Strategic Cyber Security Report — August 2023 Edition

Andre Camillo, CISSP

Published in InfoSec Write-ups · 8 min read · Aug 31, 2023

A Monthly summary of Strategic Information for Cyber Security Leaders

This is a series spun from a need I identified when talking to CISOs — as explained on the kick-off article, this series follows the format of:

> What's Top of mind in 3 domains: People, Processes, Technology for CISOs.

People

The state of AI legislation in different US states as of August 2023

The US law system is different from some countries. As explained by bing chat (sources linked):

> *"In the United States, the 50 individual states and the United States as a whole are each sovereign jurisdictions1. Under constitutional laws, states are permitted to create, implement, and enforce their own laws in addition to federal laws2. This is because every state in the United States is a sovereign entity in its own right and is granted the power to create laws and regulate those laws according to their needs"*

This means that each state can pass laws that are different to others. And this is applied to the field of AI legislation too.

The Electronic Privacy Information Center (EPIC) organization has documented the current state of AI legislation in different states across the US here.

It's a great snapshot of different bills and AI regulation in the US in the following themes:

- **Laws going into effect in 2023**
- **Laws passed this legislative session**
- **Laws proposed this legislative session:**

> *AI Regulation as part of Comprehensive Consumer Privacy Bills*
>
> *AI Regulation to Prevent General Harms*
>
> *Regulating AI in Employment Settings*
>
> *Regulating AI in Healthcare*
>
> *Regulating AI in Insurance*
>
> *Regulating AI Used by the Government*
>
> *Regulating Generative AI*
>
> *Bills to Increase Transparency and Understanding Around AI*
>
> *Other AI-related Bills*

Read all the details and the full article here.

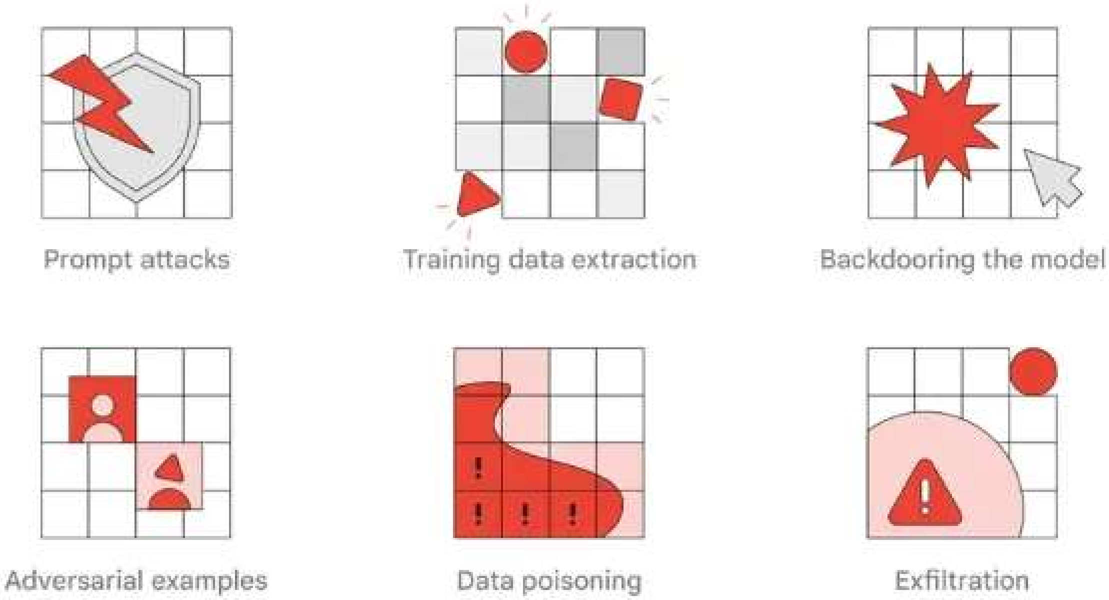
Google's AI Red team tips

This is a great report by Google's Red team on AI security. You can find it here.

It reinforces the value of Google's Secure AI Framework (SAIF) for practices and principles underlying AI Security.

The paper above talks about the approach of Red teaming with AI.

In it, they summarize common Attacker TTPs against AI in these 6 forms:



Source: Google

Read the report for details on each of them.

Lastly, they provide a summary of their lessons learned, key for every large enterprise working with AI these days, which I will further summarize into these bullet points:

- Red teams will benefit from having an AI subject matter expert.
- Some attacks may not have simple fixes.

- Many attacks against models and systems can be effectively mitigated by well implemented traditional lock down controls.
- Many AI threats can be mitigated the same way traditional attacks are. Other techniques (Prompt attacks, Content Issues) will require layering multiple security models.

