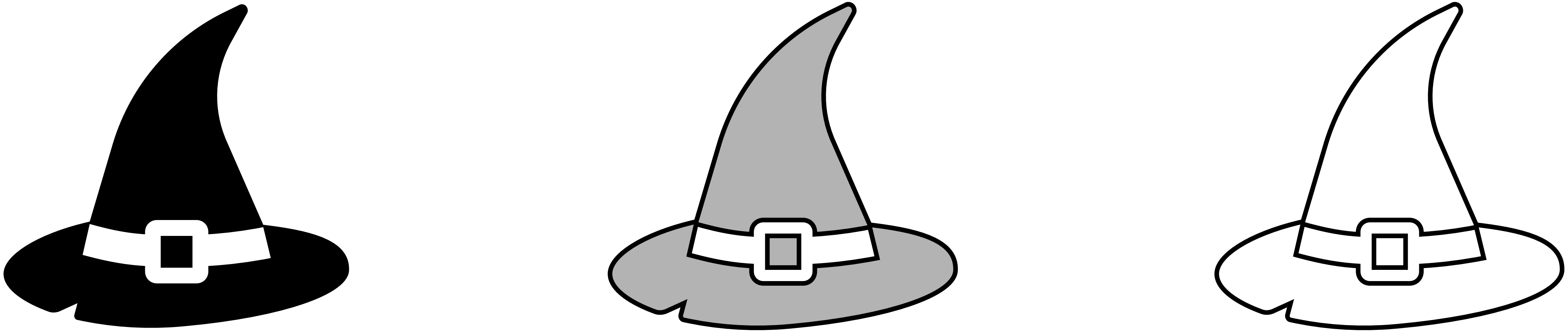
Hacking – Life hack

Hacking - benytte verktøy, teknologi og kunnskap

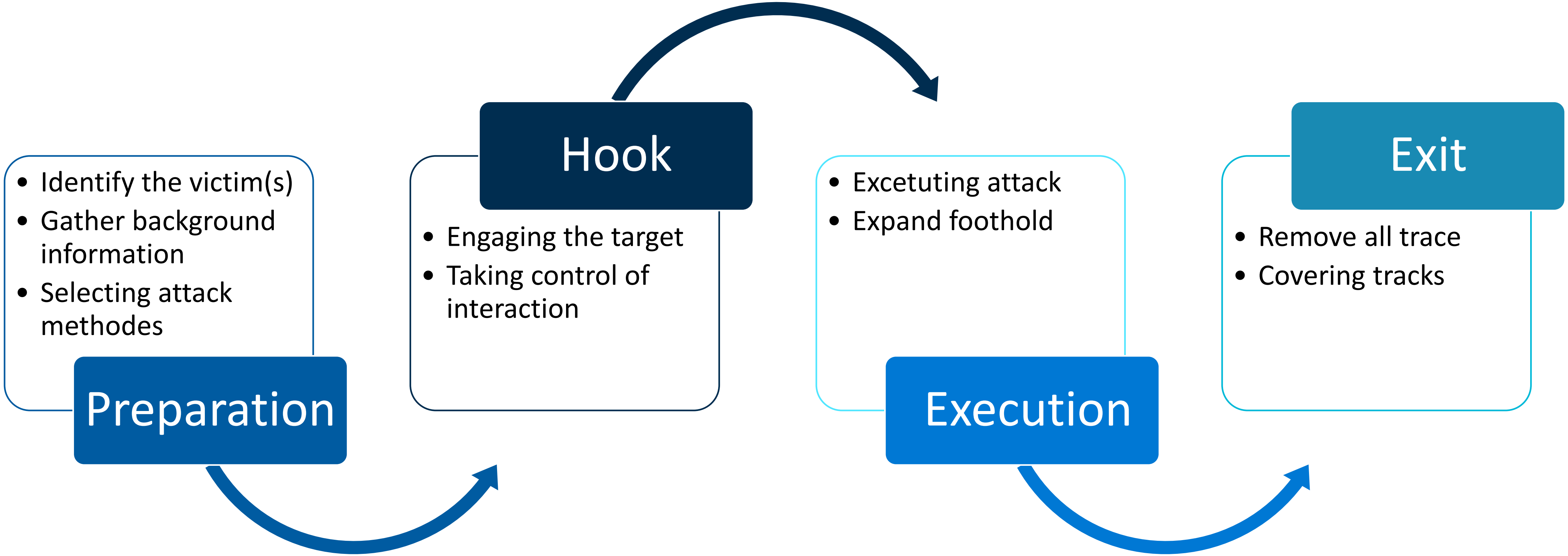
Computer hacking

«The act of compromising digital devices and networks through unauthorized access to an account or computer system» - Fortinet

Magikerne



Livssyklus



Preparation

- Identify the victim(s)
- Gather background information
- Selecting attack methodes

Hook

- Engaging the target
- Taking control of interaction

Execution

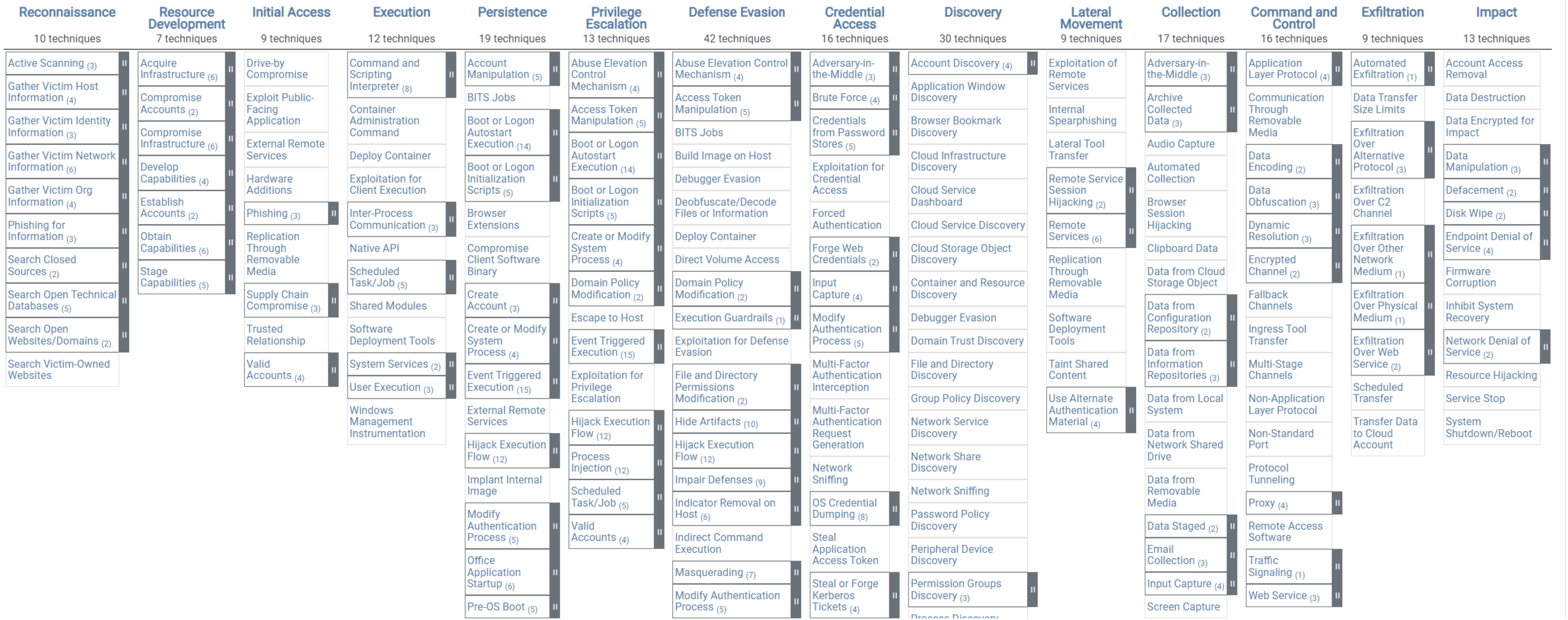
- Excetuting attack
- Expand foothold

Exit

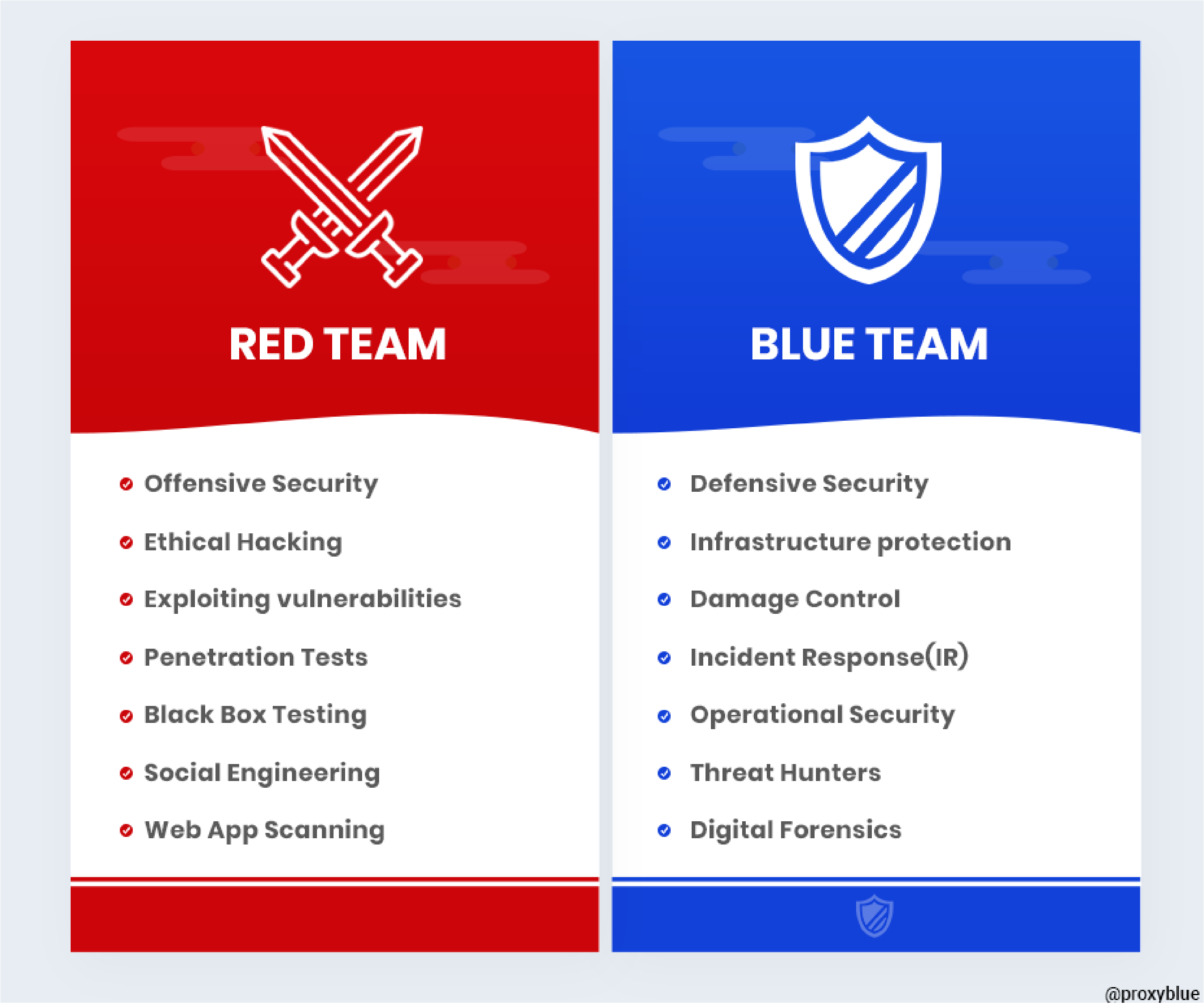
- Remove all trace
- Covering tracks

Fysisk og digital sikkerhetstesting

Mitre Attack rammeverk



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (3)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Direct Volume Access	Modify Authentication Process (5)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	OS Credential Dumping (8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process (5)	Valid Accounts (4)	Hide Artifacts (10)	Steal Application Access Token	Network Service Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Hijack Execution Flow (12)	Steal or Forge Kerberos Tickets (4)	Network Share Discovery		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Impair Defenses (9)		Network Sniffing		Input Capture (4)	Traffic Signaling (1)		
						Indicator Removal on Host (6)		Password Policy Discovery		Screen Capture	Web Service (3)		
						Indirect Command Execution		Peripheral Device Discovery					
						Masquerading (7)		Permission Groups Discovery (3)					
						Modify Authentication Process (5)		Process Discovery					



