

Member-only story

Strategic Cyber Security Report — March 2023 Edition



Andre Camillo, CISSP

Published in Geek Culture · 9 min read · Apr 3, 2023



4



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

Latitude Hacked — 300k+ customers data leaked.

Major Australian financial company Latitude has been hacked, with over 328,000 customers affected, including their drivers' license information.

The report by news.com.au mentions:

ASX-listed Latitude, which provides credit cards to thousands of Australians, announced on Thursday morning that it has been targeted in a “sophisticated and malicious cyber-attack”.

“The attacker appears to have used the employee login credentials to steal personal information that was held by two other service providers,” the company said in a statement to the ASX.

“Latitude apologises to the impacted customers and is taking immediate steps to contact them,” the statement added.

They provide services to major retailers and as this enters the supply chain hack category...

News.com.au [reported it here](#).

Palo Alto Networks' 2023 Cloud Native Security Report

One of the cyber security leaders has released their latest report, this one for Cloud Native Security. It's a follow up to 2020, 2022 editions.

In it, they surveyed more than 2 thousand people “representing both executive leadership and practitioners in security and DevOps roles”.

These organizations range from a number of different industries across 7 countries.

The report answers to the open-ended question:

What challenges are you facing in cloud-native security, and what strategies and solutions are helping you achieve your desired outcomes?

From an operation perspective, Cloud Native is top of mind to these customers, many committing new code and deploying with more frequency. Some of the numbers according to the report:



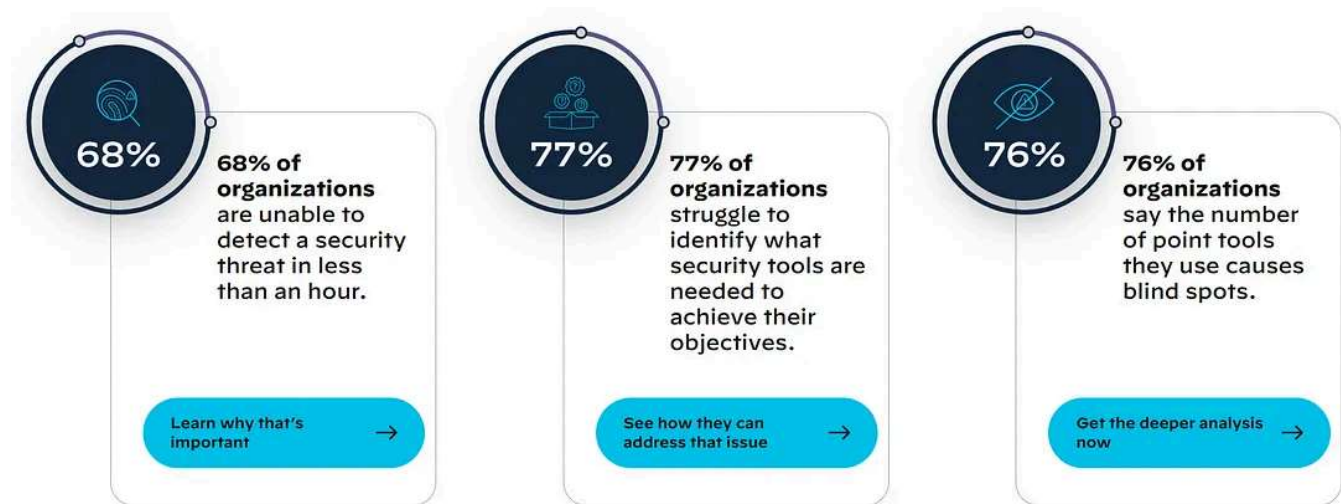
Source: [2023 Cloud Native Security Report](#) — Palo Alto Networks

Also, In this front, security is still a challenge to many, with more than half organizations being unable to detect security threats in less than an hour (which if we cross reference reports from other vendors that indicate attackers are taking little more than an hour to move laterally or escalate privileges in some scenarios, is extremely worrying).

More than 3 quarters:

- struggle to identify what security tools are needed to achieve their objectives and;
- say point tools causes blind spots (leading to solutions with broader coverage).

Some numbers from the report on this indicate:



Source: [2023 Cloud Native Security Report — Palo Alto Networks](#)

The Full report can be [found here](#).