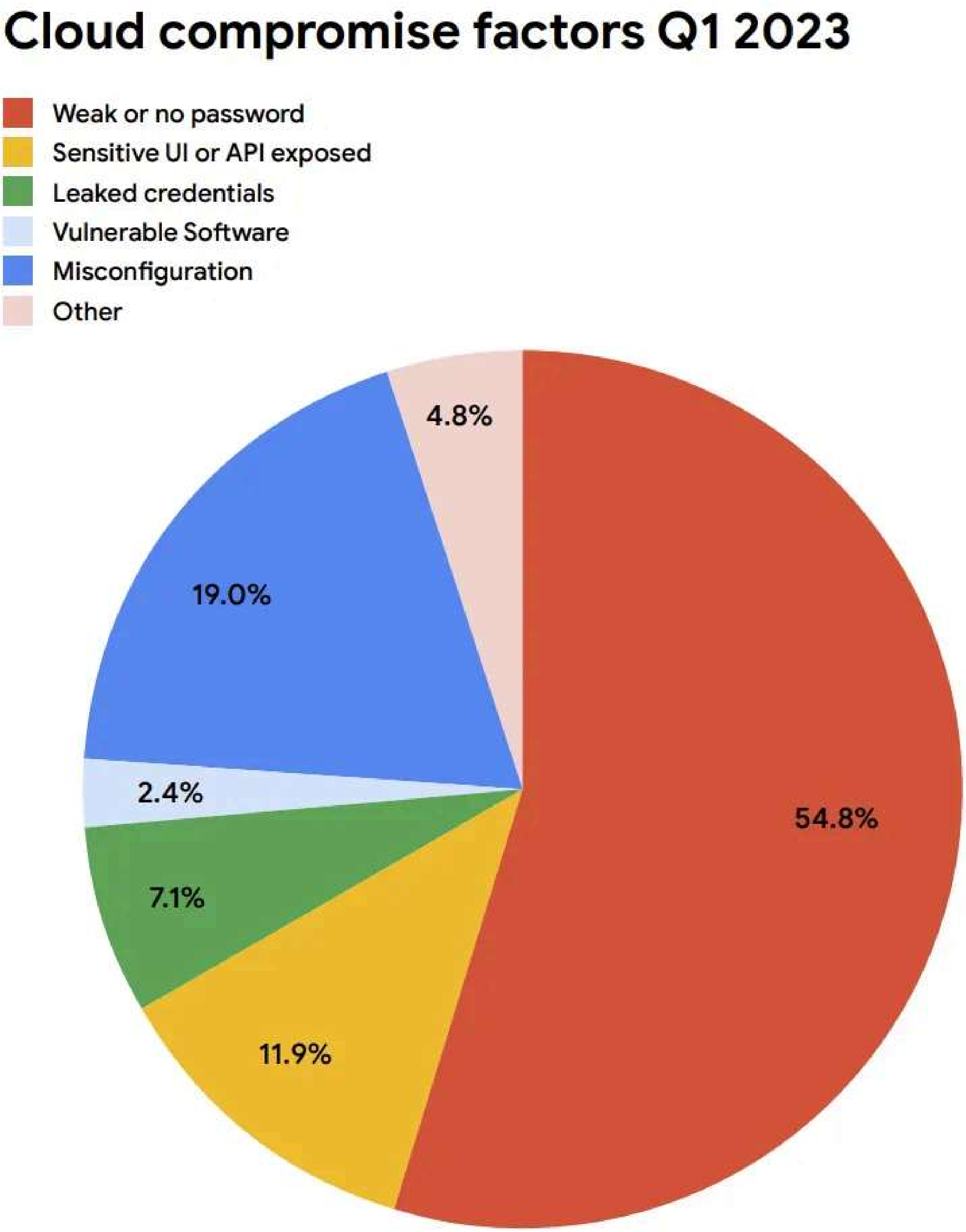
Read the article here.

Google Cybersecurity Action Team Threat Horizons

Google release a new threat horizons report with sightings from its action team.

According to observations from their Incidents response teams, the main factor leading to cloud compromises is still credential issues alloting more than 60% of compromise factors. Misconfiguration is next in line with 19% compromise factor incidence.

From the report:



Source: Google Report

Read Anton Chuvakin’s summary in this blog post.

The report also includes information on the top risky actions that lead to compromises which is by far: "Cross-Project abuse og GCP token access generation permission" associated with MITRE ATT&CK® tactic of Privilege Escalation (TA0004) and technique of Valid Accounts: Cloud Accounts (T1078.004).

Next I want to touch on Supply Chain section they reported. According to the report, the below image:

> *"highlights eight different ways the supply chain can be compromised between the developer producing software and the end user consuming it. Though a developer may be creating software with good intent, this doesn't stop malicious actors from compromising the supply chain before it reaches customers."*

