Strategic Cyber Security Report — November 2023 Edition

Andre Camillo, CISSP

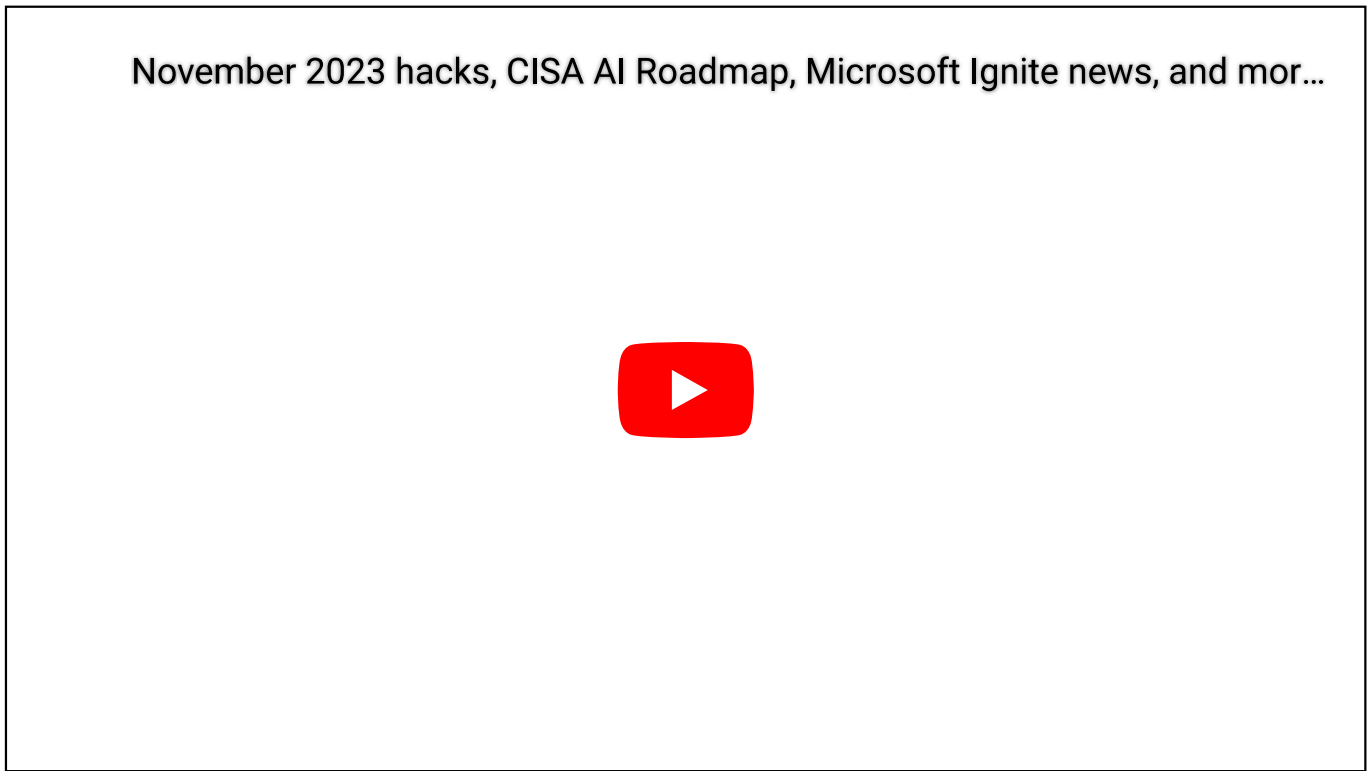
Published in CloudnSec · 8 min read · Dec 2, 2023

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.

And if you prefer to access this all in Video/Audio, you can find it in Youtube and Spotify:



People

Major Optus Outage

At the beginning of the month of november, Optus Au's customers experienced a massive outage impacting businesses and individuals.

The impact spread from mobile phones lines to internet, banking, hospital and public transport services for more than 12 hours last week.

And the cause was disclosed a few days later... but first, the reports from its impact, which according to abc.net.au :

> *"CEO of the Cyber Security Cooperative Research Centre, Rachael Falk, has echoed engineers and digital security experts in saying that today's outage exposed how vulnerable Australian telcos are"*

This could cause reputational damage, a Marketing expert highlighted — according to the same report above:

> *Australian National University marketing expert Dr Andrew Hughes says this latest incident could do even more damage.*

Getting back to the cause, it was all caused by changes to routing information in their network, an infromation disclosed a little later.