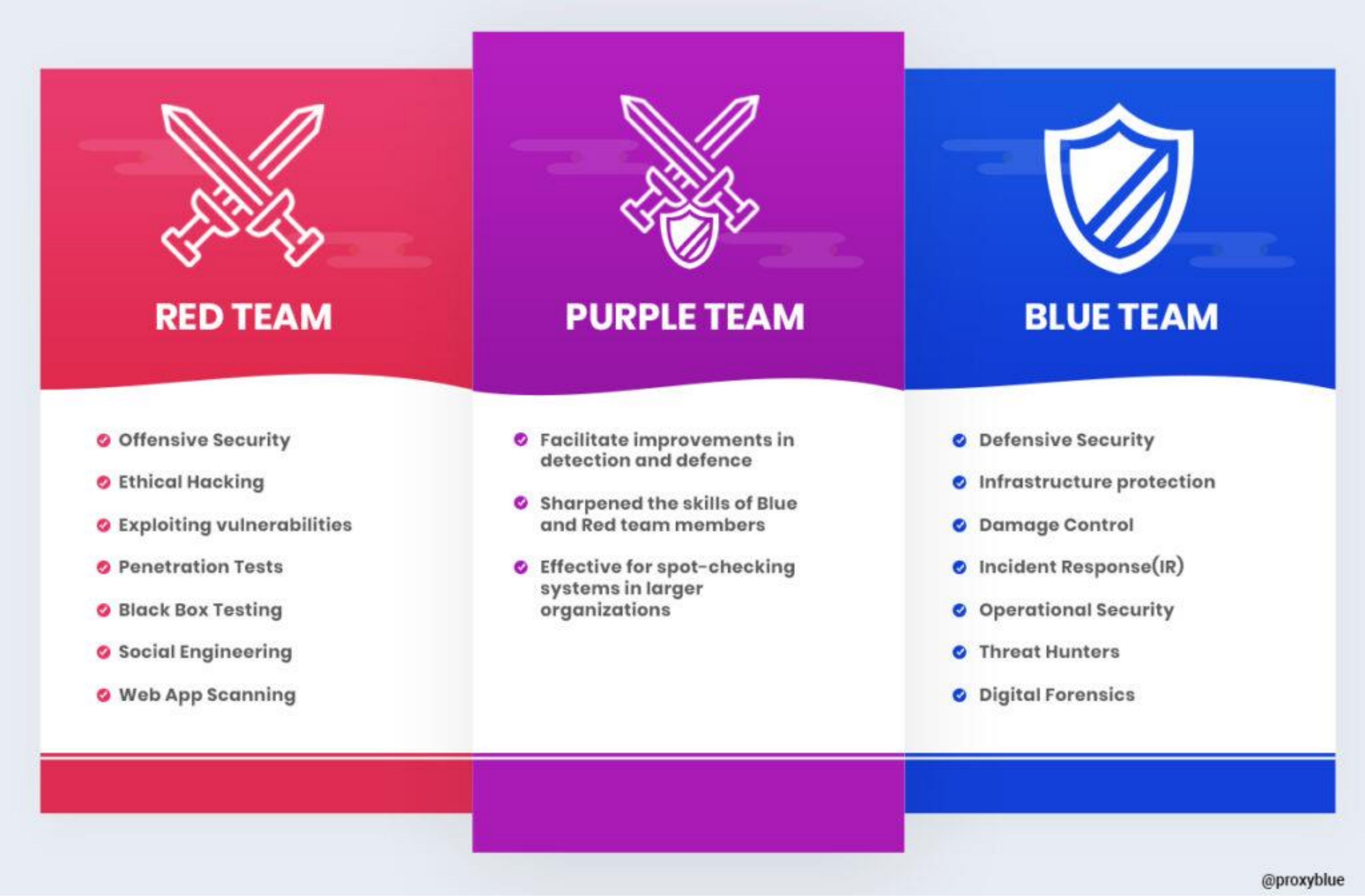
RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

@proxyblue



RED TEAM

- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

PURPLE TEAM

- Facilitate improvements in detection and defence
- Sharpened the skills of Blue and Red team members
- Effective for spot-checking systems in larger organizations

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

@proxyblue

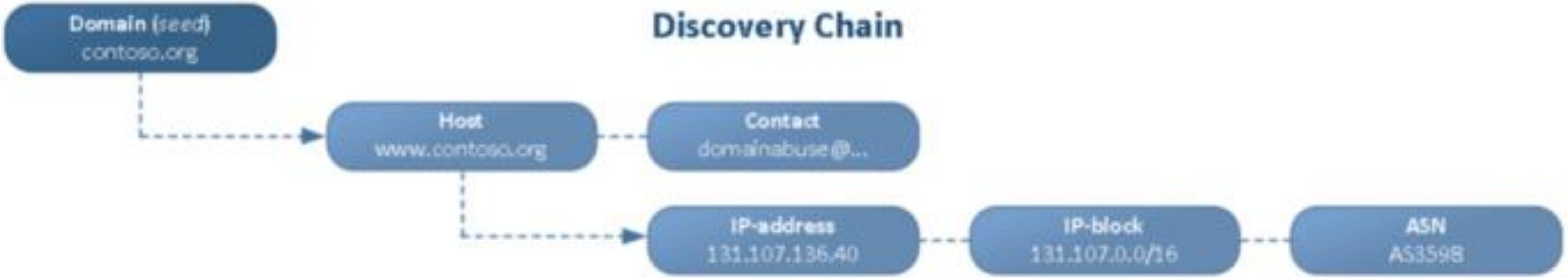
Microsoft Azure

Microsoft Defender External Attack Surface Management (Defender EASM)

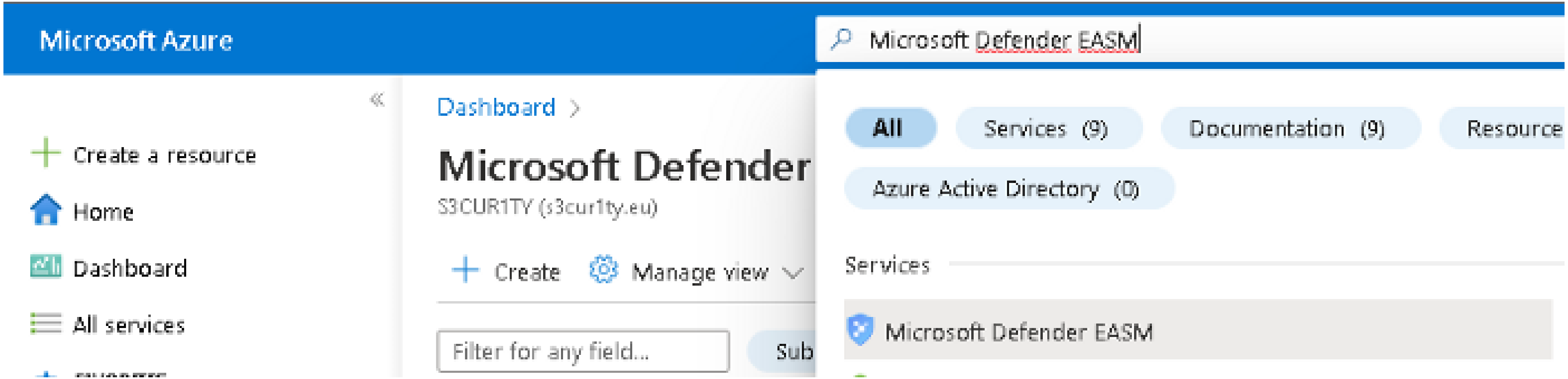
Azure Sentinel (SIEM & SOAR)

Microsoft Defender for Cloud (CSPM & CWPP)

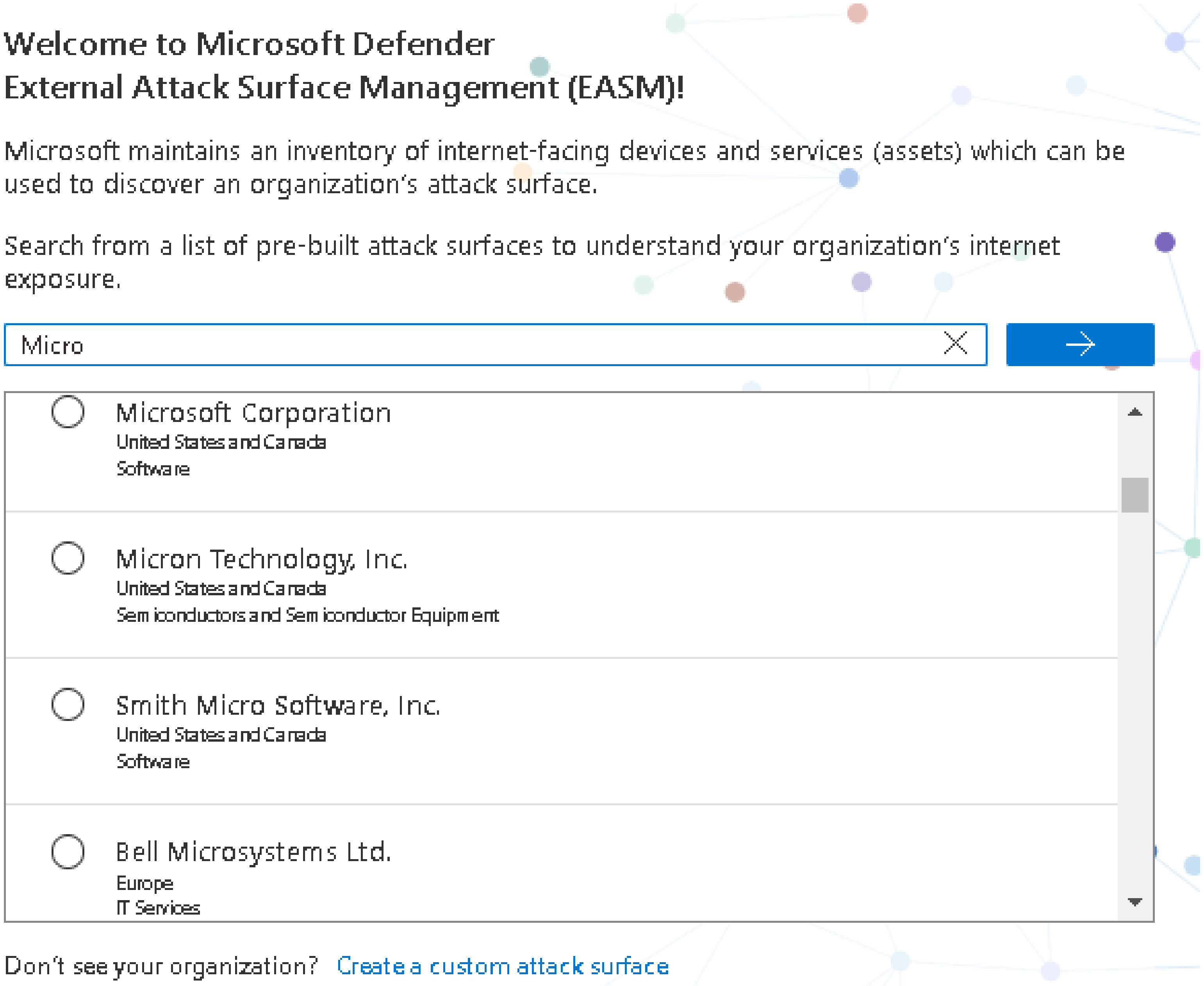
Defender EASM



Discovery Chain



Microsoft Defender EASM



Welcome to Microsoft Defender External Attack Surface Management (EASM)!

Microsoft maintains an inventory of internet-facing devices and services (assets) which can be used to discover an organization's attack surface.

Search from a list of pre-built attack surfaces to understand your organization's internet exposure.