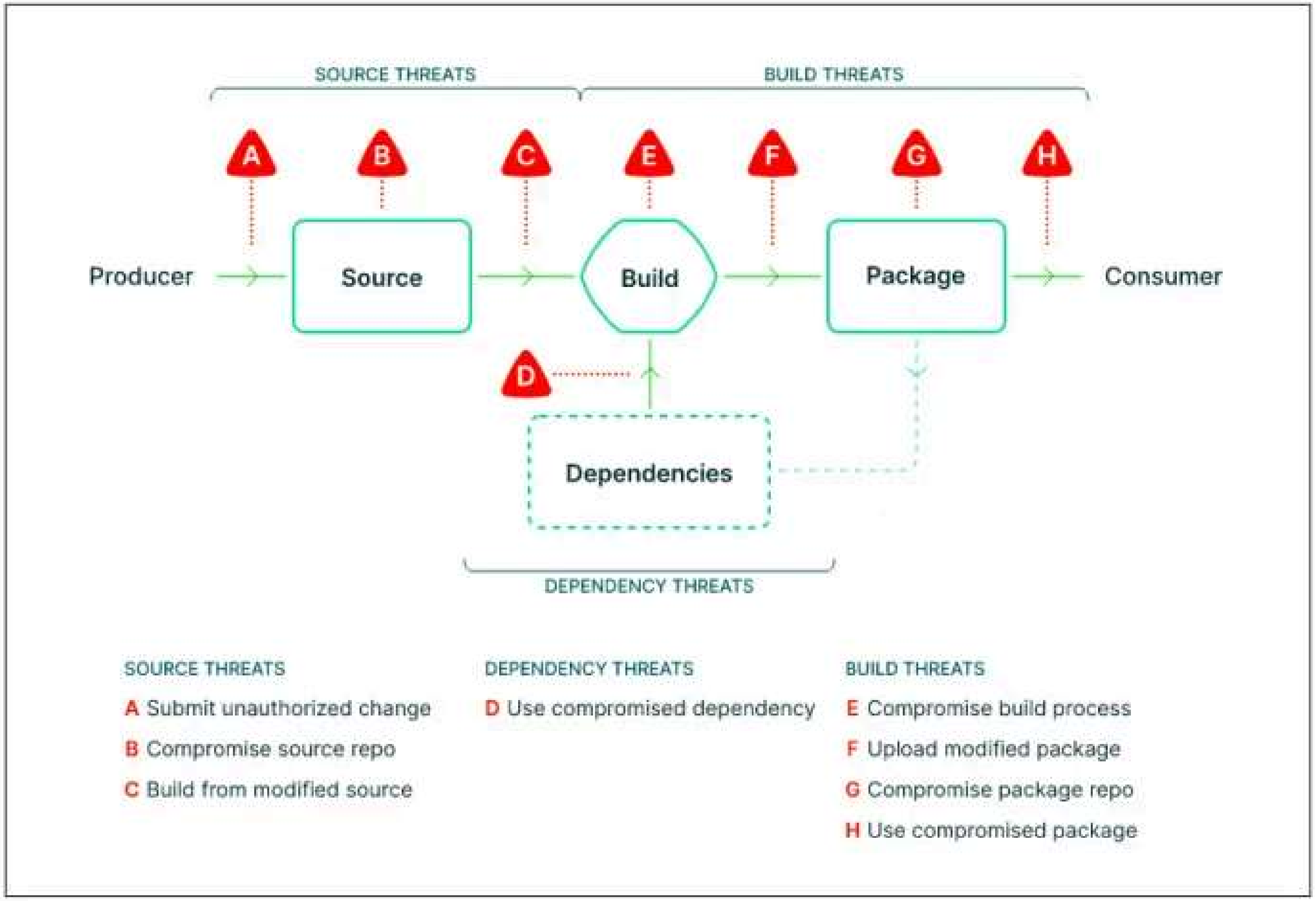
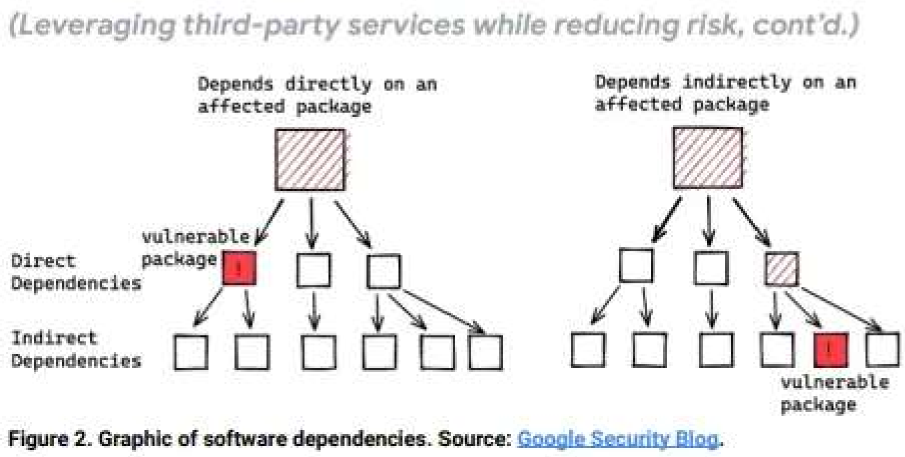

SOURCE THREATS
BUILD THREATS
A
B
C
E
F
G
H
Producer
Source
Build
Package
Consumer
D
Dependencies
DEPENDENCY THREATS
SOURCE THREATS
A Submit unauthorized change
B Compromise source repo
C Build from modified source
DEPENDENCY THREATS
D Use compromised dependency
BUILD THREATS
E Compromise build process
F Upload modified package
G Compromise package repo
H Use compromised package

Figure 1. Graphic outlighting supply chain threats. Source: Supply-chain Levels for Software Artifacts

Source: Google Threat horizons report July 2023.

Supply chain threats can stem from direct or indirect package dependencies, as their report:



(Leveraging third-party services while reducing risk, cont'd.)

Depends directly on an affected package
Depends indirectly on an affected package
vulnerable package
Direct Dependencies
Indirect Dependencies
!
!
vulnerable package

Figure 2. Graphic of software dependencies. Source: Google Security Blog.