Hopefully the streak of similar news ceases for Optus' customers.

Toyota confirmed hack

A subsidiary of Toyota Motor Corporation detected malicious activity in some of their systems across Europe and Africa. Medusa Ransomware claimed the attack, as reported by Bleeping computer:

> *"Toyota Financial Services (TFS) has confirmed that it detected unauthorized access on some of its systems in Europe and Africa after Medusa ransomware claimed an attack on the company.*
>
> *Toyota Financial Services, a subsidiary of Toyota Motor Corporation, is a global entity with a presence in 90% of the markets where Toyota sells its cars, providing auto financing to its customers."*

Alledgedly, data was stolen and a ransom of 8M USD was posted on the dark web, asked to delete the data.

The victim did not confirm whether data was stolen, but made a public announcement that operations were being restored at the time of reporting by Bleeping computer.

It's not the first time the Toyota group is hit by cyber threats, with ocurrences happening in 2022, 2021 and 2019, with supply chain breaches being the reason on more than one of these occasions.

Major Logistics provider Hacked in Australia

DP World, a major port and logistics provider in Australia was hit by threat actors. As reported by the Register:

> *"DP World's tech go offline at four Australian ports late last Friday. The facilities remain closed at the time of writing.*
>
> *The major logistics provider handles 40 percent of the containers coming into Australia's ports"*

Other reports by Financial Review detail the impact of data tampered with:

> *"In an update on Tuesday, DP World said some personal information of current and former employees in Australia had been stolen in the early November hack, but client information had not."*

And according to the same report, the breach was caused due to unpatched, publicly-known vulnerability exploited by a russian threat actor.

Australia Home Affairs Miniter stated:

> *"A known problem, with a known patch — Australia needs to do better than this," she said. "Our nation just won't have a cyber secure future if this continues."*

Let us remember that Australia has made the headlines recently with financial investment announcements to its cyber security programs, which proves that important than big investments is to start with the basics of good cyber security hygiene.

Process

MITRE and Microsoft collaboration evolution on Atlas

MITRE and Microsoft announced more capabilities to Atlas, a threat-focused framework for AI systems.

According to the post by MITRE:

> *"Microsoft and MITRE worked with the ATLAS community to launch the first version of the ATLAS framework for tabulating attacks on AI systems in 2020, and ever since, it has become the de facto Rosetta Stone for security professionals to*

> *make sense of this ever-shifting AI security space," said Ram Shankar Siva Kumar, Microsoft data cowboy. "Today's latest ATLAS evolution to include more LLM attacks and case studies underscores the framework's incredible relevance and utility."*

Read about it here.

Solarwinds and CISO charged by SEC

The Securities and Exchange commision charged Solarwinds and Timothy Brown (CISO) for fraud and internal control failures their actions between 2018 and 2020, just before Solarwinds was hit by the massive attack that was dubbed "SUNBURST". According to the plaintiff (SEC) the defedants to the charge have actively (SolarWinds Corporation and Timothy G. Brown (sec.gov)):

> *"(Solarwinds and Brown) defrauded SolarWinds' investors and customers through misstatements, omissions, and schemes that concealed both the Company's poor cybersecurity practices and its heightened — and increasing — cybersecurity risks"*

It will be interesting to see the developments and impact of such an (unprecendent?) case.

According to CSO online:

> *"It is unusual for a company CISO to be named in SEC charges for non-disclosure. The SolarWinds case could act as a pivotal point for the role of a CISO, transforming it into one that requires a lot more scrutiny and responsibility."*