Crowdstrike's 2023 Global Threat Report

Crowdstrike released their Global Threat report, and some surprising metrics are shared in their report.

Corroborating with other vendor's reports (Microsoft's Digital Defense Report) of the past year, the amount of time it took adversaries to start acting after entry was a little more than an hour — 84 minutes to be precise, according to the report.

They added that almost 3 quarters of attacks were malware-free — according to the report.

In another note, also in line with what other vendors have seen, the use of access brokers in the cybercrime space has greatly increased, this is part of “Cybercrime as a Service” — or services sold in the dark web.

IMO — It's unsurprising to see cloud exploitation rising, as so does cloud consumption, it's expected to see the battleground transition to this new fabric of enterprises/businesses.

Lastly, they mention that a Nation State threat actor has been especially active in the period. Wonder what the reasons would be around this... Just look at geopolitical tensions to get some ideas — that's my tip.



source: [2023 Global Threat Report | CrowdStrike](#)

Their report can be [found here](#).

Process

CISO Lens 2023 Benchmark

CISO lens is an Australian organization dedicated to reports of cyber security leaders from all around the globe.

Amongst the findings:

- Increased budget in all industries for Cyber Security
- They measured the number of women in teams (slide 12)
- Top 5 priorities changed from 2020 to this year, with Identity and Access Management taking first spot.

Rank	2020 Benchmark	2022 Benchmark
1	Maturing existing capability	Identity and access management
2	Uplifting capability	Maturing existing capability
3	Identity and access management	Vulnerability management
4	Cloud	Uplifting capability
5	Awareness and engagement	Cloud

source: [Benchmark \(cisolens.com\)](https://www.cisolens.com/benchmark)

The report can be found [here](#).

USA National Cybersecurity Strategy 2023

A lot has been said over the last week about the USA's national cybersecurity strategy 2023 released on the march 1st.

The document is a great read — as it highlights the importance of many topics we often discuss in our daily lives in the industry — but from the unique perspective of a leading country in the world.

The document expresses the 5 pillars of the 2023 Cybersecurity strategy:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

As you can see, **resilience** is top of mind.

Whilst I will strive to read it thoroughly, the start I recommend to most is to read [this fact sheet](#), issued by the white house, a “TL; DR” of some kind to this actual full document.

It's important to note the full Strategy document can also be found through the page above.

Technology

Gartner's Magic Quadrant for EPP 2022

Gartner released its Endpoint Protection platform magic quadrant — [a summary of it available here](#). The report looks at:

Endpoint protection platforms (EPPs) provide the facility to deploy agents or sensors to secure managed endpoints, including desktop PCs, laptop PCs, servers and mobile devices.

EPPs are designed to prevent a range of known and unknown malicious attacks. In addition, they provide the ability to investigate and remediate any incidents that evade protection controls.

Very Important to point out that EPPs are modern platforms, looking at capabilities that can hinder and stop the most hideous threats out there — I often talk to customers about EPPs and there's misconception about what they can provide in terms of protection against modern threats...

Microsoft announced it in a blog post given its leadership (once again).

Figure 1: Magic Quadrant for Endpoint Protection Platforms



Source: Gartner (December 2022)

According to the blog post: Microsoft has introduced several innovations in the past 12 months to help organizations protect their endpoints:

- Microsoft 365 Defender portal, which offers a unified security experience for endpoints, email, identities, and SaaS applications. It empowers

defenders by combining endpoint, identity, email, and cloud app security products into an end-to-end XDR solution.

- Multi-platform Microsoft Defender for Endpoint: Endpoint security solution for all platforms, including Windows, Linux, macOS, Android, and iOS.
- Introduced simplified endpoint security configuration and management experiences, including Microsoft Defender for Business, which offers small business customers a streamlined way to protect their organizations, and a new alert suppression experience that saves IT and security teams countless hours of manual tasking.

Read more about [this here](#).

SE Labs annual Report 2023



SE Labs (a private, independently-owned and run testing company that assesses security products and services) has released their Annual Threat Intelligence Report — AND its Security Awards for 2023.