source: Google

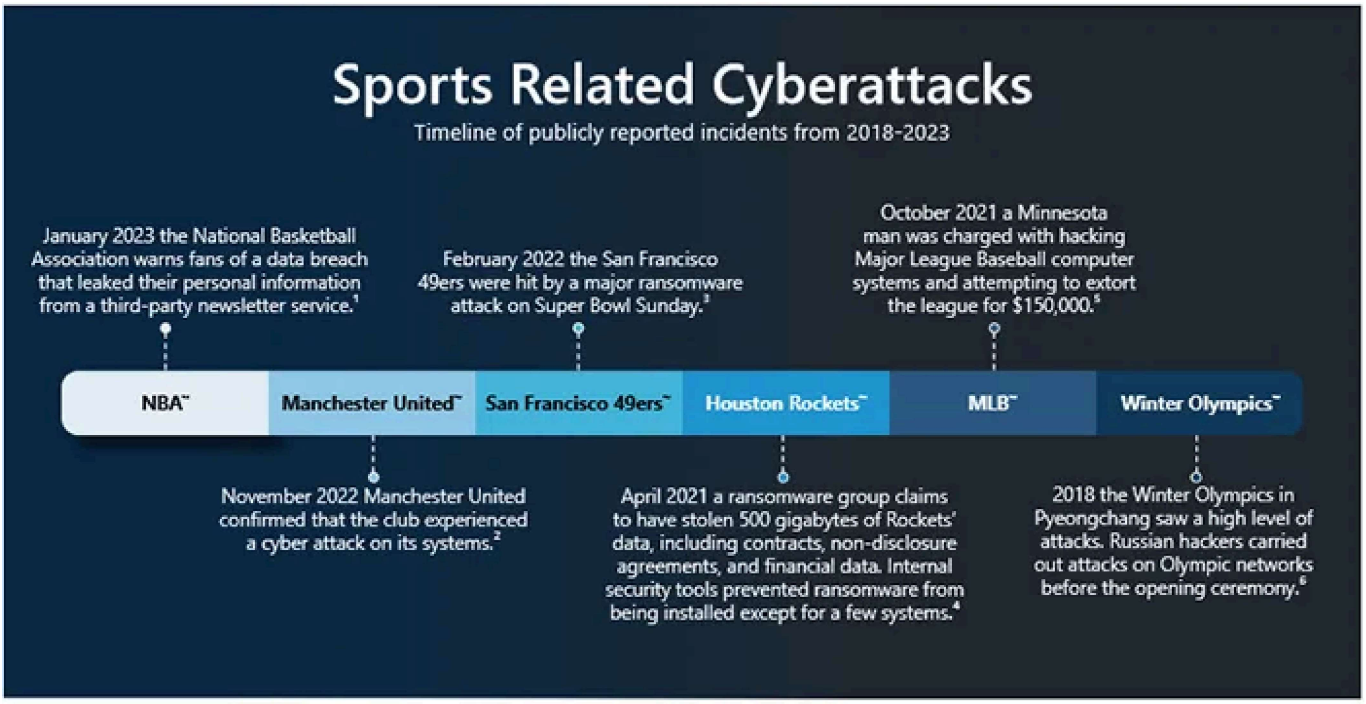
The report goes on to detail these threats in a cloud environment and better yet, how to mitigate them.

There are heaps more interesting bits in the report, I highly recommend you check it out, the full report can be found here.

Microsoft Cyber Signals 5

Microsoft released a new Cyber Signals report, issue 5.

In this report, the security team reports on attacks against Sports events — which the team supported including the FIFA world cup 2022. ⚽



Sports Related Cyberattacks

Timeline of publicly reported incidents from 2018-2023

January 2023 the National Basketball Association warns fans of a data breach that leaked their personal information from a third-party newsletter service.[1]

November 2022 Manchester United confirmed that the club experienced a cyber attack on its systems.[2]

February 2022 the San Francisco 49ers were hit by a major ransomware attack on Super Bowl Sunday.[3]

April 2021 a ransomware group claims to have stolen 500 gigabytes of Rockets' data, including contracts, non-disclosure agreements, and financial data. Internal security tools prevented ransomware from being installed except for a few systems.[4]

October 2021 a Minnesota man was charged with hacking Major League Baseball computer systems and attempting to extort the league for $150,000.[5]

2018 the Winter Olympics in Pyeongchang saw a high level of attacks. Russian hackers carried out attacks on Olympic networks before the opening ceremony.[6]

source: Microsoft

Microsoft provided a number of recommendations including:

> ***Augment the SOC team:*** *Have an additional set of eyes monitoring the event around the clock to proactively detect threats and send notifications. This helps correlate more hunting data and discover early signs of intrusion. It should include threats beyond endpoint, like identity compromise or device to cloud pivot.*
>
> ***Conduct a focused cyber risk assessment:*** *Identify potential threats specific to the event, venue, or nation where the event occurs. This assessment should include vendors, team and venue IT professionals, sponsors, and key event stakeholders.*
>
> ***Consider least privileged access a best practice:*** *Grant access to systems and services only to those who need it, and train staff to understand access layers.*

Read the report here.

Process

CSPM Market analysis by Kuppingercole

The report provides a guide to the CSPM (Cloud Security Posture Management) market and helps organizations choose the solution that suits their needs.

It looks at solutions that help you continuously find and manage certain risks related to using cloud services. And it evaluates how well these solutions can meet the CSPM needs of all organizations to watch, check, and handle these risks.

As explained by the publisher:

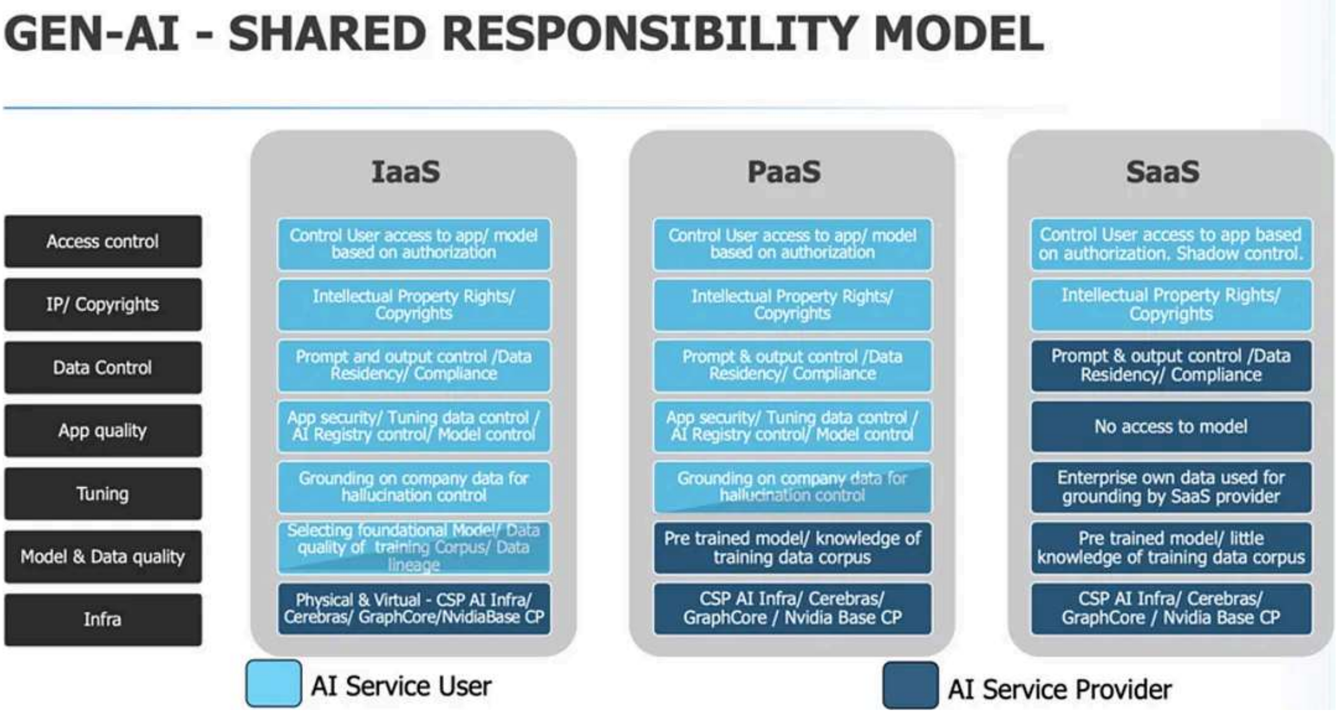
> *"This report provides an overview of the CSPM (Cloud Security Posture Management) market and a compass to help you find a solution that best meets your needs. It examines solutions that provide a way to continuously identify and control certain risks associated with the use of cloud services. It provides an assessment of the capabilities of these solutions to meet the CSPM needs of all organizations to monitor, assess, and manage these risks."*

They have an image representing the leaders which include Microsoft and other vendors. To access it you need to sign up, Read more about it here.

AI Security Shared responsibility Model

The Cloud Security Alliance has published some thoughts on Generative AI considerations for organizations adoption this technology.

They have a proposed responsibility model which you can see below:



GEN-AI - SHARED RESPONSIBILITY MODEL

	IaaS	PaaS	SaaS
Access control	Control User access to app/ model based on authorization	Control User access to app/ model based on authorization	Control User access to app based on authorization. Shadow control.
IP/ Copyrights	Intellectual Property Rights/ Copyrights	Intellectual Property Rights/ Copyrights	Intellectual Property Rights/ Copyrights
Data Control	Prompt and output control /Data Residency/ Compliance	Prompt & output control /Data Residency/ Compliance	Prompt & output control /Data Residency/ Compliance
App quality	App security/ Tuning data control / AI Registry control/ Model control	App security/ Tuning data control / AI Registry control/ Model control	No access to model
Tuning	Grounding on company data for hallucination control	Grounding on company data for hallucination control	Enterprise own data used for grounding by SaaS provider
Model & Data quality	Selecting foundational Model/ Data quality of training Corpus/ Data lineage	Pre trained model/ knowledge of training data corpus	Pre trained model/ little knowledge of training data corpus
Infra	Physical & Virtual - CSP AI Infra/ Cerebras/ GraphCore/NvidiaBase CP	CSP AI Infra/ Cerebras/ GraphCore / Nvidia Base CP	CSP AI Infra/ Cerebras/ GraphCore / Nvidia Base CP

AI Service User

AI Service Provider

Source: CSA

Read the article by CSA here.