Micro

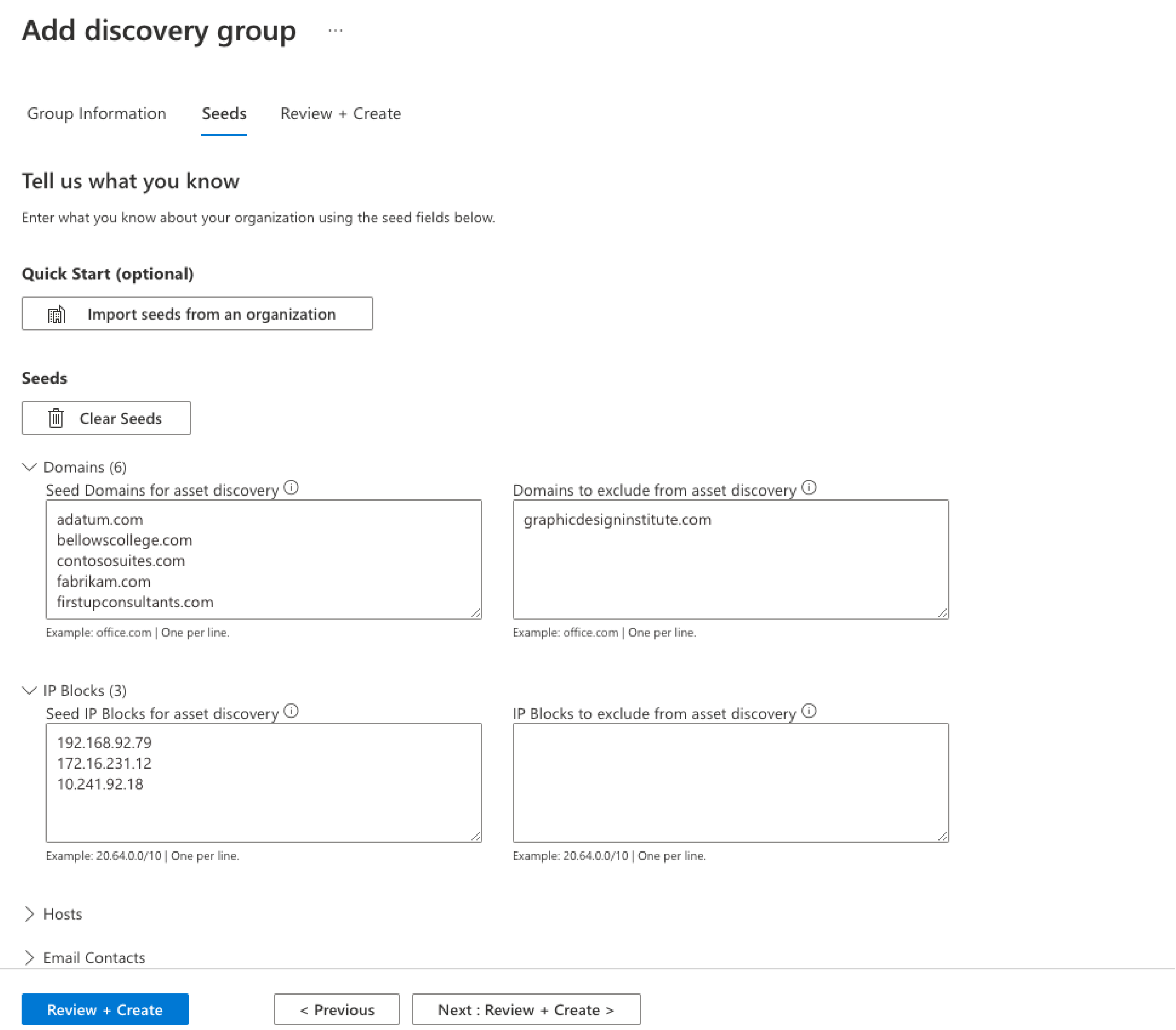
○ Microsoft Corporation
United States and Canada
Software

○ Micron Technology, Inc.
United States and Canada
Semiconductors and Semiconductor Equipment

○ Smith Micro Software, Inc.
United States and Canada
Software

○ Bell Microsystems Ltd.
Europe
IT Services

Don't see your organization? Create a custom attack surface



Add discovery group ···

Tell us what you know

Enter what you know about your organization using the seed fields below.

Quick Start (optional)

Seeds

Domains (6)

Seed Domains for asset discovery ⓘ

adatum.com
bellowscollege.com
contososuites.com
fabrikam.com
firstupconsultants.com

Example: office.com | One per line.

Domains to exclude from asset discovery ⓘ

graphicdesigninstitute.com

Example: office.com | One per line.

IP Blocks (3)

Seed IP Blocks for asset discovery ⓘ

192.168.92.79
172.16.231.12
10.241.92.18

Example: 20.64.0.0/10 | One per line.

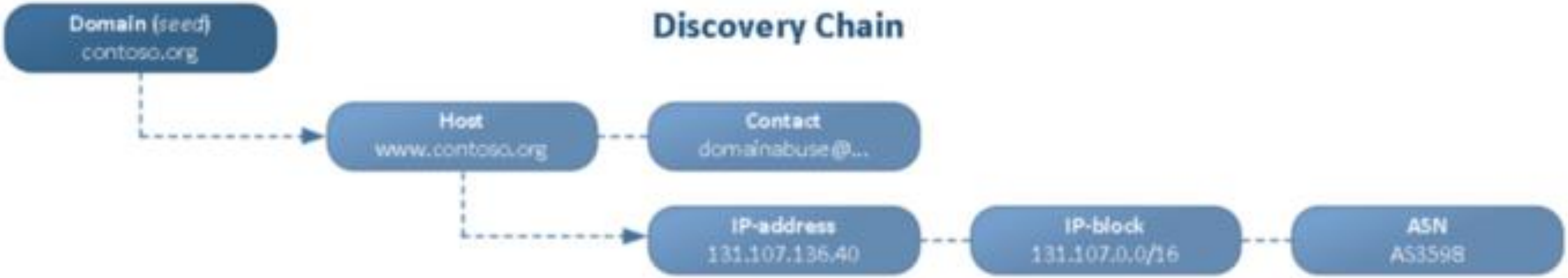
IP Blocks to exclude from asset discovery ⓘ

Example: 20.64.0.0/10 | One per line.

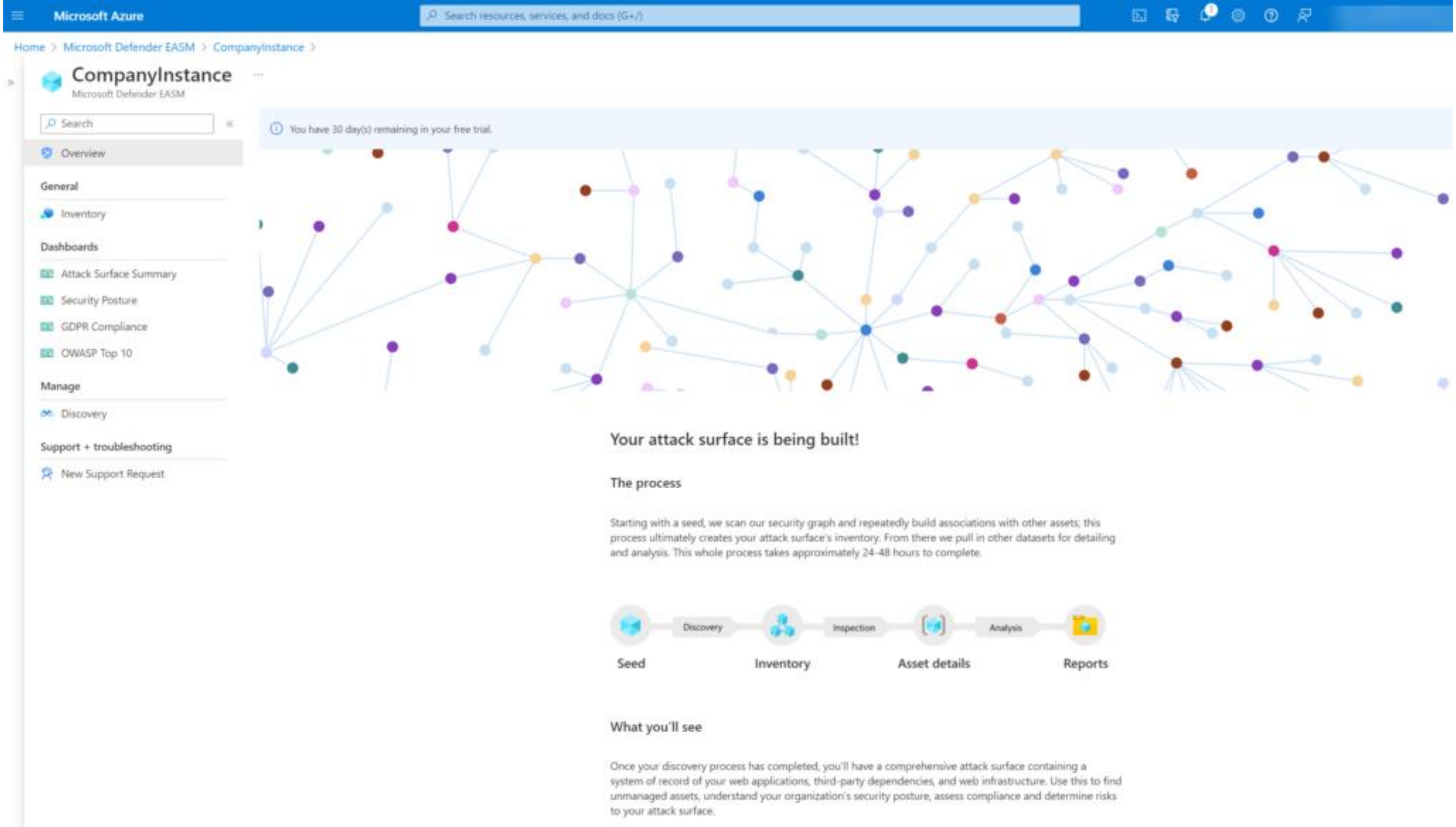
› Hosts

› Email Contacts

MVP-Dagen



Discovery Chain



You have 30 day(s) remaining in your free trial.

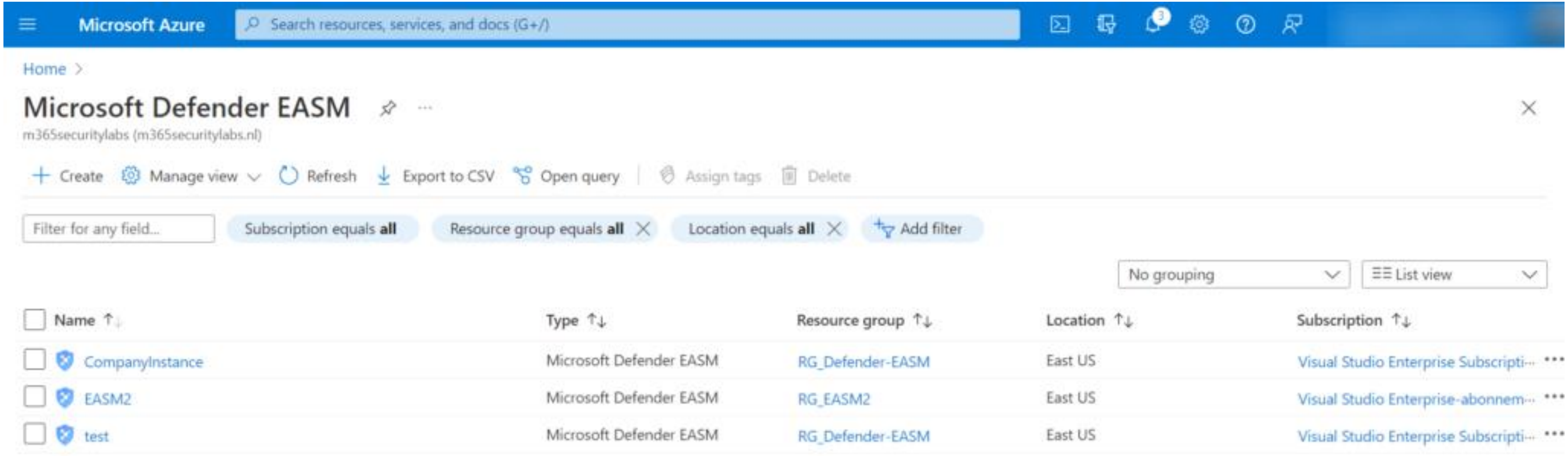
Your attack surface is being built!

The process

Starting with a seed, we scan our security graph and repeatedly build associations with other assets; this process ultimately creates your attack surface's inventory. From there we pull in other datasets for detailing and analysis. This whole process takes approximately 24-48 hours to complete.

What you'll see

Once your discovery process has completed, you'll have a comprehensive attack surface containing a system of record of your web applications, third-party dependencies, and web infrastructure. Use this to find unmanaged assets, understand your organization's security posture, assess compliance and determine risks to your attack surface.



Microsoft Defender EASM

m365securitylabs (m365securitylabs.nl)

Filter for any field...

