Strategic Cyber Security Report — September 2023 Edition

Andre Camillo, CISSP

Published in CloudnSec · 9 min read · Oct 2, 2023

28

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.

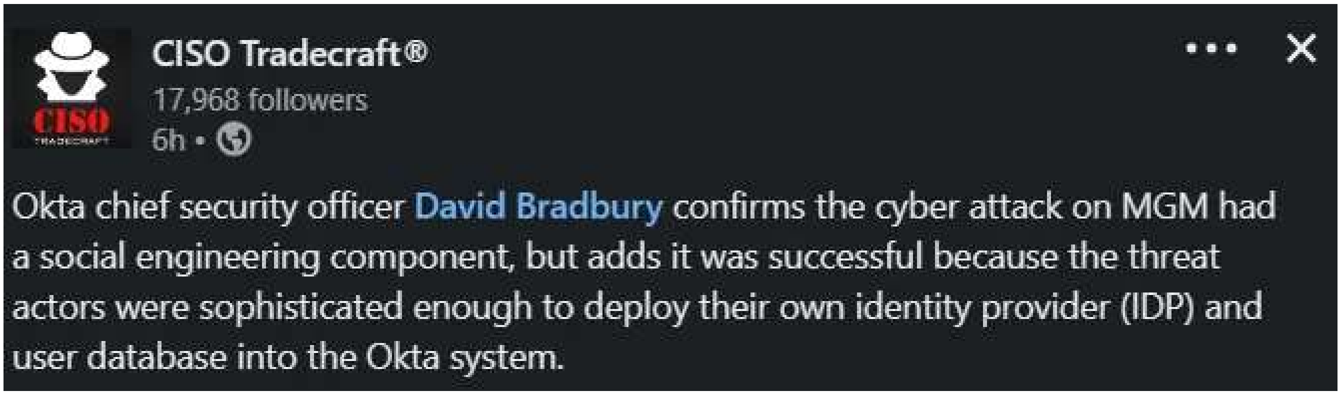
People

MGM Hotels hit by Cyber attack

MGM Resorts International, a major resort operation that owns more than two dozen hotel and casino locations around the world has been hit by a Ransomware attack. They released a timeline of what happened, soures include vox.com:

The attack began with a social engineering breach of the company’s information technology help desk, where hackers used vishing or convincing phone calls to gain access to systems. The hackers then used ransomware made by ALPHV, or BlackCat, to encrypt and demand payment for the data.

The attack affected many of MGM’s systems, including hotel room digital keys, slot machines, websites and guest information.


CISO Tradecraft®
17,968 followers
6h •

Okta chief security officer David Bradbury confirms the cyber attack on MGM had a social engineering component, but adds it was successful because the threat actors were sophisticated enough to deploy their own identity provider (IDP) and user database into the Okta system.

Darkreading reported that Okta IDP was used in the attack.

The impact?

The company said it was working to resolve the issue and protect its systems and data. However, some guests reported that their paychecks were late or they had trouble checking in or getting receipts.

It's not the first time they're hit by ransomware, in 2019 another incident impacted them and caused more than 10M hotel stayers information to be exposed, as bbc reported.

CNAPP Survey by Cloud Security Alliance

Cloud Native Application Protection Platforms (CNAPPs) are a category of security tooling that have become increasingly important in recent years. They are designed to help secure multi-cloud environments, which can be complex and difficult to manage. CNAPPs consolidate the capabilities of many security tools, such as Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP), Cloud Infrastructure Entitlement Management (CIEM), network security, and secure DevOps. By using CNAPPs, organizations can more easily protect their cloud-based applications and data from a wide range of threats — still, some questions regarding how organizations perceive these themes are unanswered.

And these are what Cloud Security Alliance (CSA) has attempted to answer in the Survey report: “Cloud Native Application Protection Platform Survey Report” released last August.