Highlights of their TI report:

Their source is mentioned in the footprint:

Data shown here is representative of that reported to us by clients and found in reports such as the Verizon Data

Breach Report 2022, UK government statistics and other, smaller surveys from reputable sources

According to their report:

For every \$1 we spend on protection, cyber criminals make \$40. But there is hope

- Access to targets is sold for less than USD1 by criminals
- One third of breaches involve malware
- Email phishing behind 20% of breaches

Highlights of their Security awards:

- Email Protection Service: Microsoft
- Enterprise Endpoint: Broadcom
- Next Generation Firewall: Cisco
- Endpoint Detection and Response: Crowdstrike

Both can be [found here](#).

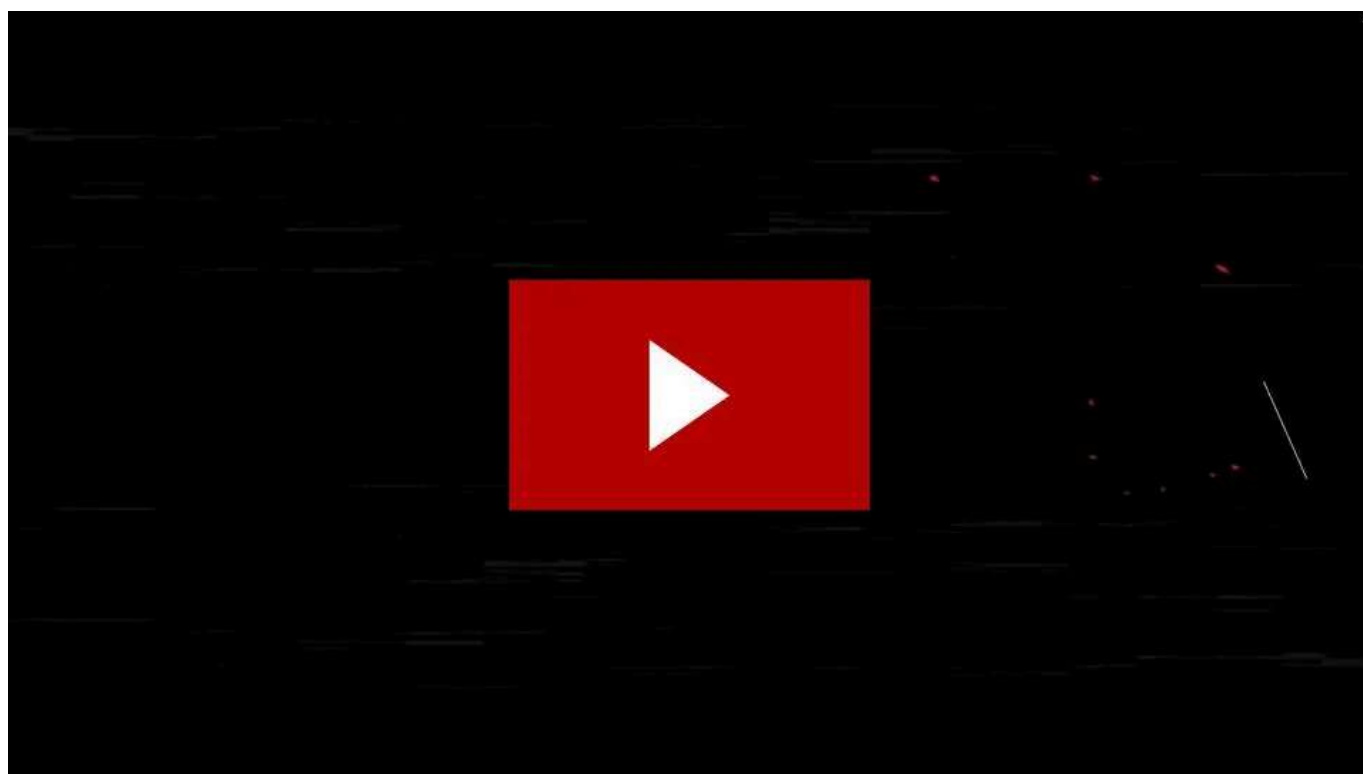
Red Canary Threat Report



Red Canary released its 2023 Threat report this month. According to them, the report:

is based on in-depth analysis of nearly 40,000 threats detected across our 800+ customers' endpoints, networks, cloud workloads, identities, and SaaS applications over the past year.