Subscription equals **all**

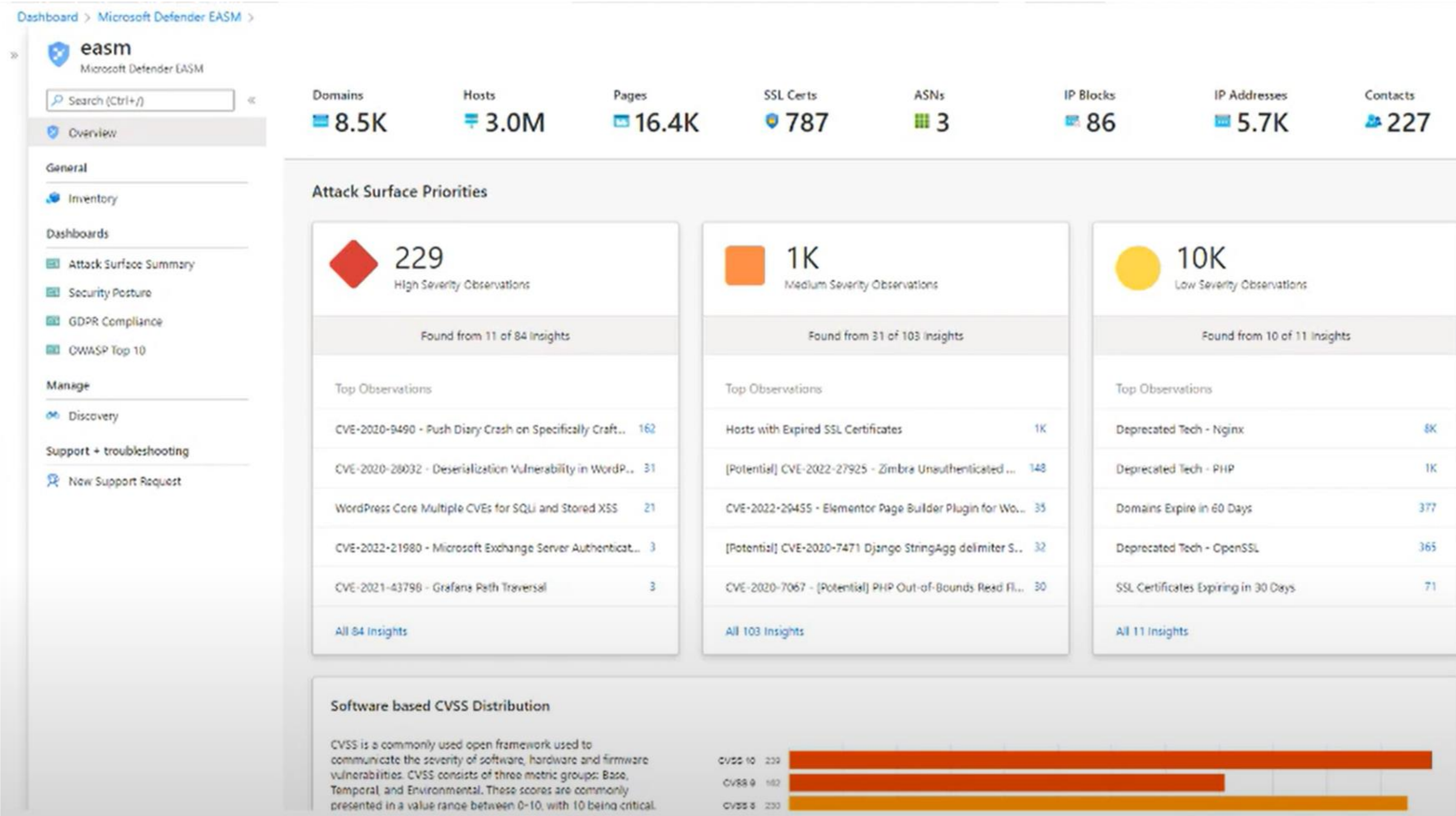
Resource group equals **all**

Location equals **all**

No grouping

List view

Name	Type	Resource group	Location	Subscription
CompanyInstance	Microsoft Defender EASM	RG_Defender-EASM	East US	Visual Studio Enterprise Subscripti...
EASM2	Microsoft Defender EASM	RG_EASM2	East US	Visual Studio Enterprise-abonnem...
test	Microsoft Defender EASM	RG_Defender-EASM	East US	Visual Studio Enterprise Subscripti...



Domains	Hosts	Pages	SSL Certs	ASNs	IP Blocks	IP Addresses	Contacts
8.5K	3.0M	16.4K	787	3	86	5.7K	227

Attack Surface Priorities

229 High Severity Observations

Found from 11 of 84 Insights

Top Observations	
CVE-2020-9490 - Push Diary Crash on Specifically Craft...	162
CVE-2020-28032 - Deserialization Vulnerability in WordP...	31
WordPress Core Multiple CVEs for SQLi and Stored XSS	21
CVE-2022-21980 - Microsoft Exchange Server Authenticat...	3
CVE-2021-43798 - Grafana Path Traversal	3

All 84 Insights

1K Medium Severity Observations

Found from 31 of 103 Insights

Top Observations	
Hosts with Expired SSL Certificates	1K
[Potential] CVE-2022-27925 - Zimbra Unauthenticated ...	148
CVE-2022-29455 - Elementor Page Builder Plugin for Wo...	35
[Potential] CVE-2020-7471 Django StringAgg delimiter S...	32
CVE-2020-7067 - [Potential] PHP Out-of-Bounds Read Fl...	30

All 103 Insights

10K Low Severity Observations

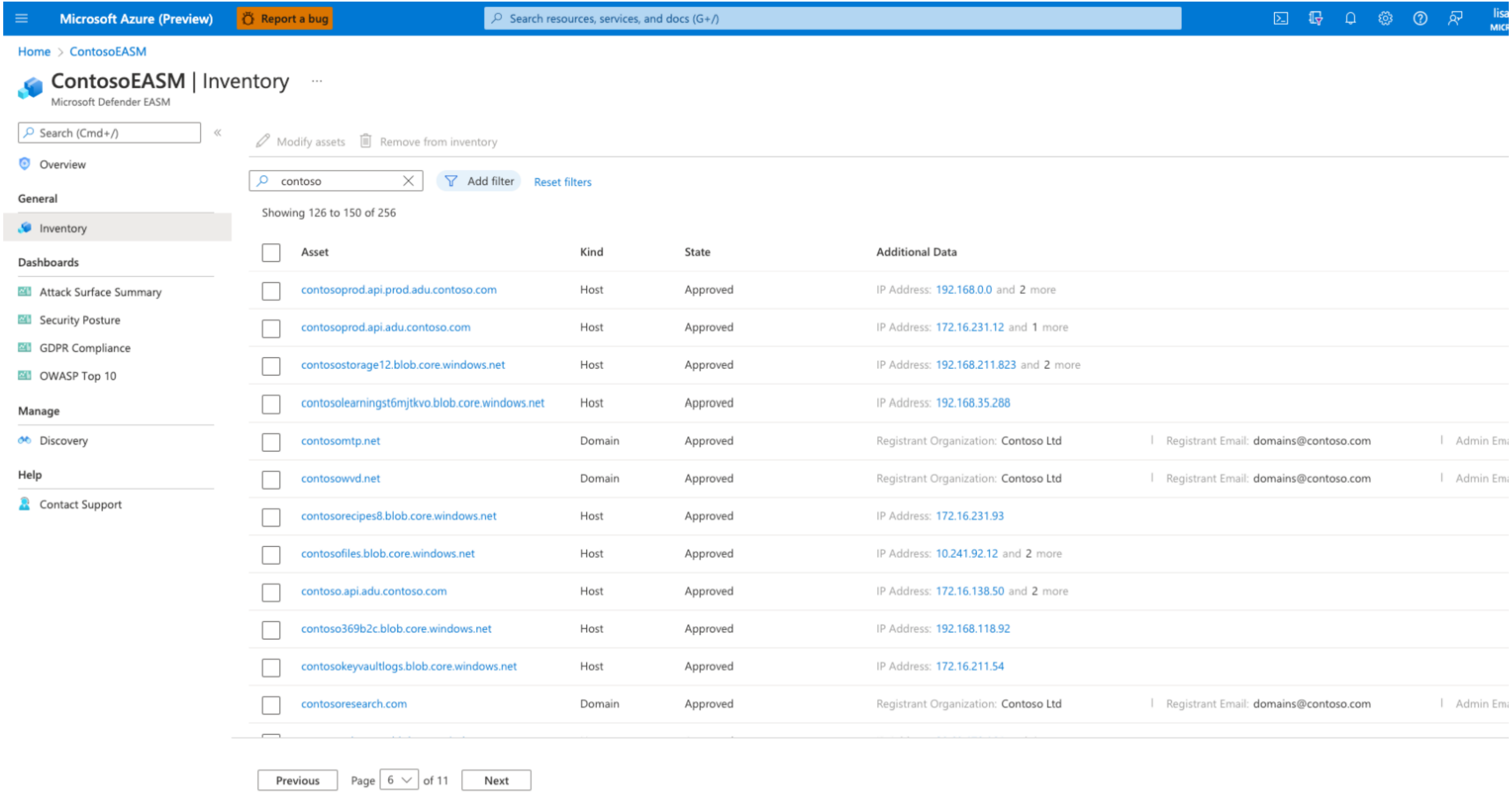
Found from 10 of 11 Insights

Top Observations	
Deprecated Tech - Nginx	8K
Deprecated Tech - PHP	1K
Domains Expire in 60 Days	377
Deprecated Tech - OpenSSL	365
SSL Certificates Expiring in 30 Days	71

All 11 Insights

Software based CVSS Distribution

CVSS is a commonly used open framework used to communicate the severity of software, hardware and firmware vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. These scores are commonly presented in a value range between 0-10, with 10 being critical.



Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
Home > ContosoEASM

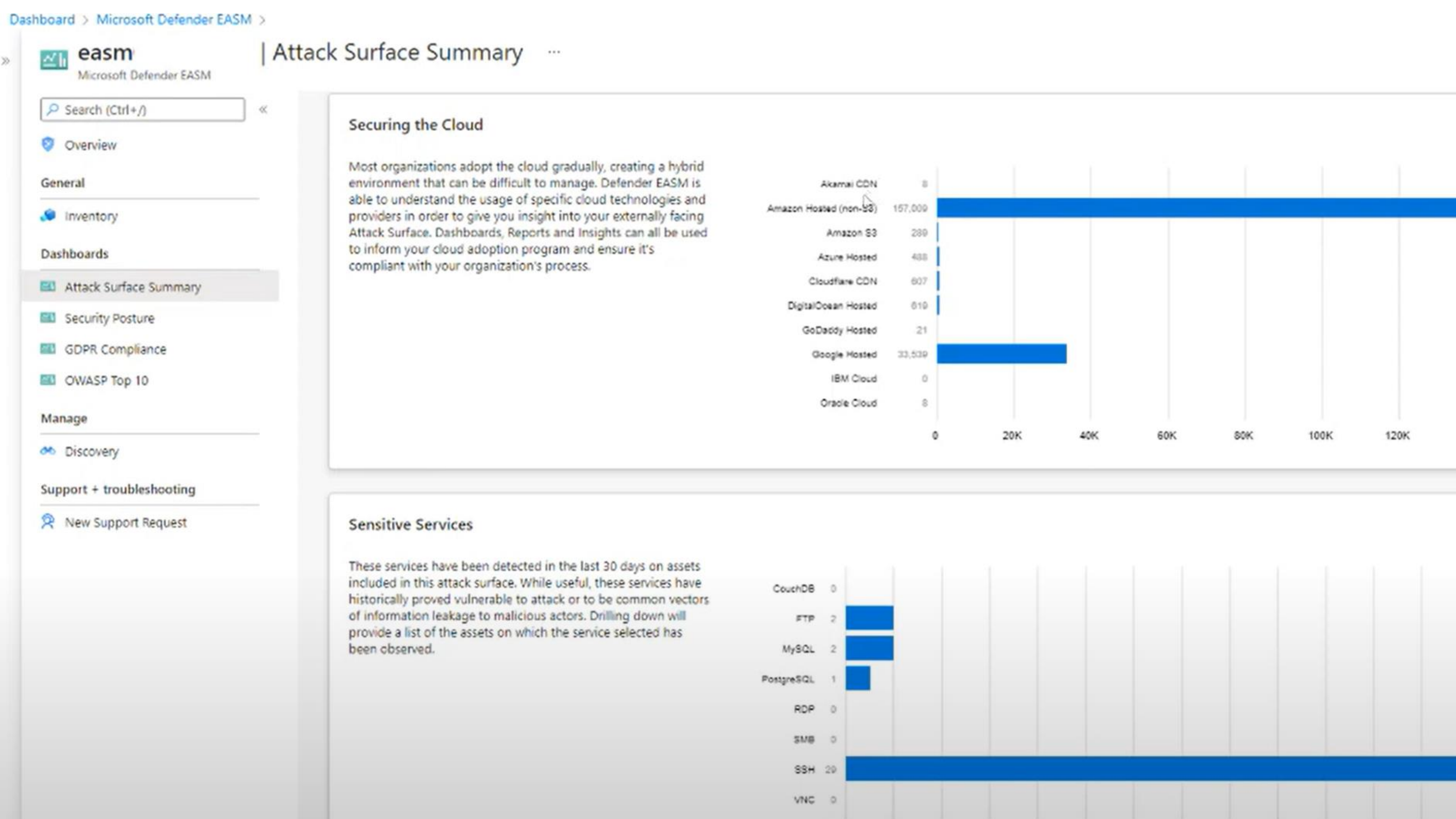
ContosoEASM | Inventory

Microsoft Defender EASM

Search: contoso

Showing 126 to 150 of 256

□	Asset	Kind	State	Additional Data
□	contosoprod.api.prod.adu.contoso.com	Host	Approved	IP Address: 192.168.0.0 and 2 more
□	contosoprod.api.adu.contoso.com	Host	Approved	IP Address: 172.16.231.12 and 1 more
□	contosostorage12.blob.core.windows.net	Host	Approved	IP Address: 192.168.211.823 and 2 more
□	contosolearningst6mjtkvo.blob.core.windows.net	Host	Approved	IP Address: 192.168.35.288
□	contosomtp.net	Domain	Approved	Registrant Organization: Contoso Ltd | Registrant Email: domains@contoso.com | Admin Em
□	contosowvd.net	Domain	Approved	Registrant Organization: Contoso Ltd | Registrant Email: domains@contoso.com | Admin Em
□	contosorecipes8.blob.core.windows.net	Host	Approved	IP Address: 172.16.231.93
□	contosofiles.blob.core.windows.net	Host	Approved	IP Address: 10.241.92.12 and 2 more
□	contoso.api.adu.contoso.com	Host	Approved	IP Address: 172.16.138.50 and 2 more
□	contoso369b2c.blob.core.windows.net	Host	Approved	IP Address: 192.168.118.92
□	contosokeyvaultlogs.blob.core.windows.net	Host	Approved	IP Address: 172.16.211.54
□	contosoresearch.com	Domain	Approved	Registrant Organization: Contoso Ltd | Registrant Email: domains@contoso.com | Admin Em



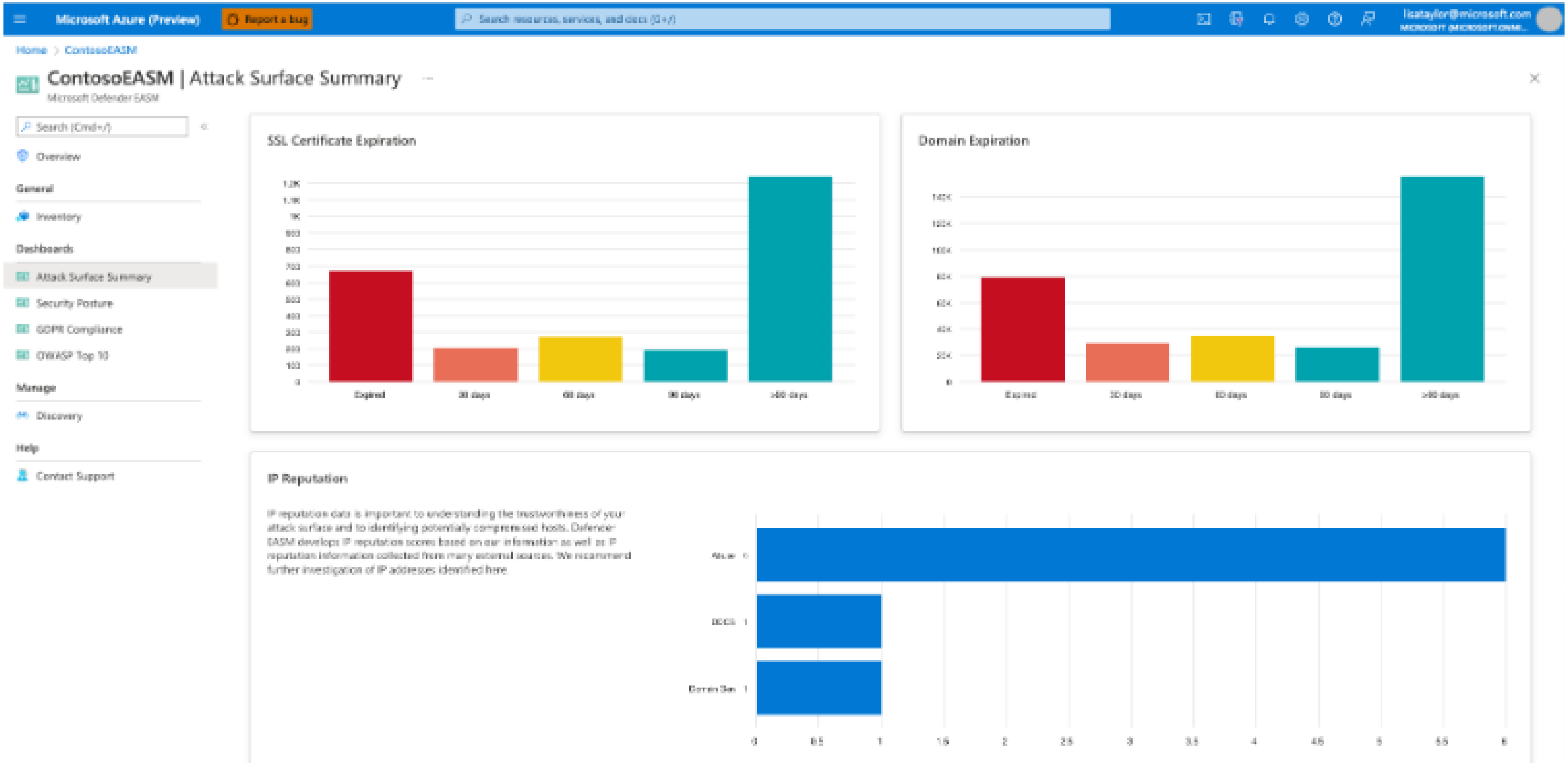
| Attack Surface Summary

Securing the Cloud

Most organizations adopt the cloud gradually, creating a hybrid environment that can be difficult to manage. Defender EASM is able to understand the usage of specific cloud technologies and providers in order to give you insight into your externally facing Attack Surface. Dashboards, Reports and Insights can all be used to inform your cloud adoption program and ensure it's compliant with your organization's process.

Sensitive Services

These services have been detected in the last 30 days on assets included in this attack surface. While useful, these services have historically proved vulnerable to attack or to be common vectors of information leakage to malicious actors. Drilling down will provide a list of the assets on which the service selected has been observed.



ContosoEASM | Attack Surface Summary

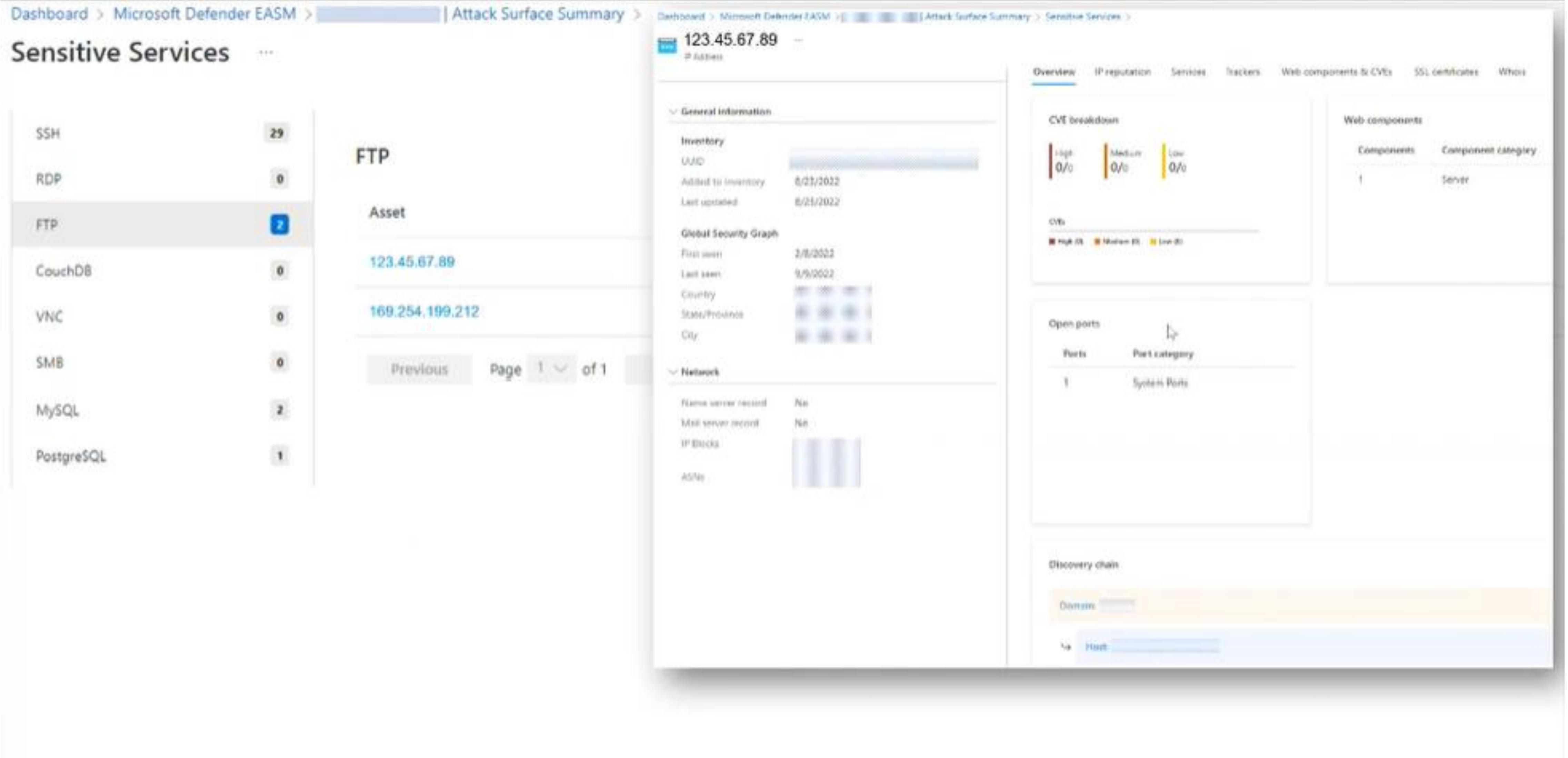
Microsoft Defender EASM

SSL Certificate Expiration

Domain Expiration

IP Reputation

IP reputation data is important to understanding the trustworthiness of your attack surface and to identifying potentially compromised hosts. Defender EASM develops IP reputation scores based on our information as well as IP reputation information collected from many external sources. We recommend further investigation of IP addresses identified here.