According to the report, the key takeaways are:

> - *3 out of 4 organizations use CNAPP to protect their multi-cloud environment.*
>
> - *32% of organizations are struggling with prioritizing security improvements due to the overwhelming and often incorrect information they receive from alerts.*
>
> - *51% of organizations are in the process of integrating security into their DevOps practices, with only 35% reporting complete integration.*
>
> - *Network security, out of all the categories, was most mature, with 43% of organizations reporting full integration in a multi-cloud environment for network security, compared to just 28% for CSPM.*
>
> - *Just under half (43%) of organizations identified misconfiguration of permissions as their top concern with cloud permissions in a multi-cloud environment.*

You can authenticate with CSA and download the full report here.

Microsoft mitigates exposure of internal information

A recent Coordinated Vulnerability Disclosure between Microsoft and Wiz.io resulted on the finding and report of internal information disclosure from Microsoft — and its mitigation.

According to Microsoft, throughout the whole process:

> ***No customer data was exposed, and no other internal services were put at risk because of this issue. No customer action is required in response to this issue.***

And they shared what and how they’ve worked to ensure this issue does not happen again.

So, what happened?

A Microsoft employee accidently shared a URL for a blob store in a Public GitHub repo for Open-source AI learning models. The URL contained over-permissive Shared Access Signature (SAS) token for an internal storage account. There was no vulnerability in the platform or the handling of the token by the platform. But Microsoft assured:

> ***“are making ongoing improvements to further harden the SAS token feature and continue to evaluate the service to bolster our secure-by-default posture.”***

Wasn’t it picked up by Continuous assessment?

Yes, but incorrectly flagged as false positive, the process has been reviewed to avoid this same issue in the future.

> *“Microsoft additionally performs complete historical rescans of all public repositories in Microsoft-owned or affiliated organizations and accounts. This system detected the specific SAS URL identified by Wiz in the ‘robust-models-transfer’ repo, but the finding was incorrectly marked as a false positive. The root cause issue for this has been fixed and the system is now confirmed to be detecting and properly reporting on all over-provisioned SAS tokens.”*

Lastly, in their post, Microsoft makes a few remarks on how to handle SAS tokens properly:

> *Apply the Principle of Least Privilege*
>
> *Use Short-Lived SAS*
>
> *Handle SAS Tokens Carefully*
>
> *Have a Revocation Plan*
>
> *Monitor and Audit Your Application*

Read the full report here.

Free eBook: Azure Defenses for Ransomware Attack

Microsoft published a Free eBook regarding Azure Defenses, specifically to Ransomware attacks, it covers:

> *“This eBook provides our customers with guidance on how to leverage our Azure cloud native controls to optimize their defenses against ransomware attacks.”*

Amongst some key info I saw in it, this graphic representation of industries that have been targeted by Ransomware:

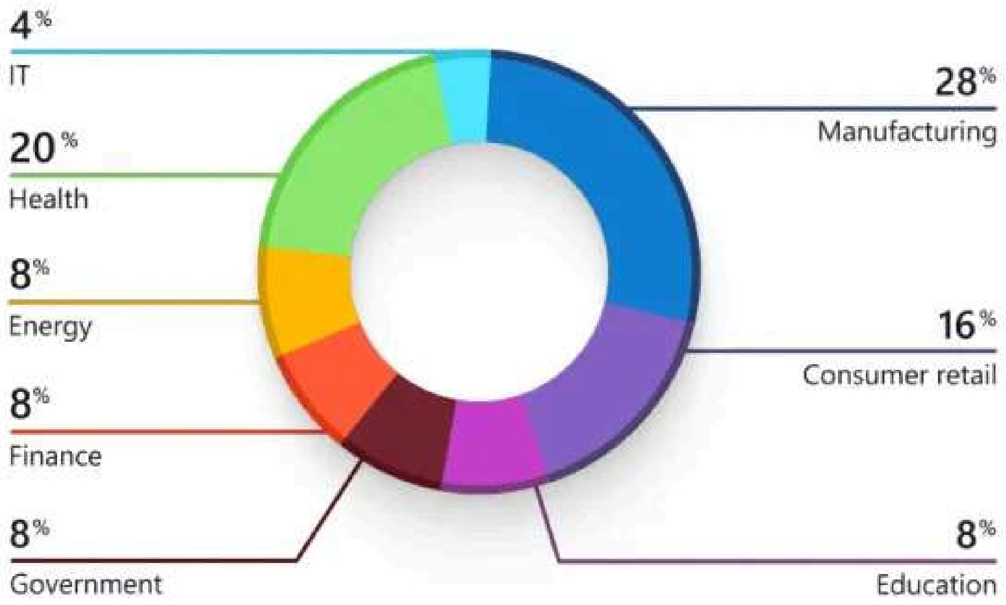


Figure 1: Percentage Distribution of Key Sectors Targeted in Recent Ransomware Attacks