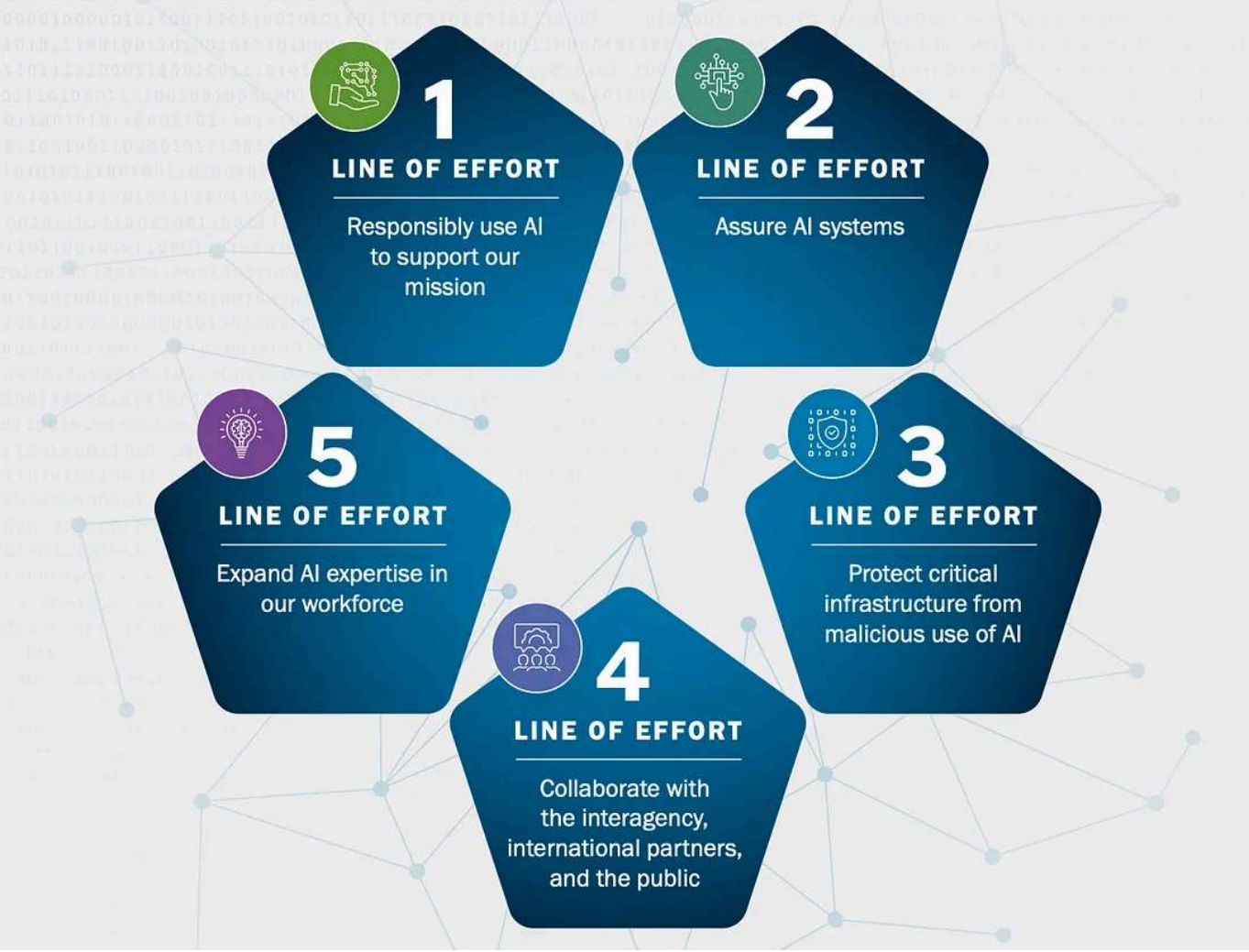
Read the full announcement by SEC, here.

CISA's Roadmap for AI

CISA has released it's guidance for AI adoption, according to the agency:

> *"CISA has developed a Roadmap for AI, a whole-of-agency plan aligned with national AI strategy, to address our efforts to: promote the beneficial uses of AI to enhance cybersecurity capabilities, ensure AI systems are protected from cyber-based threats, and deter the malicious use of AI capabilities to threaten the critical infrastructure Americans rely on every day."*

The roadmap encompasses 5 Line of Efforts that they'll take towards Securing AI:



- LoE 1: Response Use of AI
- LoE 2: Assure AI systems
- LoE 3: Protect Infra from Malicious use of AI
- LoE 4: Collaborate (with Agencies/International partners/public)
- LoE 5: Expand AI expertise in workforce

The take from these efforts to the wider cyber security community is the clear focus on AI security and how organizations are tackling their strategy.

Check out this link for the file.

NIST releases IR 8496 for Data Classification

NIST released IR 8496 for Data Classification Concepts and Considerations for Improving Data Protection for Public comment:

> *"The NIST National Cybersecurity Center of Excellence (NCCoE) has released for public comment Draft NIST Internal Report (NIST IR) 8496,* Data Classification Concepts and Considerations for Improving Data Protection. *The comment period is open now through* ***January*** *9, 2024."*

The publication, according to NIST:

> *"defines basic terminology and explains fundamental concepts in data classification so there is a common language for all to use. It can also help organizations improve the quality and efficiency of their data protection approaches by becoming more aware of data classification considerations and taking them into account in business and mission use cases, such as secure data*

> *sharing, compliance reporting and monitoring, zero-trust architecture, and large language models."*

The document can be found here.