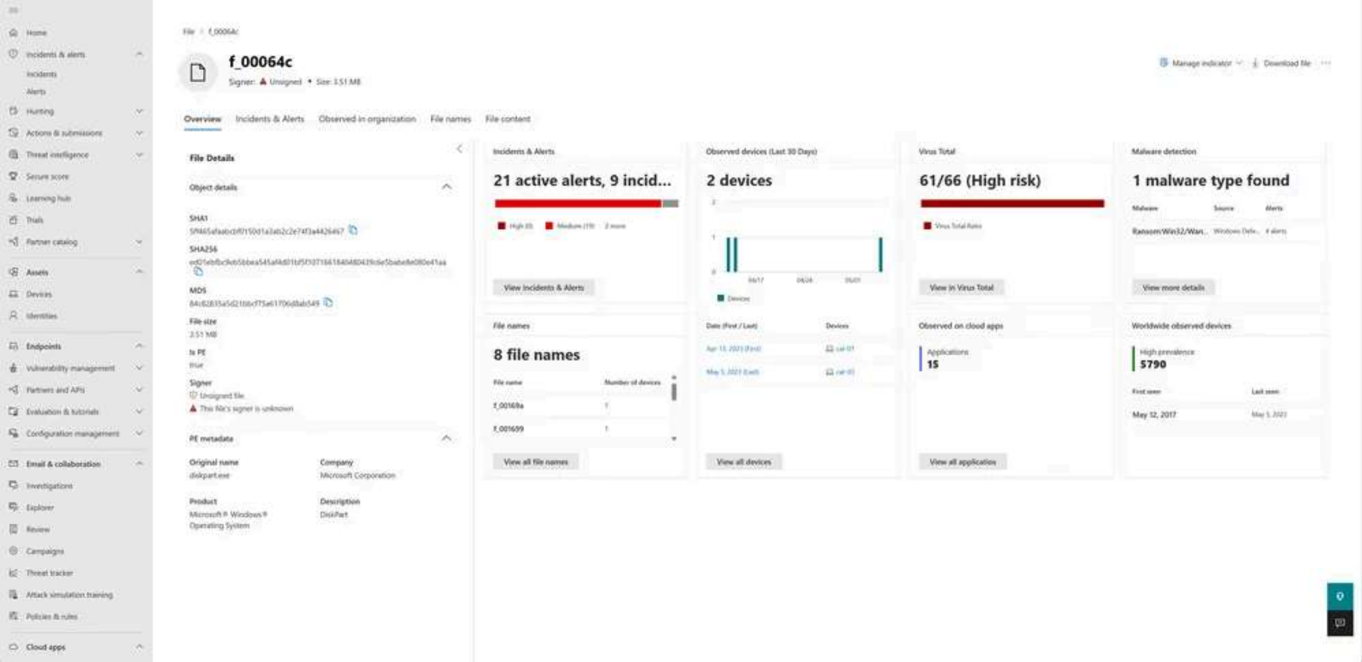
Technology

Microsoft 365 Defender news

The M365 Defender suite is an all-encompassing brand of solutions for User security. This monthly newsletter from Product Manager Heike touches on the latest news on the many different products within the suite. Here are some of my personal highlights:

Microsoft 365 Defender:

- *New File page* in public preview allows security teams to analyze and pivot across devices and cloud applications.



f_00064c

Signer: Unsigned • Size: 3.51 MB

File Details

Object details

SHA1
[illegible]

SHA256
[illegible]

MD5
[illegible]

File size
3.51 MB

Is PE
true

Signer
Unsigned file
This file's signer is unknown

PE metadata

Original name
diskpart.exe

Company
Microsoft Corporation

Product
Microsoft® Windows® Operating System

Description
DiskPart

Incidents & Alerts
21 active alerts, 9 incid...

Observed devices (Last 30 Days)
2 devices

Virus Total
61/66 (High risk)

Malware detection
1 malware type found

Malware	Source	Alerts
Ransom:Win32/Wan...	Windows Defe...	4 alerts

File names
8 file names

File name	Number of devices
f_00169a	1
f_001699	1

Date (First / Last)	Devices
Apr 13, 2023 (First)	cat-01
May 5, 2023 (Last)	cat-01

Observed on cloud apps
Applications
15

Worldwide observed devices
High prevalence
5790

First seen	Last seen
May 12, 2017	May 5, 2023

source: Monthly news — August 2023 — Microsoft Community Hub

- *New URL page* Including improved URL and domains investigation page reducing need to navigate on different interfaces.

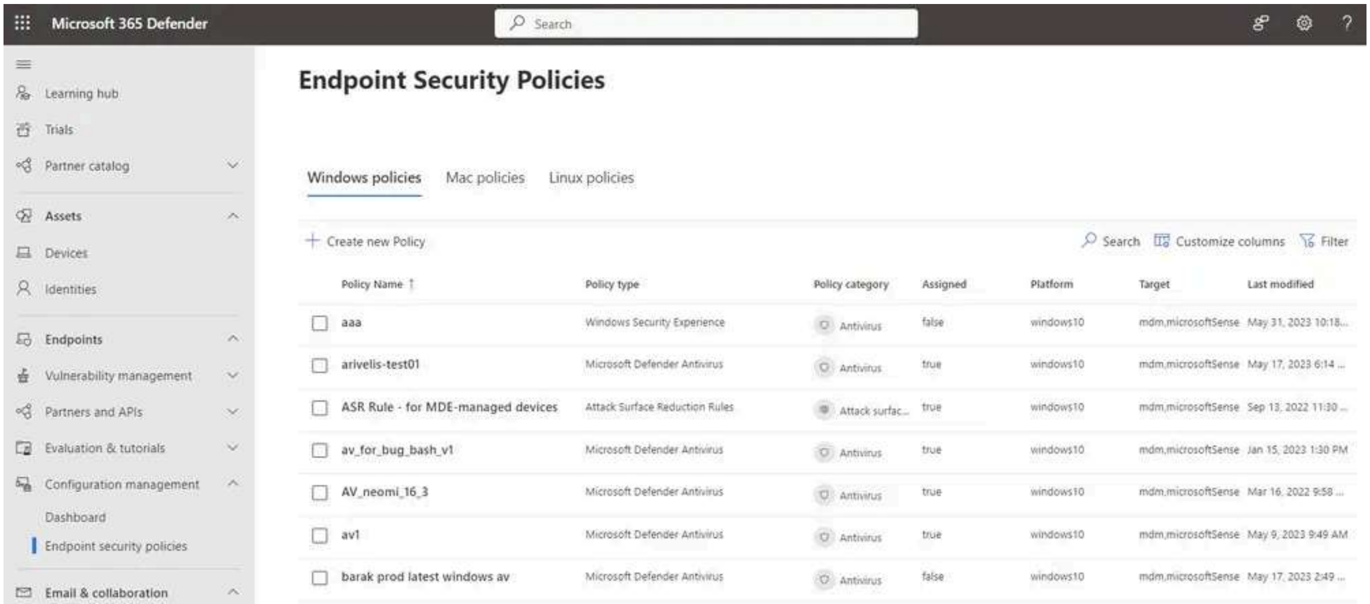
Microsoft Security Experts:

- Microsoft Defender experts for XDR, a managed XDR service that helps SOCs.

