Strategic Cyber Security Report — October 2023 Edition

Andre Camillo, CISSP

Published in CloudnSec · 7 min read · Nov 4, 2023

140

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

Sony Confirms breach affecting almost 7000 employees

At the end of September, there were rumours of a data breach affecting Sony (I covered it last month).

And at the beginning of October so he has confirmed that the word getting in touch with current and former employees warning that their personal information was compromised but the system breach occurred in May they said.

The attack was claimed by the ransomware group Cl0p explointing a vulnerability on file transfer server called MOVEit. Sony was one of the many organisations affected by this cyber attacks against this platform.

What's striking to me here is that the provider of the softer informed Sony of the vulnerability on the 31st May, so than later Sony investigates and found the origin of the hack to have been on May 28th.

The impact however doesn’t seem to disrupt their operations despite might having affected nearly 7000 employee data terms of corporate data around three gigs of data was stolen and according to sunny no adverse impact once on the operations.

Read more about it here.

Genetics' data breached: 23andMe data breach

This is the complicated one so on October 6 the organisation part in confirms that user data had been stolen from its website user data including names use of birth and General description of genetic data.

Which complicates things that was that a few days later someone claiming to be the attacker and the hacker has posted data for millions of records on one forms according to Techcrunch.

Exposure through forms indicates that there has been a serious breach in Seishun systems however with complicates matters is that we can see schnitzel is not recognising all the public about a possible breach the order stating that the problem is this has been caused by people re-using passwords so think of password spray attacks which would have let hackers access personal data leveraging reuse passwords for all users other platforms my personal take on this is complicated due to gauge what's true and what's not until more information surfaced but it's very unlikely that hackers would've surfaced and attempted to re-use passwords of millions of people on their platform instead of exfiltrating data…

Read more about it here.

About 5000 Okta employees' data Breached by third party

So the problem here was that actor utilises the provider to find healthcare plans for its employees and their provider, called "Rightway" was breached.

About 5000 employees data including name and Social Security number might have impacted by this a breach.

This incident did not affect any of Okta’s customers or their data.

Read more about it here.

Process

NIST SP 800 82r3 — Guide to Operational Technology (OT) Security

This is one I believe will become a staple for OT secrutiy for years to come. A refresh of NISP SP 800–82 which covers the the basics of secure oppression of technology while addressing performance reliability and safety requirements of these systems.

What makes this document very compelling for summer security operators is how it provides overview of OTM typical system topologies it also identifies common threats in for the police assistance and provide recommended security counter measures to me to get risks unique set of direction for working with OT equipment.

Find the publication here: Guide to Operational Technology (OT) Security (nist.gov)

NSA and CISA Guidance on IAM

There's something I wasn't aware of Cesar and NSA work together to author documents aiming to address risks that threaten critical infrastructure and national security systems in the US they call this partnership ESF which stands for enduring security framework.

The publication that I want to bring over to you today was just released on the beginning of October and their address is best practices for admin's related to identity in excess management so I am they look to provide guidance stress technology gaps that limit adoption and secure employment of identity and access management technologies such as MFA and SSO.

The publication targets large organisations however the recommendations are applicable to smaller organisations making the document relevant to everyone in the industry. I highly recommend a read.