Source, Microsoft Digital Defense Report 2022 & Azure Defenses eBook

Additionally, this representation of compromise techniques used in Ransomware attacks shows how different domains need to be crossed for a typical campaign:

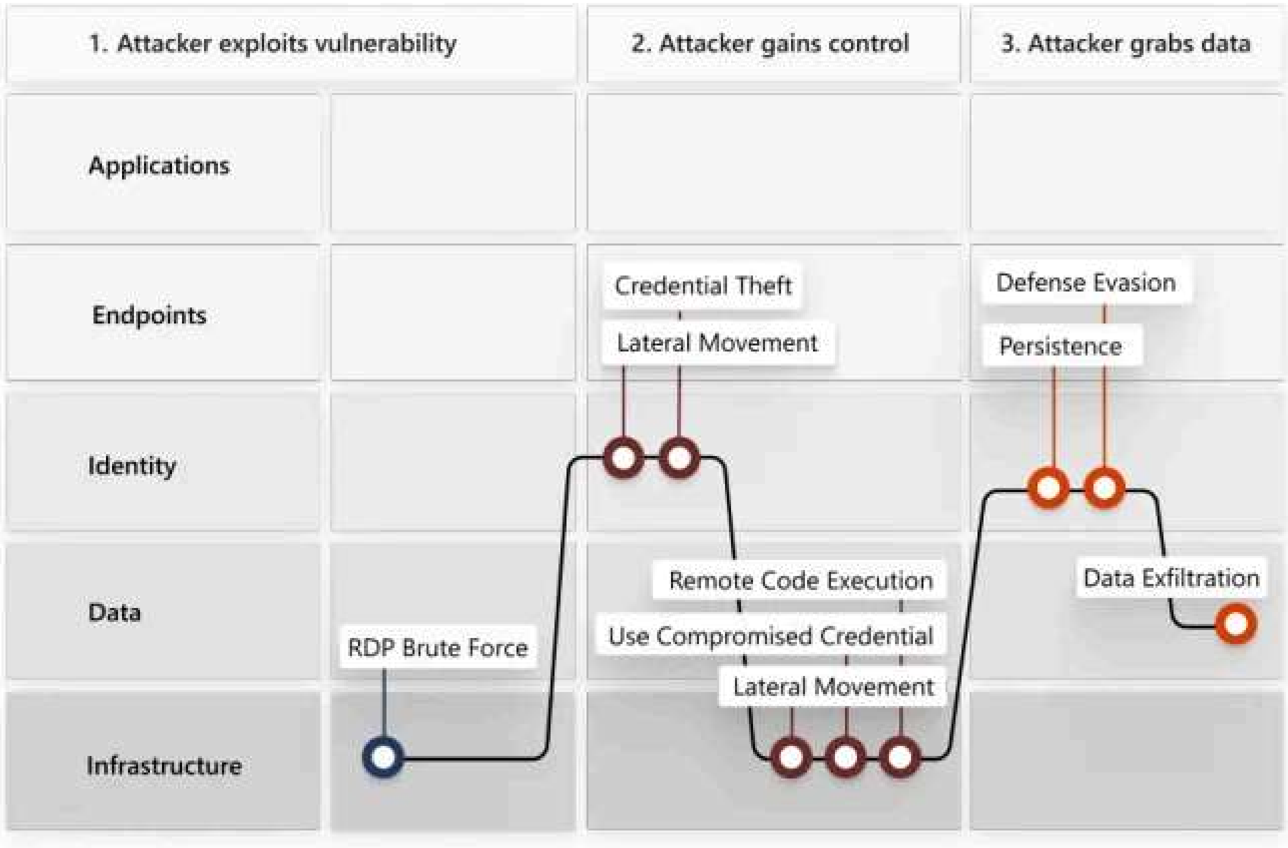


Figure 3: Ransomware Compromise Techniques

The report then goes on in details, how to utilize Azure configuration to mitigate and close potential gaps that would allow such compromises. A great reference for Cloud security engineers.