Microsoft Defender for Endpoint:

Run the drum rolls for the much anticipated…

- *Security Settings management natively in M365 Defender* portal now in Public Preview — something I really looked forward to 😎



Endpoint Security Policies

	Policy Name ↑	Policy type	Policy category	Assigned	Platform	Target	Last modified
□	aaa	Windows Security Experience	Antivirus	false	windows10	mdm,microsoftSense	May 31, 2023 10:18...
□	arivelis-test01	Microsoft Defender Antivirus	Antivirus	true	windows10	mdm,microsoftSense	May 17, 2023 6:14 ...
□	ASR Rule - for MDE-managed devices	Attack Surface Reduction Rules	Attack surfac...	true	windows10	mdm,microsoftSense	Sep 13, 2022 11:30 ...
□	av_for_bug_bash_v1	Microsoft Defender Antivirus	Antivirus	true	windows10	mdm,microsoftSense	Jan 15, 2023 1:30 PM
□	AV_neomi_16_3	Microsoft Defender Antivirus	Antivirus	true	windows10	mdm,microsoftSense	Mar 16, 2022 9:58 ...
□	av1	Microsoft Defender Antivirus	Antivirus	true	windows10	mdm,microsoftSense	May 9, 2023 9:49 AM
□	barak prod latest windows av	Microsoft Defender Antivirus	Antivirus	false	windows10	mdm,microsoftSense	May 17, 2023 2:49 ...

source: Monthly news — August 2023 — Microsoft Community Hub

- *Device Isolation and AV scanning for Linux and MacOS* — great new response actions for MDE in these platforms.

Microsoft Defender for Cloud Apps:

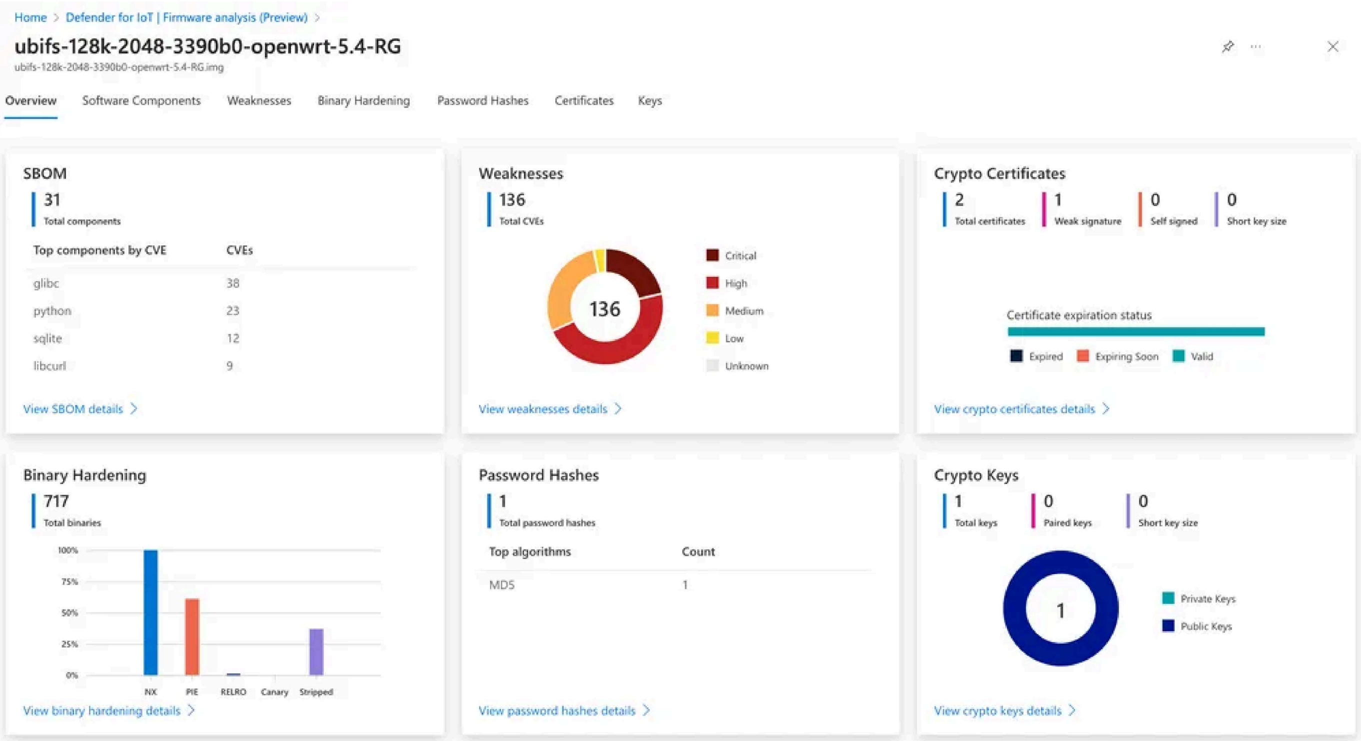
- *Default redirect* from legacy MDCA portal to M365 Defender portal.

Microsoft Defender for Identity:

- *Search for AD groups in M365 Defender* now in Preview, great for security engineers.
- *Report downloading and scheduling in M365 Defender for MDI*. This creates parity in report functionality with the classic Defender for Identity portal. Download and schedule reports in Microsoft 365 Defender from the Settings > Identities > Report management page.