Their video about the report is really instructive:



Source: [Welcome to the Red Canary 2023 Threat Detection Report](#)

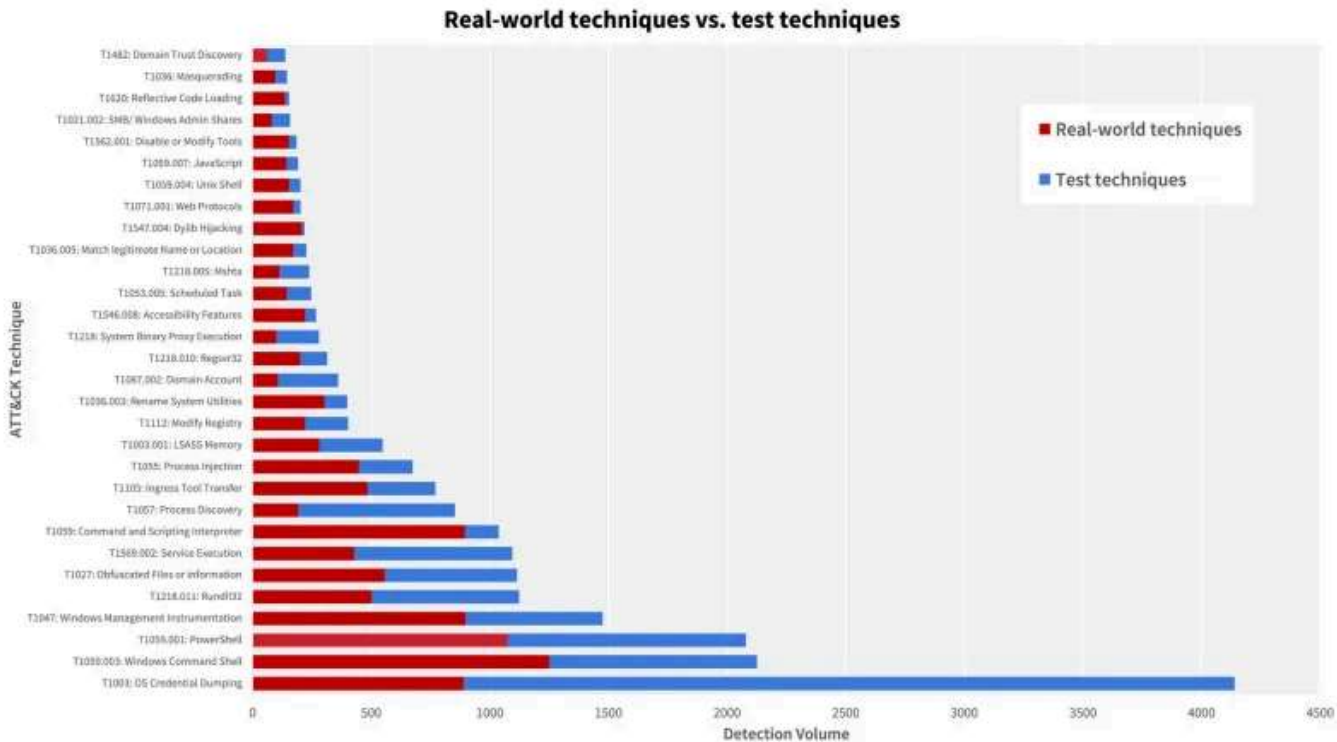
Essentially, the report looks at Windows/Linux/Mac OS across Network/Cloud/On-prem threats — and a lot more.

Plus, personal shout out to its designers — the report looks slick with red canaries all around (I'm a big fan of canaries this being the mascot of the

Brazilian football squad 😊).

What’s striking from this report is its focus (more than half of its 111 pages dedicated TTPs — and how to simulate and prepare for these kinds of attacks — it’s a really technical report).

The below is an excerpt from it, detailing Real-world vs Test techniques that they observed — the outcome from this chart is that defenders are somewhat testing for the right TTPs.