CISA Mitigation guide for: Healthcare and Public Health (HPH) Sector

Imagine a mitigation guide specifically tailored for Healthcare and Public Health sector, now imagine it being created by CISA, this is what we got here. 😄

According to the announcement from CISA:

> *"This Cybersecurity and Infrastructure Security Agency (CISA) Mitigation Guide offers recommendations and best practices to combat pervasive cyber threats affecting the Healthcare and Public Health (HPH) Sector. CISA developed this guide as a supplemental companion to the HPH Cyber Risk Summary distributed to HPH organizations in July 2023"*

The Guide includes strategies for these core domains:

- Asset Management and Security
- Identity Management and Device security
- Vulnerability, patch and Configuration Management.
- Secure By design

Find the document here.

Technology

Microsoft Ignite 2023 Security Highlights

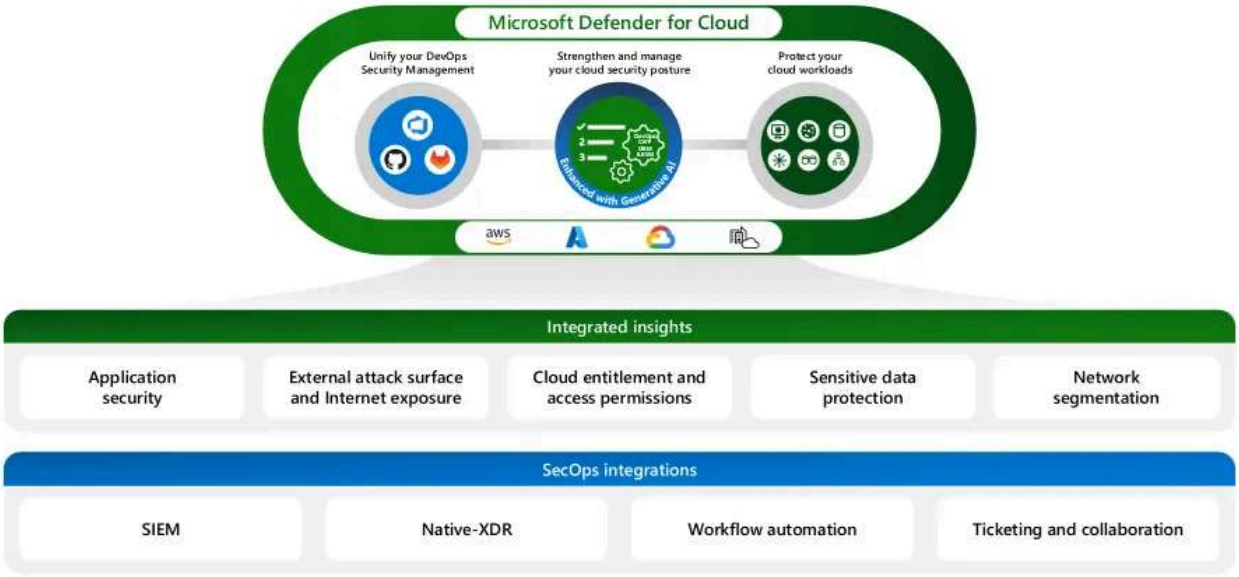
Microsoft hosted its annual “Ignite” conference this month and a raft of announcements ensued.

In the Security , Identity and Data Governance/protection fronts, some of the highlights for me include:

Security:

- M365 Defender is now called Defender XDR
- Security Copilot “skills” for EASM, Entra ID, Purview and more
- Security Copilot embbeded into many portal.
- Defender XDR + SIEM Unified portal (plus Security copilot embbeded)
- Deception capabilities in Defender for Endpoint

Defender for Cloud news.



- More features announced that cement Defender for cloud as a CNAPP solution, including:
- Entra Permissions management in Defender for Cloud recommendations
- API security plan.
- DevOps protection capabilities included in the Solution.
- Multicloud attack path analysis

Purview:

- Visibility of purview alerts from security copilot.
- DLP Alerts now get Insider Risk Management enrichment

Entra:

- Entra Private Access full VPN replacement for full ZTNA capabilities
- MFA to all on-premises apps
- Entra Internet Access expand its preview to include context-aware Secure Web Gateway (SWG) capabilities for all internet apps and resources

You can find the Book of News here.