Microsoft Defender for IoT:

- *Analyze IoT/OT device firmware with MDIoT.*



Home > Defender for IoT | Firmware analysis (Preview) >

ubifs-128k-2048-3390b0-openwrt-5.4-RG

ubifs-128k-2048-3390b0-openwrt-5.4-RG.img

SBOM

31 Total components

Top components by CVE	CVEs
glibc	38
python	23
sqlite	12
libcurl	9

View SBOM details >

Weaknesses

136 Total CVEs

View weaknesses details >

Crypto Certificates

2 Total certificates

1 Weak signature

0 Self signed

0 Short key size

View crypto certificates details >

Binary Hardening

717 Total binaries

View binary hardening details >

Password Hashes

1 Total password hashes

Top algorithms	Count
MD5	1

View password hashes details >

Crypto Keys

1 Total keys

0 Paired keys

0 Short key size

View crypto keys details >

source: Monthly news — August 2023 — Microsoft Community Hub

Microsoft Defender for Office 365:

- ***New DMARC policy handing defaults*** — choose how to handle emails that fail DMARC validation and choose different actions.
- ***New content available under Attack Simulation Training*** — now includes content from SANS, on top of the Terranova training content.

> *“To preview these training modules as an admin before assigning to individuals, navigate to the [Training modules] section under the [Content library] tab in AST. All the training modules have a “SANS” tag so applying that filter to content library search will easily pull up the SANS training content.”*

Read the full post here.

Defender for cloud Releases in August

Microsoft Defender for Cloud updates for the month of August Include:

- **Business Model & Pricing updates:** Which incur in changes on Defender for DNS: Defender for Servers Plan 2 customers gain access to Defender for DNS value as part of Defender for Servers Plan 2 at no extra cost
- **New security alerts in Defender for Servers Plan 2: Detecting potential attacks abusing Azure virtual machine extensions:** Extensions are small applications that run on virtual machines and provide various capabilities, but they can also be abused by threat actors for malicious purposes, such as data collection, code execution, credential resetting, and disk encryption — The new alerts help monitor for these threats.
- **Preview release of GCP support in Defender CSPM:** The new plan (Defender CSPM) already getting new features, with support for GCP workloads, these include: Attack path analysis Agentless scanning, Data-aware security posture and more.
- **Extended properties in Defender for Cloud security alerts are masked from activity logs:** This change aims at improving sensitive customer information, which no longer is added to activity logs. Instead, it's masked with asterisks. This information is still available through the alerts API, continuous export, and the Defender for Cloud portal, however.
- **Recommendation release: Microsoft Defender for Storage should be enabled with malware scanning and sensitive data threat detection:** This is a new recommendation for Defender for Storage — to be enabled at subscription level with malware scanning and sensitive data threat detection capabilities. The announcement states: "This new

> recommendation will replace the current recommendation `Microsoft Defender for Storage should be enabled`”

Read all the updates here.

Learn more about my Cloud and Security Projects: https://linktr.ee/acamillo

Consider subscribing to Medium (here) to access more content that will empower you!

Thank you for reading and leave your thoughts/comments!

References

Scattered throughout the document.

Report Cybersecurity Cloud Computing Google Microsoft

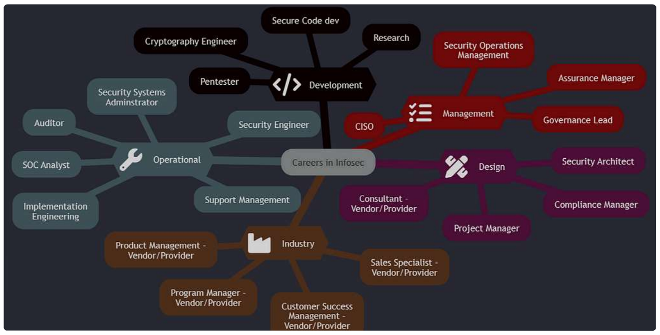
Written by Andre Camillo, CISSP

Edit profile

1K Followers · Writer for InfoSec Write-ups

Cloud and Security technologies, Career, Growth Mindset. Follow: https://linktr.ee/acamillo .
Technical Specialist @Microsoft. Opinions are my own.

More from Andre Camillo, CISSP and InfoSec Write-ups

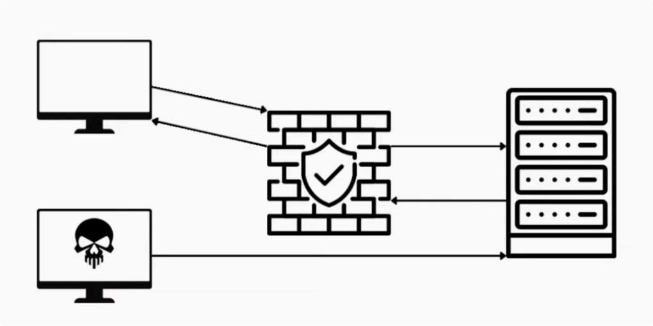

Secure Code dev
Cryptography Engineer
Research
Security Operations Management
Pentester
Development
Security Systems Adminstrator
Assurance Manager
Auditor
Security Engineer
CISO
Management
Governance Lead
SOC Analyst
Operational
Careers in Infosec
Design
Security Architect
Implementation Engineering
Support Management
Consultant - Vendor/Provider
Compliance Manager
Project Manager
Product Management - Vendor/Provider
Industry
Sales Specialist - Vendor/Provider
Program Manager - Vendor/Provider
Customer Success Management - Vendor/Provider

Andre Camillo, CISSP in CloudnSec

Cybersecurity Careers and Jobs for 2024

I've recently had the chance to talk about Diversity & Inclusion & the cyber security fiel…

Feb 21 52 2



Ott3rly in InfoSec Write-ups

Bypass Firewall by Finding Origin IP

Bypass WAF by finding origin IP address as a method. We will explore multiple ways how…

May 7 695 7