Dashboard > Microsoft Defender EASM > [redacted] | Attack Surface Summary >

Sensitive Services

SSH	29
RDP	0
FTP	2
CouchDB	0
VNC	0
SMB	0
MySQL	2
PostgreSQL	1

FTP

Asset
123.45.67.89
169.254.199.212

Previous   Page 1 of 1

Dashboard > Microsoft Defender EASM > [redacted] | Attack Surface Summary > Sensitive Services >

123.45.67.89
IP Address

Overview | IP reputation | Services | Trackers | Web components & CVEs | SSL certificates | Whois

General information

Inventory

UUID	[redacted]
Added to inventory	8/23/2022
Last updated	8/23/2022

Global Security Graph

First seen	2/8/2022
Last seen	9/9/2022
Country	[redacted]
State/Province	[redacted]
City	[redacted]

Network

Name server record	No
Mail server record	No
IP Blocks	[redacted]
ASNs	[redacted]

CVE breakdown

High 0/0   Medium 0/0   Low 0/0

CVEs

■ High (0)   ■ Medium (0)   ■ Low (0)

Web components

Components	Component category
1	Server

Open ports

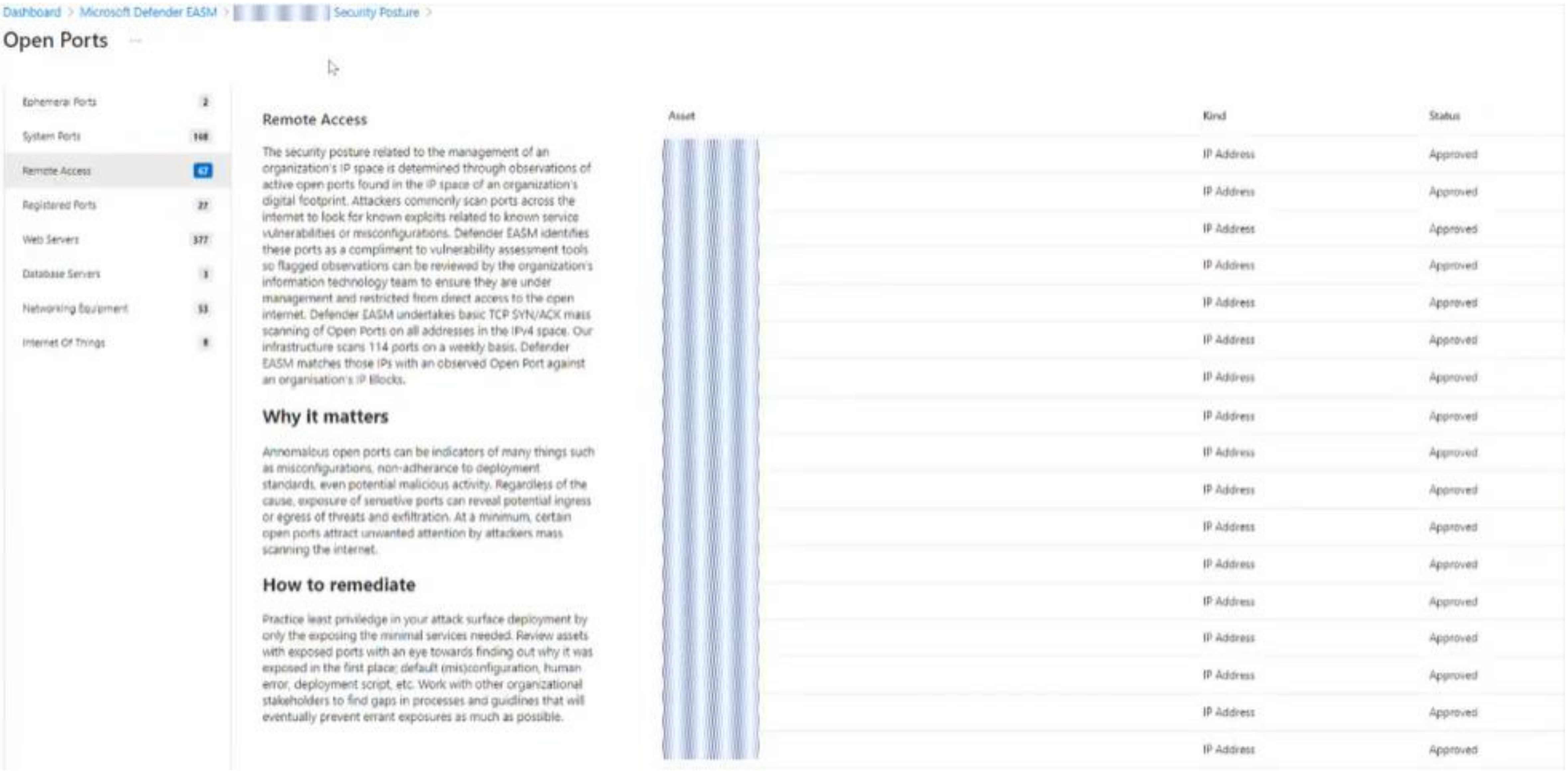
Ports	Port category
1	System Ports

Discovery chain

Domain [redacted]

↳ Host [redacted]

MVP-Dagen



Dashboard > Microsoft Defender EASM > [redacted] Security Posture >

Open Ports

Ephemeral Ports	2
System Ports	168
Remote Access	67
Registered Ports	27
Web Servers	377
Database Servers	1
Networking Equipment	53
Internet Of Things	8

Remote Access

The security posture related to the management of an organization's IP space is determined through observations of active open ports found in the IP space of an organization's digital footprint. Attackers commonly scan ports across the internet to look for known exploits related to known service vulnerabilities or misconfigurations. Defender EASM identifies these ports as a compliment to vulnerability assessment tools so flagged observations can be reviewed by the organization's information technology team to ensure they are under management and restricted from direct access to the open internet. Defender EASM undertakes basic TCP SYN/ACK mass scanning of Open Ports on all addresses in the IPv4 space. Our infrastructure scans 114 ports on a weekly basis. Defender EASM matches those IPs with an observed Open Port against an organisation's IP Blocks.

Why it matters

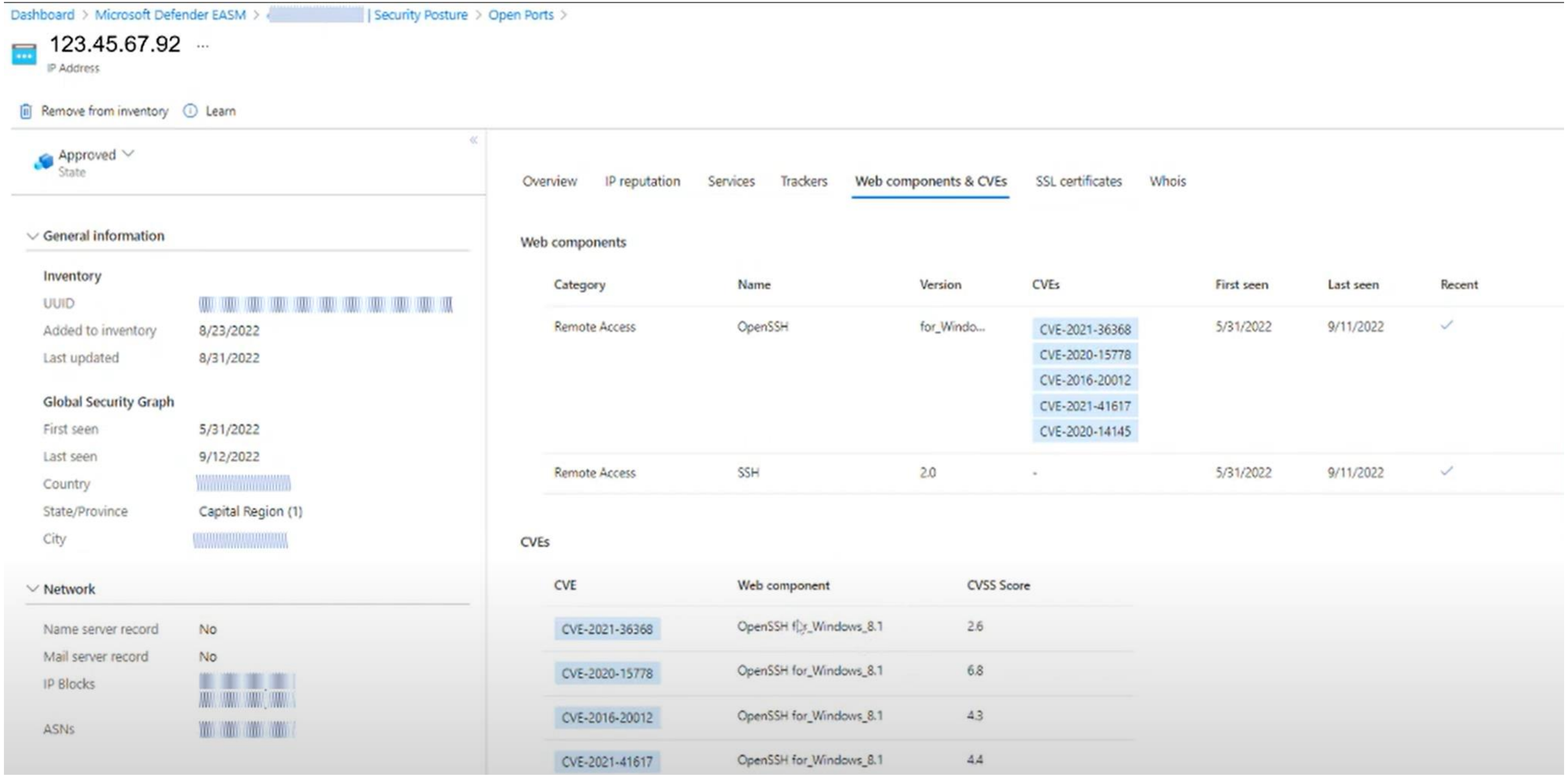
Anomalous open ports can be indicators of many things such as misconfigurations, non-adherance to deployment standards, even potential malicious activity. Regardless of the cause, exposure of sensetive ports can reveal potential ingress or egress of threats and exfiltration. At a minimum, certain open ports attract unwanted attention by attackers mass scanning the internet.

How to remediate

Practice least priviledge in your attack surface deployment by only the exposing the minimal services needed. Review assets with exposed ports with an eye towards finding out why it was exposed in the first place; default (mis)configuration, human error, deployment script, etc. Work with other organizational stakeholders to find gaps in processes and guidlines that will eventually prevent errant exposures as much as possible.

Asset	Kind	Status
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved
[redacted]	IP Address	Approved

Remote Access Port – IP associated – W8.1 - Unpatched



Dashboard > Microsoft Defender EASM > [redacted] | Security Posture > Open Ports >

123.45.67.92 ...

IP Address

Approved
State

General information

Inventory

UUID [redacted]

Added to inventory 8/23/2022

Last updated 8/31/2022

Global Security Graph

First seen 5/31/2022

Last seen 9/12/2022

Country [redacted]

State/Province Capital Region (1)

City [redacted]

Network

Name server record No

Mail server record No

IP Blocks [redacted]

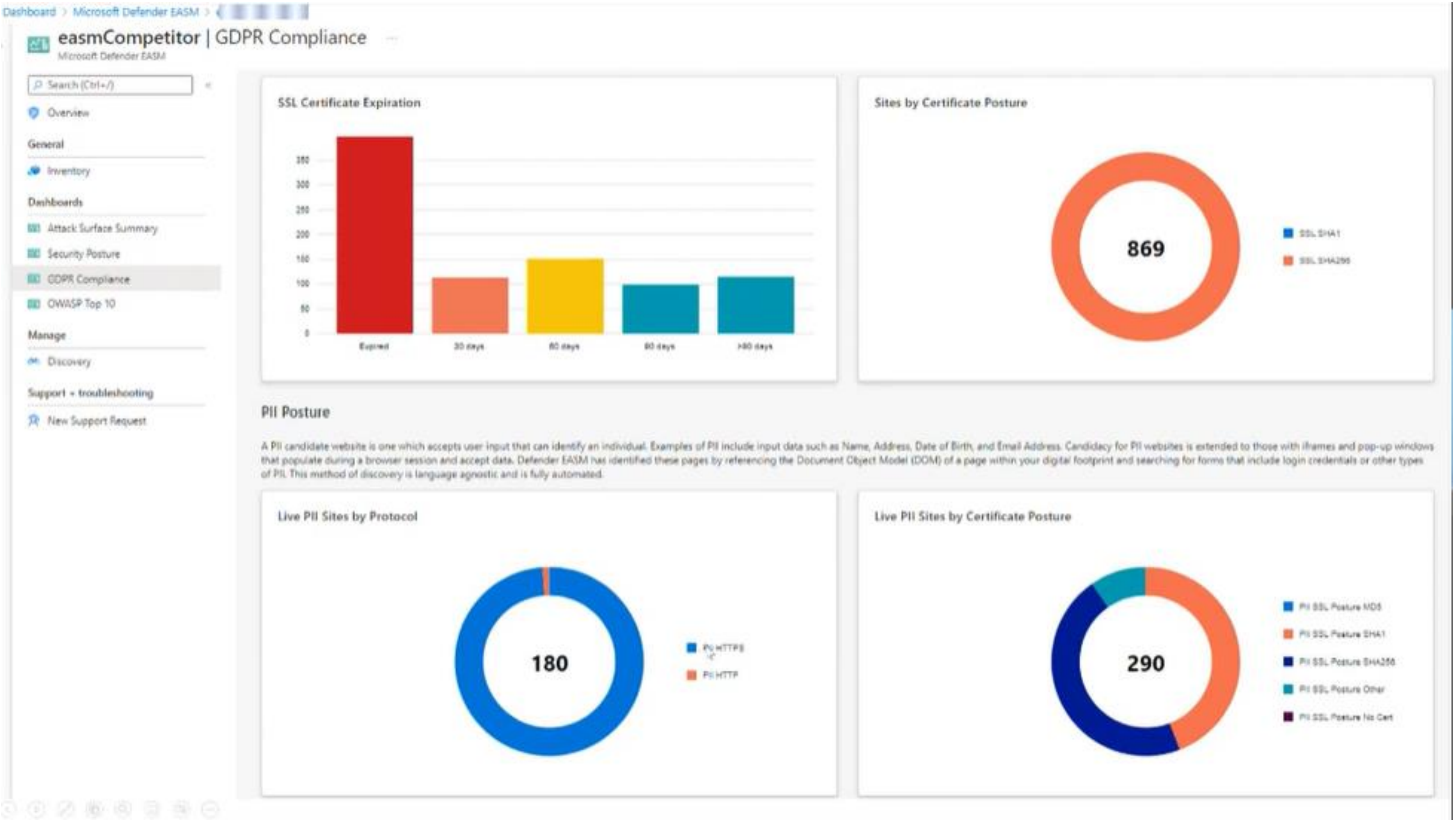
ASNs [redacted]