The most prominent Threat observed by team at Red Canary was Qbot:

Also known as “Qakbot,” the Qbot banking trojan has been active since at least 2007. Initially focused on stealing user data and banking credentials, Qbot’s functionality has expanded to incorporate features such as follow-on payload delivery, command and control (C2) infrastructure, and anti-analysis capabilities. Qbot is typically delivered via an email-based distribution model, and in 2022

Qbot affiliates experimented with a variety of file types to deliver malicious payloads during their campaigns, likely in response to additional security controls implemented by Microsoft throughout the year.

And the most used technique by threats was Windows Command Shell T1059.003:

The native command-line interpreter (CLI) across every version of the Windows operating system. As utilitarian as it is ubiquitous, Windows Command Shell is one of the primary ways that adversaries interact with compromised systems. Unlike its more sophisticated and capable cousin, PowerShell, Windows Command Shell's native feature set — i.e., commands that may be invoked without starting a new process on the system — is limited, having remained constant for years or even decades. Despite its limitations, an adversary can abuse Windows Command Shell to call on virtually any executable, making it an extremely versatile tool.

What I haven't seen in the report was an Impact assessment of Techniques which would be perhaps the better way to assess what to focus on.

But when we use the MITRE ATT&CK framework properly we can find the TTPs vs Threats and this is overlooked, no doubt.

Re(a)d the [full report here](#).

Forrester Wave for Data Security 2023 released

As a result of Microsoft's multi-year efforts and development of its Data Security and Compliance portfolio, Forrester Wave's Data Security 2023 has acknowledged it's platform leadership role in the segment.

According to Microsoft's post on the subject:

I am delighted to announce that Forrester listed Microsoft as a Leader in its 2023 Wave™ for Data Security Platforms. The Forrester Wave™ report evaluates the data security platform market and provides a detailed overview of the current offering, strategy, and market presence of these vendors. Microsoft received the highest possible score in the current offering category for data classification, data threat and risk visibility, data masking or redaction, encryption, rights management, privacy use cases, and integrations for Zero Trust criteria; and in the strategy category for the product vision, execution roadmap, and community engagement criteria.

In their post, they published the Wave graphic:

FIGURE 1

Forrester Wave™: Data Security Platforms, Q1 2023

THE FORRESTER WAVE™

Data Security Platforms

Q1 2023



*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Access Microsoft's blog — and the wave 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

Cybersecurity

Report

Strategy

Cloud

Industry

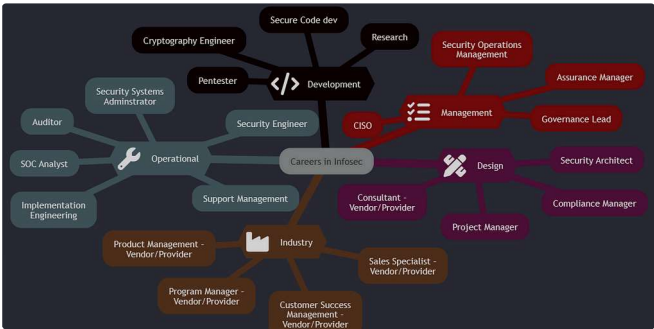



Written by Andre Camillo, CISSP

Edit profile

1K Followers · Writer for Geek Culture

More from Andre Camillo, CISSP and Geek Culture

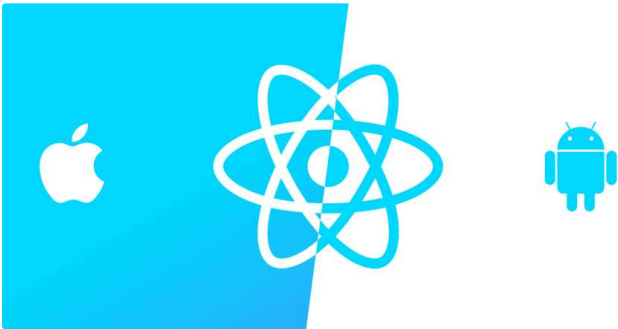


 Andre Camillo, CISSP in CloudnSec

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 📌 ⋮




 Anshul Borawake in Geek Culture

React Native Generate APK— Debug and Release APK

Generate Debug and Release APK in React Native; Windows, iOS and Linux

Apr 4, 2021 🖱️ 1.8K 💬 11 📌 ⋮




 Masud Afsar in Geek Culture

How to install Node.js by NVM?

Install and manage multiple versions of Node.js with nvm



 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...