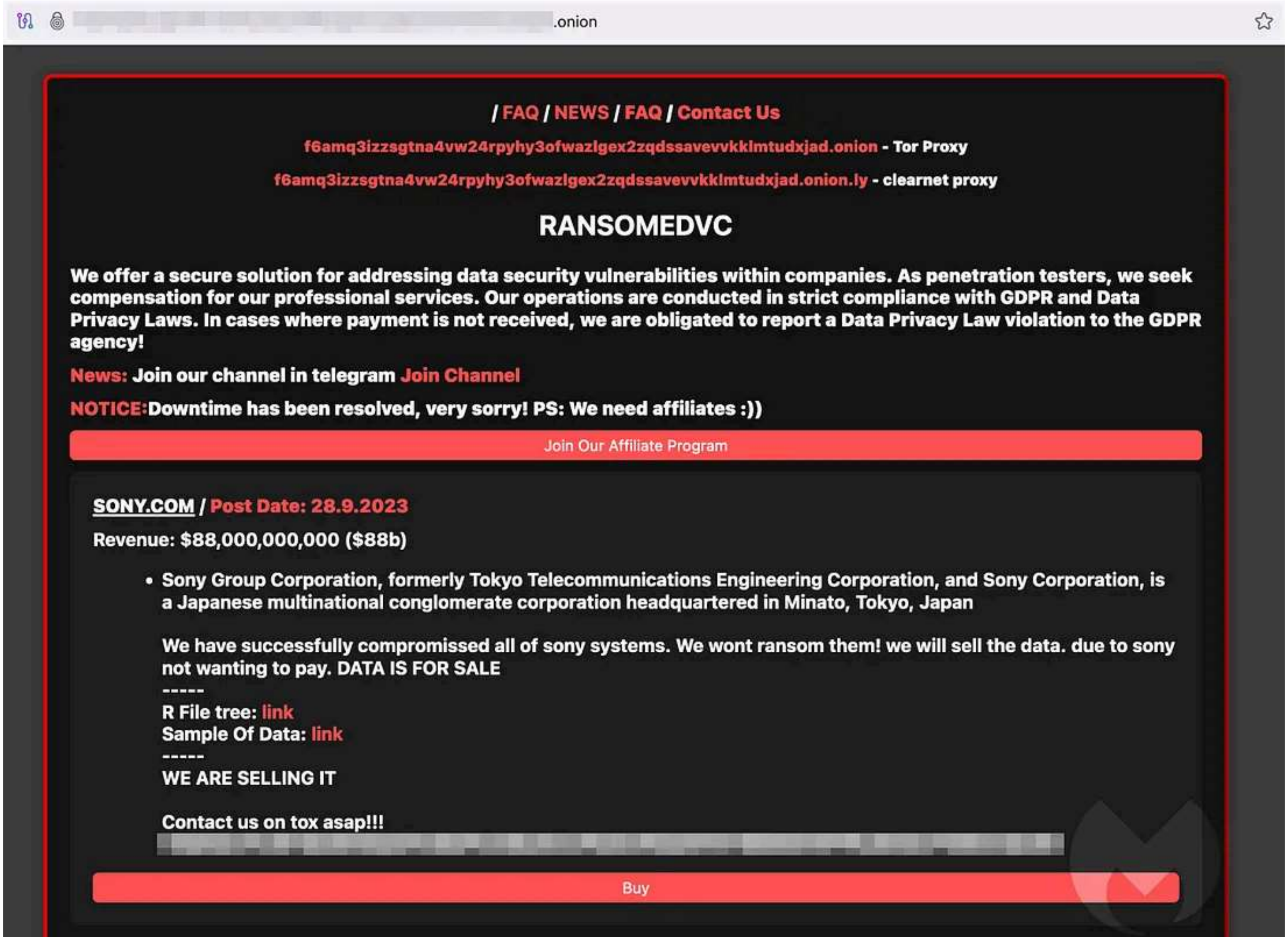
Download the eBook here.