Web components

Category	Name	Version	CVEs	First seen	Last seen	Recent
Remote Access	OpenSSH	for_Windo...	CVE-2021-36368 CVE-2020-15778 CVE-2016-20012 CVE-2021-41617 CVE-2020-14145	5/31/2022	9/11/2022	✓
Remote Access	SSH	2.0	-	5/31/2022	9/11/2022	✓

CVEs

CVE	Web component	CVSS Score
CVE-2021-36368	OpenSSH for_Windows_8.1	2.6
CVE-2020-15778	OpenSSH for_Windows_8.1	6.8
CVE-2016-20012	OpenSSH for_Windows_8.1	4.3
CVE-2021-41617	OpenSSH for_Windows_8.1	4.4



Dashboard > Microsoft Defender EASM > [redacted]

easmCompetitor | GDPR Compliance

Microsoft Defender EASM

SSL Certificate Expiration

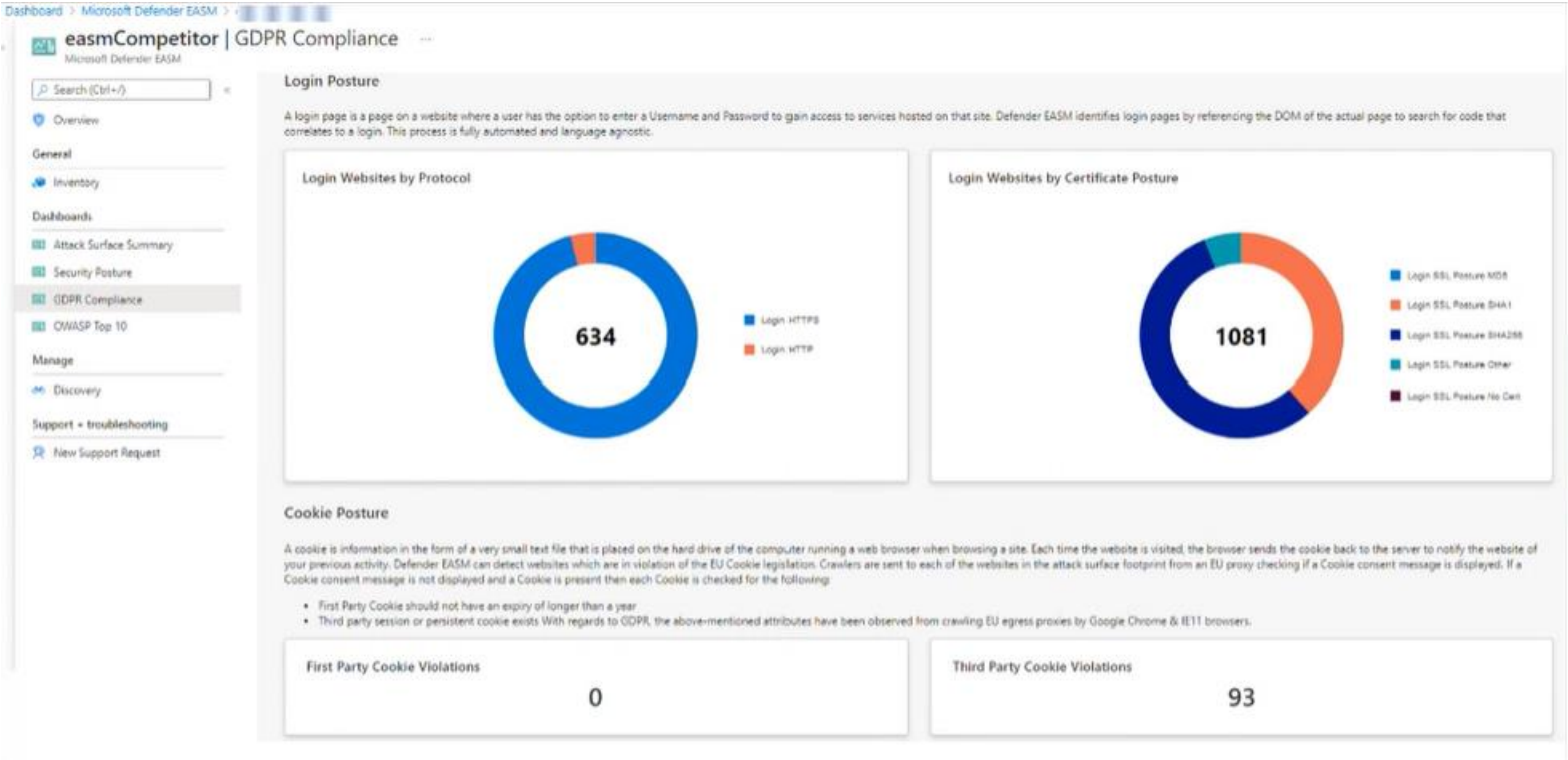
Sites by Certificate Posture

PII Posture

A PII candidate website is one which accepts user input that can identify an individual. Examples of PII include input data such as Name, Address, Date of Birth, and Email Address. Candidacy for PII websites is extended to those with iframes and pop-up windows that populate during a browser session and accept data. Defender EASM has identified these pages by referencing the Document Object Model (DOM) of a page within your digital footprint and searching for forms that include login credentials or other types of PII. This method of discovery is language agnostic and is fully automated.

Live PII Sites by Protocol

Live PII Sites by Certificate Posture



easmCompetitor | GDPR Compliance

Microsoft Defender EASM

Login Posture

A login page is a page on a website where a user has the option to enter a Username and Password to gain access to services hosted on that site. Defender EASM identifies login pages by referencing the DOM of the actual page to search for code that correlates to a login. This process is fully automated and language agnostic.

Login Websites by Protocol

634

Login Websites by Certificate Posture

1081

Cookie Posture

A cookie is information in the form of a very small text file that is placed on the hard drive of the computer running a web browser when browsing a site. Each time the website is visited, the browser sends the cookie back to the server to notify the website of your previous activity. Defender EASM can detect websites which are in violation of the EU Cookie legislation. Crawlers are sent to each of the websites in the attack surface footprint from an EU proxy checking if a Cookie consent message is displayed. If a Cookie consent message is not displayed and a Cookie is present then each Cookie is checked for the following:

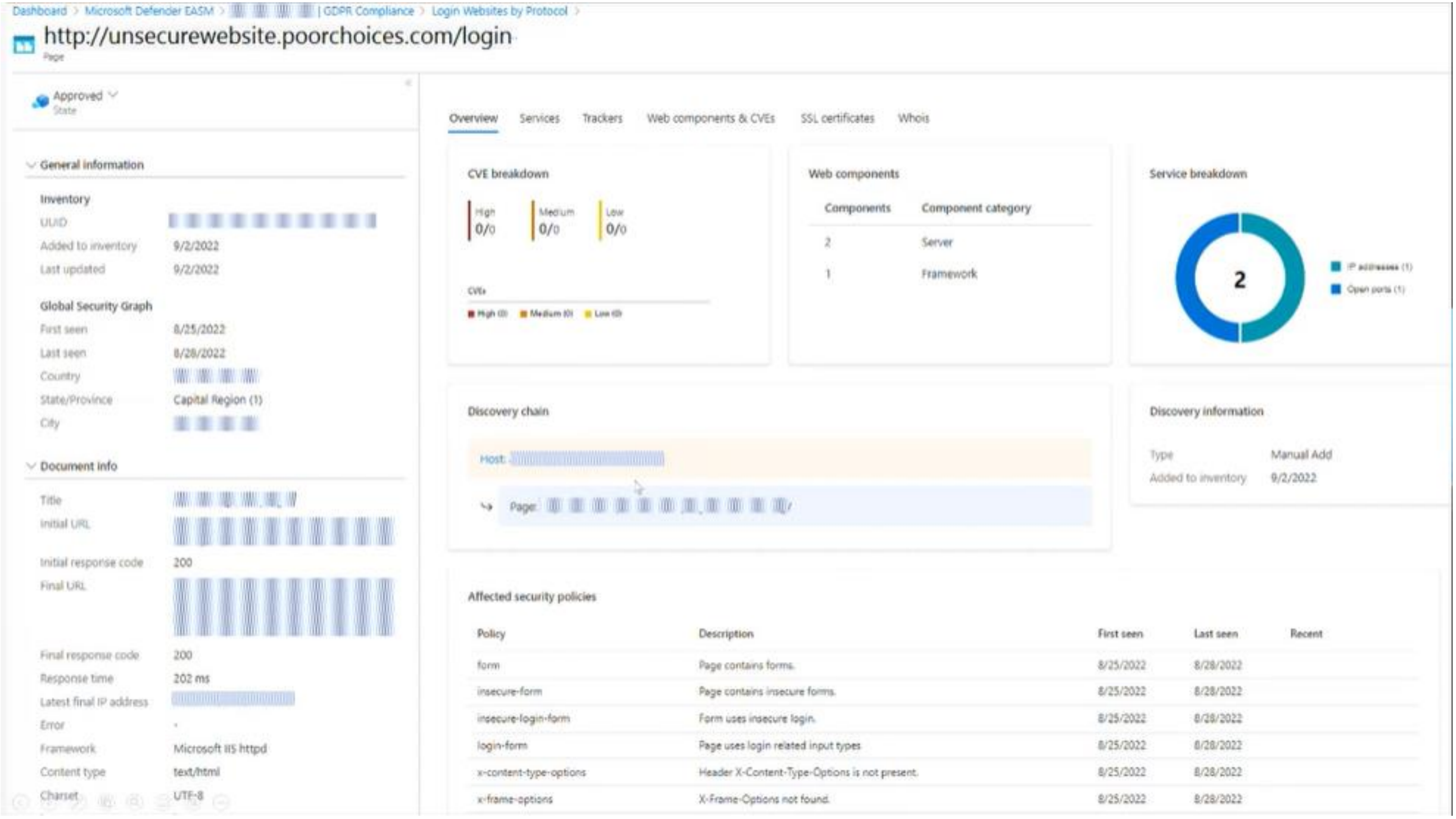
- First Party Cookie should not have an expiry of longer than a year
- Third party session or persistent cookie exists With regards to GDPR, the above-mentioned attributes have been observed from crawling EU egress proxies by Google Chrome & IE11 browsers.