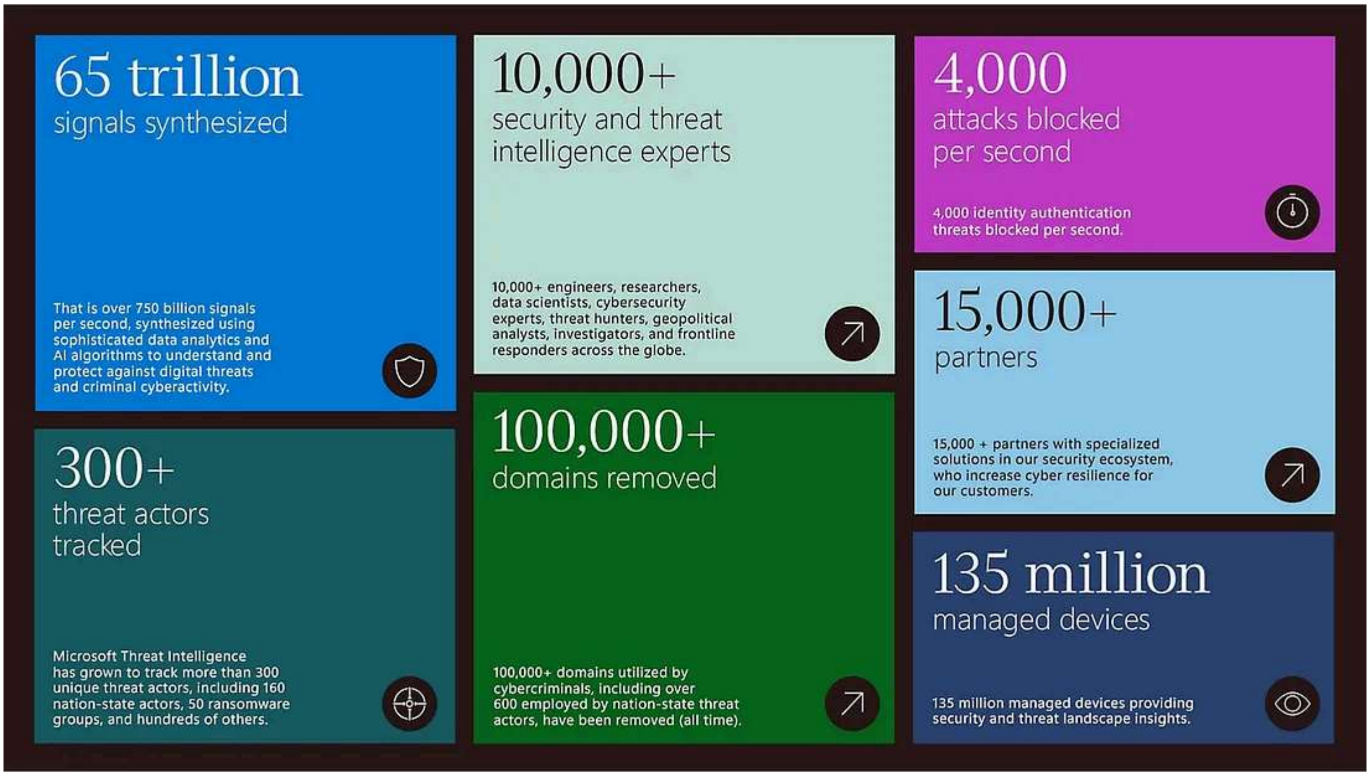
Find the official document here.

Microsoft Digital Defense Report 2023

Microsoft released their annual “Threat report”, called Digital Defense Report 2023. It covers findings from july 2022 until june 2023.

It’s 130 pages of useful and key insights from the frontlines.

The summary in the image below contains information around the reach of the threats analyzed, such as number of Signals synthesized, which are around 65 trillion; Average metric of Identity Authentication attacks blocked per second at 4000; Domains taken down in the house of +100,000 and more — check it out:



65 trillion
signals synthesized

That is over 750 billion signals per second, synthesized using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

300+
threat actors tracked

Microsoft Threat Intelligence has grown to track more than 300 unique threat actors, including 160 nation-state actors, 50 ransomware groups, and hundreds of others.

10,000+
security and threat intelligence experts

10,000+ engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across the globe.

100,000+
domains removed

100,000+ domains utilized by cybercriminals, including over 600 employed by nation-state threat actors, have been removed (all time).

4,000
attacks blocked per second

4,000 identity authentication threats blocked per second.

15,000+
partners

15,000 + partners with specialized solutions in our security ecosystem, who increase cyber resilience for our customers.

135 million
managed devices

135 million managed devices providing security and threat landscape insights.

More specifically speaking, Some of the highlights from the report, in my opinion, include:

- Amount of analyzed Signals, around 65 Trillion.
- Tracking of more then 300 Nation State threat actors
- OT/IoT Security: 78%
- **Basic Security Hygiene bell curve** (with its 5 key aspects) holds true to protecting against 99% of attacks.
- Key for defending — Using AI. Microsoft's approach for the Future of AI development follows **SD3** (Secure by Design + Secure by Default + Secure in Deployment)

Find the report here.