Group claims to have hacked Sony

Late September, a new ransomware group claimed to have hacked Sony — details are scarce though, and Sony hasn't confirmed anything.

Days after initial claims, though, some unofficial details surfaced which clearly downsizes the whole impact and group claims… Details in Seytonic's video, here.

MalwareBytes’ blog, here, includes a snippet of the ransom note:



[redacted].onion

/ FAQ / NEWS / FAQ / Contact Us

f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion - Tor Proxy

f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion.ly - clearnet proxy

RANSOMEDVC

We offer a secure solution for addressing data security vulnerabilities within companies. As penetration testers, we seek compensation for our professional services. Our operations are conducted in strict compliance with GDPR and Data Privacy Laws. In cases where payment is not received, we are obligated to report a Data Privacy Law violation to the GDPR agency!

News: Join our channel in telegram Join Channel

NOTICE:Downtime has been resolved, very sorry! PS: We need affiliates :))

Join Our Affiliate Program

SONY.COM / Post Date: 28.9.2023

Revenue: $88,000,000,000 ($88b)

- Sony Group Corporation, formerly Tokyo Telecommunications Engineering Corporation, and Sony Corporation, is a Japanese multinational conglomerate corporation headquartered in Minato, Tokyo, Japan

  We have successfully compromissed all of sony systems. We wont ransom them! we will sell the data. due to sony not wanting to pay. DATA IS FOR SALE

  R File tree: link
  Sample Of Data: link

  WE ARE SELLING IT

  Contact us on tox asap!!!
  [redacted]

Buy

Source: Malwarebytes

What’s the impact?

Sony’s yet to pronounce themselves, but initial claims from the attackers state all Sony accounts have been compromised. Given their large customers sevices, though, it’s hard to actually tell what that means.

Let’s wait for official incident investigation details from Sony.

Who’s behind the hack?

According to Malwarebytes' blog:

> *"RansomedVC is a new ransomware group, first tracked by Malwarebytes in August 2023 after it published the details of nine victims on its dark web site. The only departure it makes from the usual cut 'n' paste criminality of ransomware groups is that it threatens to report victims for General Data Protection Regulation (GDPR) violations."*

This should come up again soon…

Process

Microsoft Investigation report

On September 6th, Microsoft released the technical investigation report for an incident involving a Chinese threat actor and Key acquisitions. This is part of Microsoft's:

> *"Commitment to transparency and trust, we are releasing our investigation findings."*

As their blog reports.

What happened?

Back in My 15th (as reported by Microsoft in the investigation report):

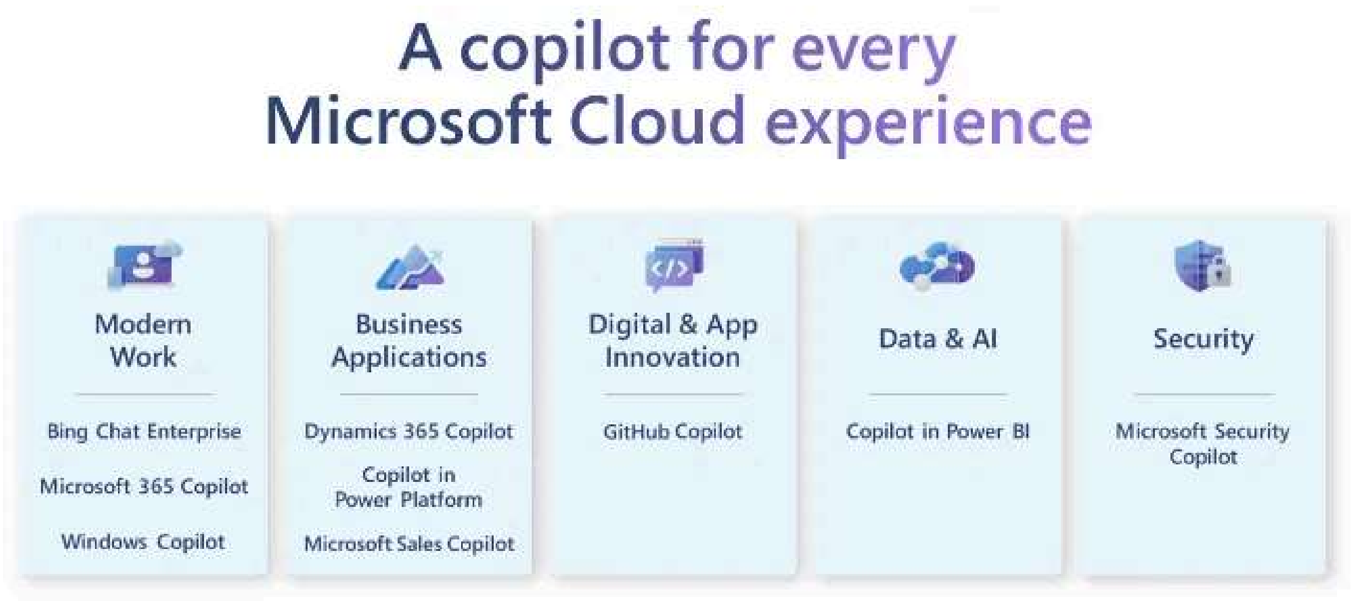
> *"the China-Based threat actor, Storm-0558, used an acquired Microsoft account (MSA) consumer key to forge tokens to access OWA and Outlook.com. Upon*