First Party Cookie Violations

0

Third Party Cookie Violations

93



Dashboard > Microsoft Defender EASM > [redacted] | GDPR Compliance > Login Websites by Protocol >

http://unsecurewebsite.poorchoices.com/login

Page

Approved
State

General information

Inventory

UUID	[redacted]
Added to inventory	9/2/2022
Last updated	9/2/2022

Global Security Graph

First seen	8/25/2022
Last seen	8/28/2022
Country	[redacted]
State/Province	Capital Region (1)
City	[redacted]

Document info

Title	[redacted]
Initial URL	[redacted]
Initial response code	200
Final URL	[redacted]
Final response code	200
Response time	202 ms
Latest final IP address	[redacted]
Error	-
Framework	Microsoft IIS httpd
Content type	text/html
Charset	UTF-8

CVE breakdown

High	Medium	Low
0/0	0/0	0/0

Web components

Components	Component category
2	Server
1	Framework

Service breakdown

Discovery chain

Host: [redacted]

↳ Page: [redacted]

Discovery information

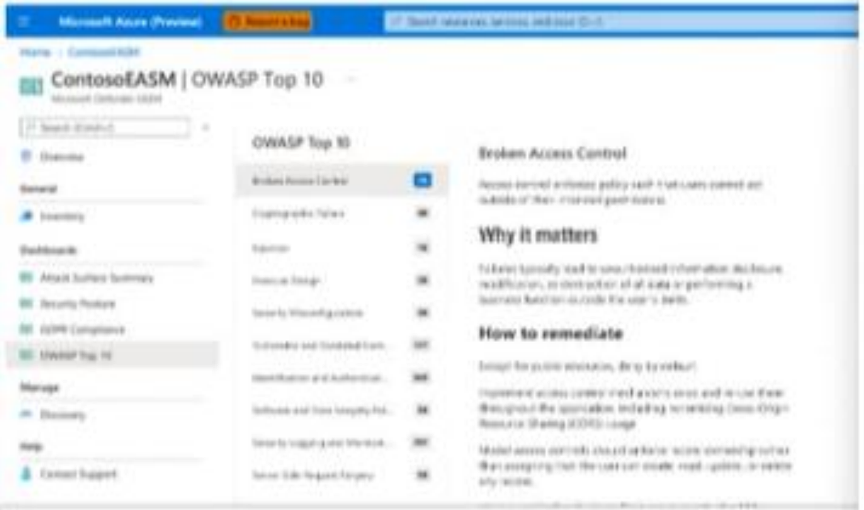
Type	Manual Add
Added to inventory	9/2/2022

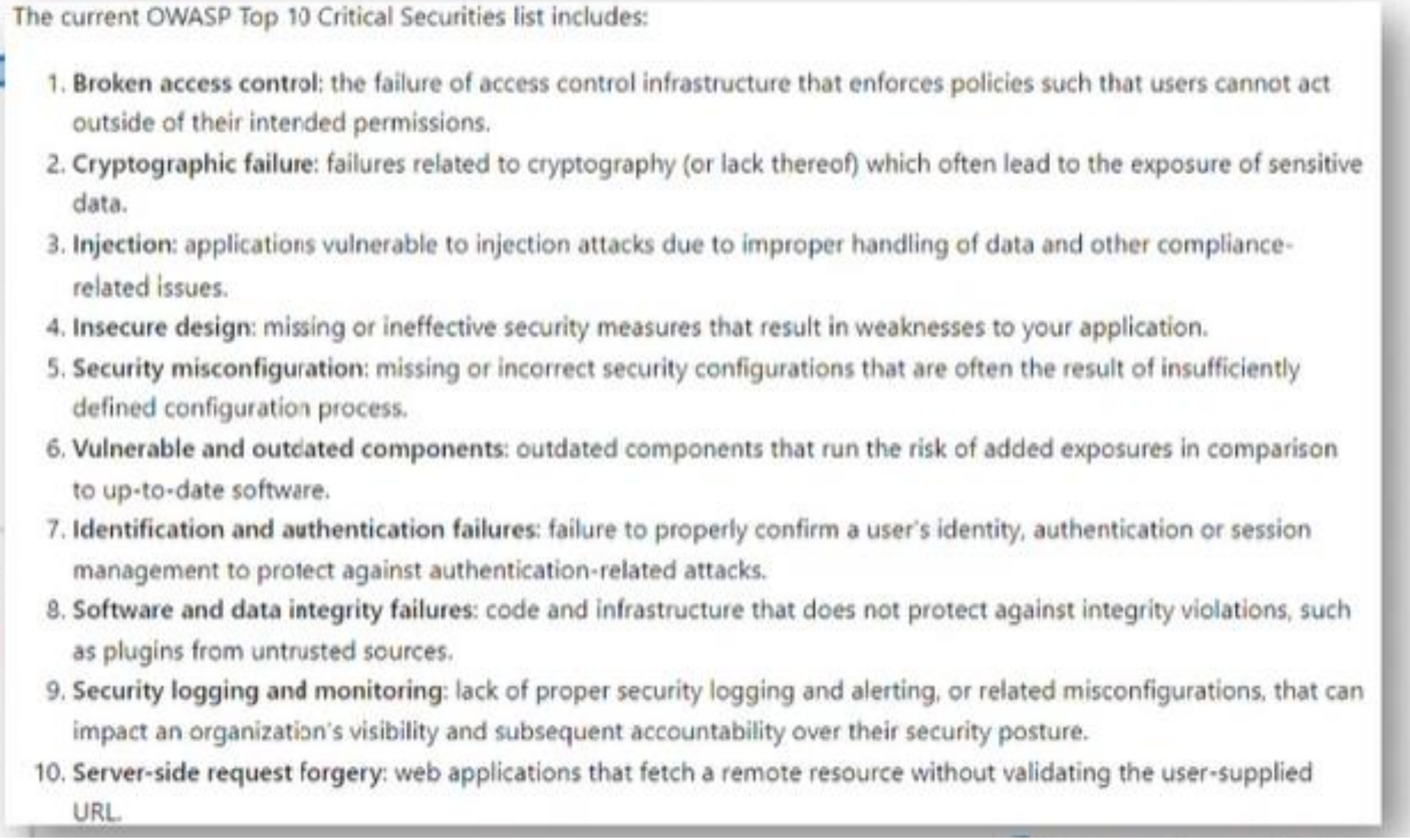
Affected security policies

Policy	Description	First seen	Last seen	Recent
form	Page contains forms.	8/25/2022	8/28/2022	
insecure-form	Page contains insecure forms.	8/25/2022	8/28/2022	
insecure-login-form	Form uses insecure login.	8/25/2022	8/28/2022	
login-form	Page uses login related input types	8/25/2022	8/28/2022	
x-content-type-options	Header X-Content-Type-Options is not present.	8/25/2022	8/28/2022	
x-frame-options	X-Frame-Options not found.	8/25/2022	8/28/2022	

OWASP top 10 dashboard

The OWASP Top 10 dashboard is designed to provide insight on the most critical security recommendations as designated by OWASP, a reputable open-source foundation for web application security. This list is globally recognized as a critical resource for developers who want to ensure their code is secure. OWASP provides key information about their top 10 security risks, as well as guidance on how to avoid or remediate the issue. This Defender EASM dashboard looks for evidence of these security risks within your Attack Surface and surfaces them, listing any applicable assets and how to remediate the risk.

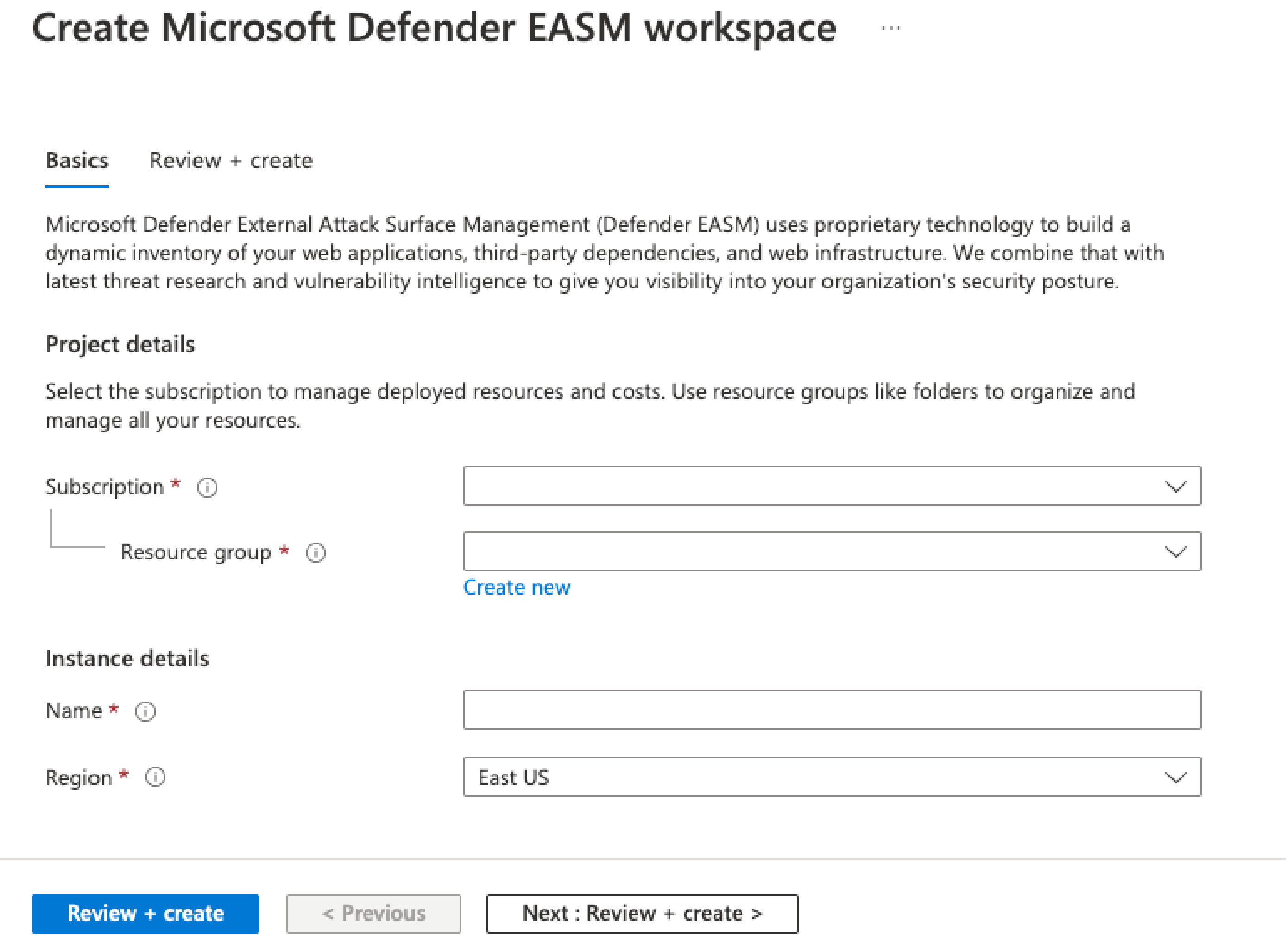




The current OWASP Top 10 Critical Securities list includes:

1. **Broken access control**: the failure of access control infrastructure that enforces policies such that users cannot act outside of their intended permissions.
2. **Cryptographic failure**: failures related to cryptography (or lack thereof) which often lead to the exposure of sensitive data.
3. **Injection**: applications vulnerable to injection attacks due to improper handling of data and other compliance-related issues.
4. **Insecure design**: missing or ineffective security measures that result in weaknesses to your application.
5. **Security misconfiguration**: missing or incorrect security configurations that are often the result of insufficiently defined configuration process.
6. **Vulnerable and outdated components**: outdated components that run the risk of added exposures in comparison to up-to-date software.
7. **Identification and authentication failures**: failure to properly confirm a user's identity, authentication or session management to protect against authentication-related attacks.
8. **Software and data integrity failures**: code and infrastructure that does not protect against integrity violations, such as plugins from untrusted sources.
9. **Security logging and monitoring**: lack of proper security logging and alerting, or related misconfigurations, that can impact an organization's visibility and subsequent accountability over their security posture.
10. **Server-side request forgery**: web applications that fetch a remote resource without validating the user-supplied URL.

Nødvendig for å komme i gang



Create Microsoft Defender EASM workspace

Microsoft Defender External Attack Surface Management (Defender EASM) uses proprietary technology to build a dynamic inventory of your web applications, third-party dependencies, and web infrastructure. We combine that with latest threat research and vulnerability intelligence to give you visibility into your organization's security posture.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	
Resource group *	
	Create new

Instance details

Name *	
Region *	East US

- Azure Subscription
- Resource Group
- Tilgjengelige regioner PT.
  - southcentralus
  - westus3
  - eastus
  - eastasia
  - swedencental
  - Australieast
  - japaneast

Kilder

https://msandbu.org/getting-started-with-microsoft-defender-easm-external-attack-surface-management/

https://learn.microsoft.com/en-us/azure/external-attack-surface-management/

https://derkvanderwoude.medium.com/introduction-into-microsoft-defender-easm-external-attack-surface-management-3fdee6ccf256

https://jeffreyappel.nl/how-to-use-microsoft-defender-easm-external-attack-surface-management/

Tusen takk!

MVP-Dagen