And if you want their own Video on the subject, they shared it here.

NIST Cybersecurity Log Management Planning Guide

The NIST SP 800–92r1 Initial Public Draft has been released. It covers Cybersecurity Log Management Planning Guide.

Commentary is open until November 29th, to log-mgmt@nist.gov.

This SP replaces the original SP 900–92 which encompasses Log Management — it was released in 2006, yeah, almost 20 years ago!

As stated by the publication, its goal:

> *"The main content of this publication is a playbook for cybersecurity log management planning. The playbook provides actionable steps that organizations can take to plan improvements to their log management practices in support of recommended practices and regulatory requirements."*

It's available here.

CISA, NSA, FBI, and MS-ISAC Release Phishing Prevention Guidance

The month has been packed with recommendations from major cyber security stations and this is yet a new one so this is guidance related to chew fishing prevention come in from CISA, NSA and FBI.

Their Recommendations to "All Organizations" include:

> *- Implement user training on social engineering and phishing attacks*
>
> *- Enable Domain-based Message Authentication, Reporting, and Conformance (DMARC) for received emails.*

> *- Ensure DMARC is set to "reject" for sent emails*
>
> *- Enable DMARC policies to lower the chance of cyber threat actors crafting emails that appear to come from your organization's domain(s).*
>
> *- Implement internal mail and messaging monitoring.*
>
> *- Implement free security tools, such as OpenDNS Home, to prevent cyber threat actors from redirecting users to malicious websites to steal their credentials.*
>
> *- Harden credentials by: Implementing FIDO or PKI-based MFA*
>
> *- Note: Deploying PKI-based MFA requires highly mature identity access and management programs and is not widely supported by commonly used services.*
>
> *- Prioritizing phishing-resistant MFA for administrator and privileged user accounts, such as those with access to e-discovery tools or broad access to customer or financial data.*
>
> *- Implementing centralized logins around a Single Sign On (SSO) program. SSO is a user lifecycle management mechanism that — among other benefits — can reduce the chance of users being socially engineered to give up their login credentials, especially when paired with MFA or phishing-resistant MFA.*
>
> *- Review MFA lockout and alert settings and track denied (or attempted) MFA logins.*

Access the guidance document here.