> *identifying that the threat actor had acquired the consumer key, Microsoft performed a comprehensive technical investigation into the acquisition of the Microsoft account consumer signing key, including how it was used to access enterprise email."*

Read the details and report blog post here.

Microsoft's Commitment to Copyright in AI

Data rights and ownership must be at the core of any new generative AI systems, and Microsoft has published their commitment to ensuring so — particularly important in a world of a "copilot" for anything.



A copilot for every Microsoft Cloud experience

Modern Work	Business Applications	Digital & App Innovation	Data & AI	Security
Bing Chat Enterprise	Dynamics 365 Copilot	GitHub Copilot	Copilot in Power BI	Microsoft Security Copilot
Microsoft 365 Copilot	Copilot in Power Platform			
Windows Copilot	Microsoft Sales Copilot			

source: Microsoft

As their official announcement states:

> *"As customers ask whether they can use Microsoft's Copilot services and the output they generate without worrying about copyright claims, we are providing a straightforward answer: yes, you can, and if you are challenged on copyright grounds, we will assume responsibility for the potential legal risks involved."*

This is an industry-first, a leading example of how tech giants should be going by using such technologies — especially in the wake and realization of impact of these technologies and a part of the workforce largely impacted by them.

Read more about it here.

MITRE Caldera(tm) for OT

MITRE recently announced the release of plugins for OT for Caldera.

It’s called MITRE Caldera(tm) for OT — which are all free and open source, following in line with the rest of the project.

It currently supports 29 OT abilities and protocols such as BACnet, Modbus, and DNP3.

Read more about it here.

Technology

Forrester Wave’s 2023 Zero Trust Platforms

Forrester published a new Wave of the Zero Trust Platforms, available publicly here: Forrester Reprint.

Amongst the information they published, I highly recommend you checking:

- The Actual Forrester Wave graphic

- The usual scoring of multiple vendors in various domains is incredibly useful.
- Figure 3, with the list of evaluated solutions from each vendor.

It’s no surprise that Microsoft, Palo Alto, Trend Micro are amongst the best scorers overall.

For a breakdown from Microsoft read their own post on the report, here.

2023 MITRE Engenuity ATT&CK Evaluations

MITRE Engenuity released their 2023 ATT&CK Evaluations for Enterprise solutions.

This years’ tests cover the threat actor dubbed “Turla”, as explained by MITRE, here.

> *“Turla is a Russian-based threat group that has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity was seen in mid-2015. Turla is known for conducting watering hole and spearphishing campaigns and leveraging in-house tools and malware. Turla’s espionage platform is mainly used against Windows machines, but has also been seen used against macOS and Linux machines.”*

Find the results from MITRE here.

Naturally, participants have come up with their own posts about their results, amongst the top performers, Microsoft, Crowdstrike and Palo alto.

Find their results posts here: Microsoft, Palo Alto.