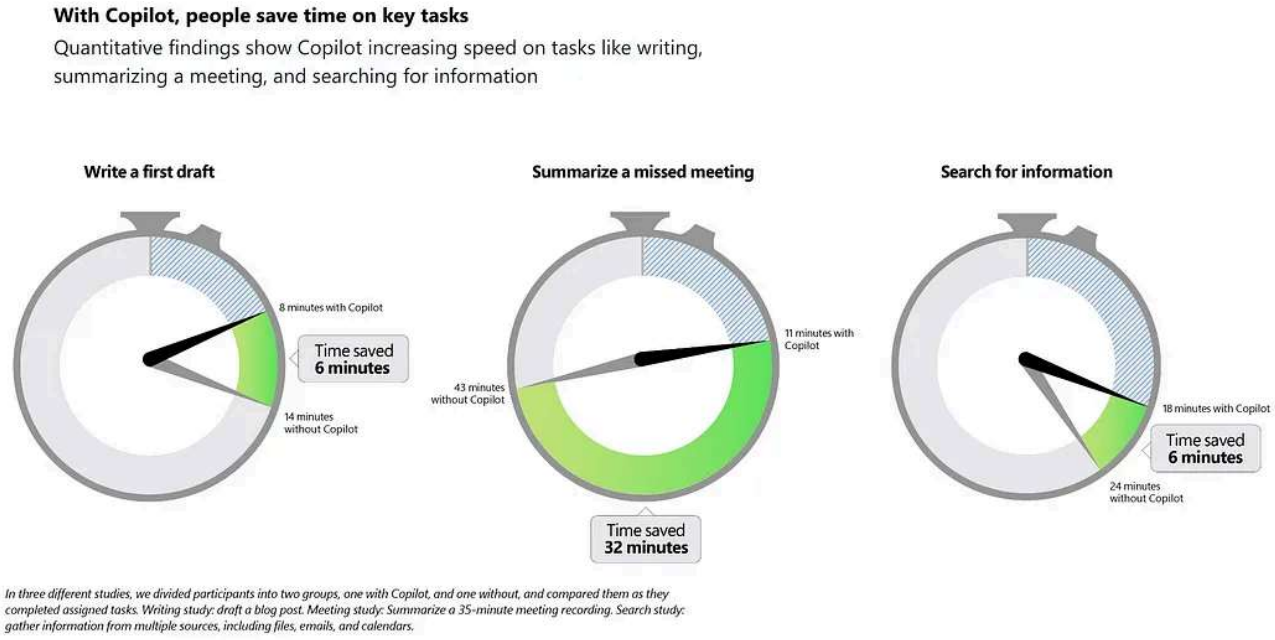
And if you want a general overview of everything announced for Defender XDR, Defender for Cloud, Sentinel, Entra check out my video, here:

Copilot produtivity evidence report

According to the research, here are the highlights:

> *70% of Copilot users said they were more productive, and 68% said it improved the quality of their work.*
>
> *Overall, users were 29% faster in a series of tasks (searching, writing, and summarizing).*
>
> *Users were able to get caught up on a missed meeting nearly 4x faster.*
>
> *64% of users said Copilot helps them spend less time processing email.*
>
> *85% of users said Copilot helps them get to a good first draft faster.*
>
> *75% of users said Copilot "saves me time by finding whatever I need in my files."*
>
> *77% of users said once they used Copilot, they didn't want to give it up.*

And in my experience, I can 100% vouch for massive gains in the last 2 of these themes — **Summarize missed meeting** and **Search for information:**



Access the report here.

Apple devices vulnerable to serious “iLeakage” vulnerability

In Early november Apple users were notified of a serious vulnerability found in Apple-silicon, which relies on “Speculative Execution” to process code quicker.

The Vulnerability affects Safari Browser in iOS and Mac OS — and it allows hackers to read all the content in a page, even if it’s a legitimate page. All they need is for the page to be open in Safari, so they can read emails and even password in “hidden” fields.

Initial reports stated that Apple had known of this vulnerability for about a year, before research and paper were made available and they provided an initial mitigation, but not an actual patch… as stated by this outlet:

> *“Apple has implemented a mitigation for iLeakage in Safari. However, it’s not enabled by default and enabling it is possible only on macOS. Added to the mix is that the mitigation is currently marked as unstable.”*

Read more about it 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 News 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