Technology

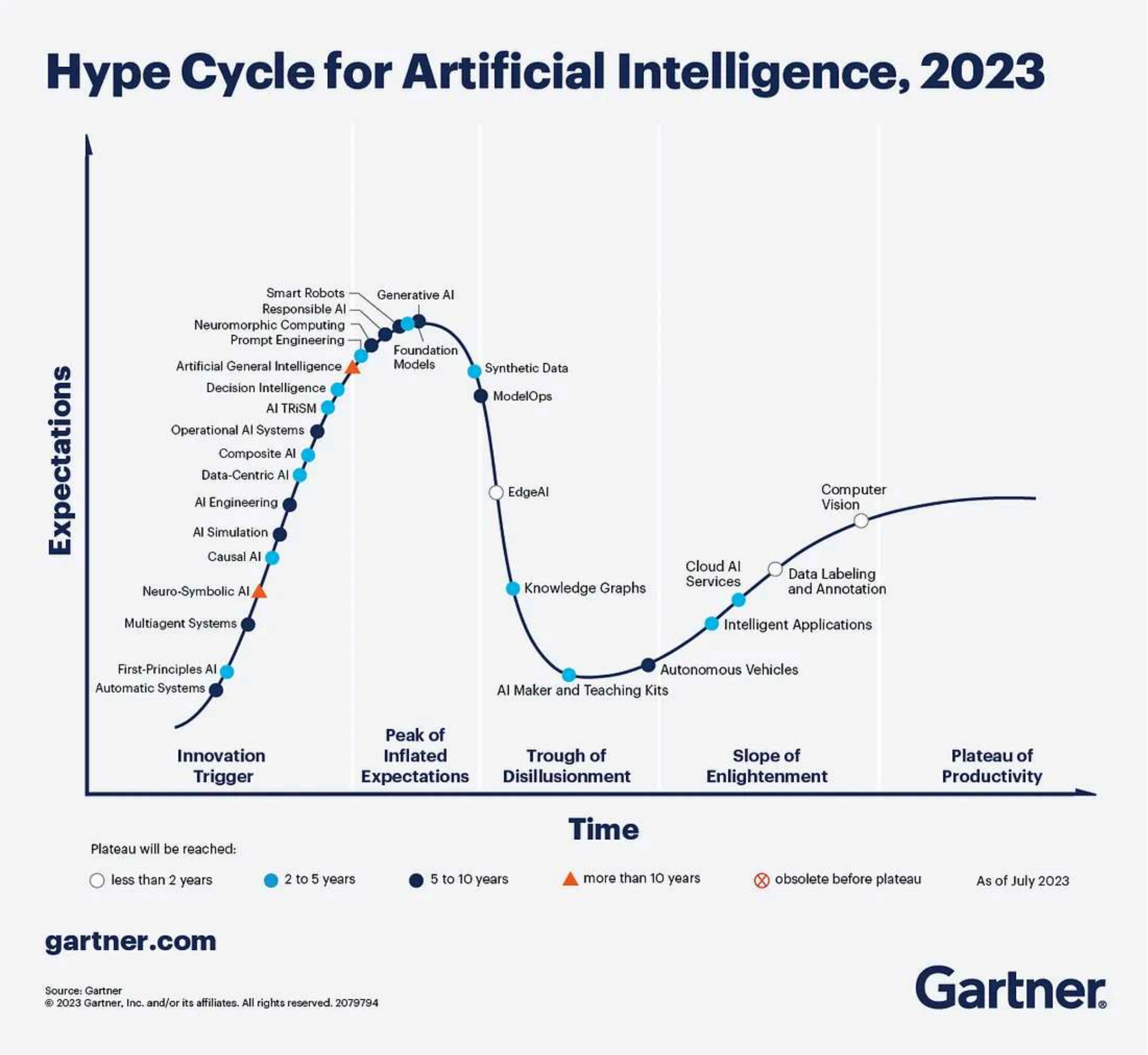
Gartner’s Hype Cycle for AI

Gardner released the hype cycle for special intelligence for the year 2023 this year is just a snapshot of what Gardner understands to be in terms of the development of the related technologies and services.

It was recommend taking this with a grain of salt but large organisations and executives will have their eyes on information from the Gardner so it's important we keep an ion why what they're telling us terms of how developed a given technology is or how popular it is at the moment and where we should expect it to go next in the life cycle.

Few highlights here would involve Vieira TV I quoted your Gardner it's a technology in its peak of inflated expectations which I would agree to be honest and it's also interesting seeing how computer vision is more mature.

What is really helps as with a horse is keeping an ion up-and-coming technologies so technology is there or about to hit its major peak or two hits really innovation trigger there so good reference for us to be aware of what's coming next.



Find the official release here.

Forrester Wave Endpoint Security Q4 2023

This is forest or waves and point security evaluation with the 13 providers that matter most in Q4 of 2023.

It's worth noting that this report focuses on "traditional" endpoint security, no Continuous monitoring with EDR, nor extended capabilities within XDR platforms.

Amongst the leaders of course Microsoft, Trend micro and Crowdstrike or make the list.

Find the report 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 Cybersecurity Report Strategy Hacking

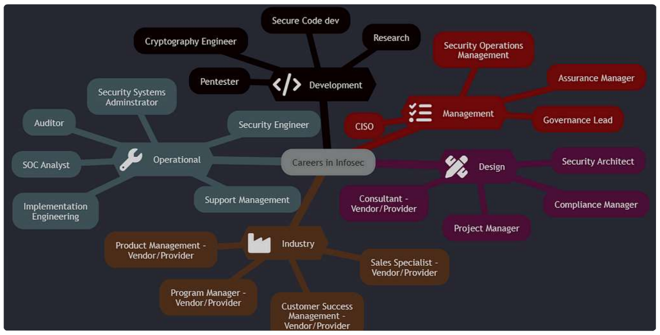
Written by Andre Camillo, CISSP

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 Adminstrator
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

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