Cisco Buys Splunk

It's been a while since I last caught up with Cisco's security technologies, almost 3 years away from it. On the 21st September, however, Cisco announced they're buying Splunk for roughly 28B USD in a combination of cash and debt.

It's a bold and interesting move from the traditional tech company.

Read more about it here.

Post-Quantum cryptography

This is an extremely important piece of news, thinking about the long-term side of data encryption, way beyond silicon-based processors. It's a future that isn't too far from us, according to developments from IBM and Microsoft in the quantum field…

Signal, the company behind the secure messaging platform, released a whitepaper describing an encryption protocol that shouuld cater for the adoption of Quantum. Called PQXDH — Post Qquantum eXtended Diffie-Hellman, they described it in their own document as:

> *"PQXDH establishes a shared secret key between two parties who mutually authenticate each other based on public keys. PQXDH provides post-quantum forward secrecy and a form of cryptographic deniability but still relies on the hardness of the discrete log problem for mutual authentication in this revision of the protocol."*

Definitely something to keep our eyes on.

Read the whitepaper here.

Appendix — Not so strategic, but Tactical

Free “For Dummies” book: Software Firewalls

Released by Palo alto, this edition of “for Dummies” covers Software firewalls which:

- Protect applications and
- Workloads

Throughout today’s complex and interrelated environments.

Find the download link and more 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.

News Report Cybersecurity Cloud Computing Microsoft

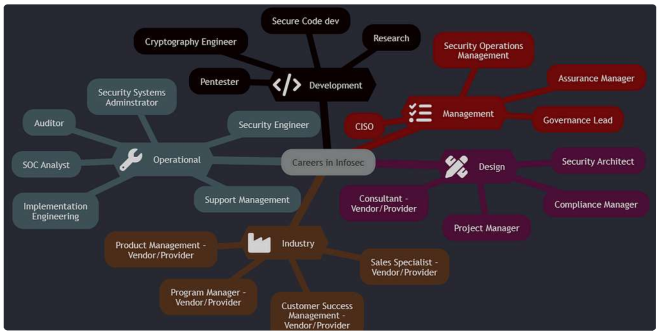
Written by Andre Camillo, CISSP

Edit profile

1K Followers · Editor for CloudnSec

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 CloudnSec



Secure Code dev
Cryptography Engineer
Research
Security Operations Management
Pentester
Development
Assurance Manager
Security Systems Administrator
Management
Auditor
Security Engineer
CISO
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...

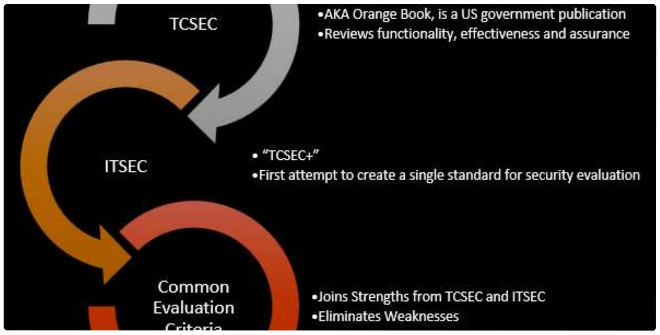
Feb 21 52 2

Andre Camillo, CISSP in CloudnSec

Microsoft Defender Threat Intelligence — All you need to get...

Since Microsoft Ignite 2023, Microsoft Defender Threat Intelligence has had a "Free...

Apr 5 21


TCSEC

•AKA Orange Book, is a US government publication
•Reviews functionality, effectiveness and assurance

ITSEC

• "TCSEC+"
•First attempt to create a single standard for security evaluation

Common Evaluation Criteria

•Joins Strengths from TCSEC and ITSEC
•Eliminates Weaknesses

Andre Camillo, CISSP in CloudnSec

Security Architecture & Evaluation Criteria Framework | CISSP Bits

The Common Criteria as a Global Standard for Cybersecurity

Feb 5 31 1

Andre Camillo, CISSP in CloudnSec

Microsoft Defender for Endpoint on Linux — Manual Scan Tips

Deploying and managing Defender for Endpoint on linux at Scale is something you'l...

Feb 14 154

See all from Andre Camillo, CISSP

See all from CloudnSec

Recommended from Medium