Clusit Associazione Italiana per la Sicurezza Informatica

ASTREA Advanced Security, Training Research, Events Agency

SECURITY SUMMIT

Security Summit

Roma, 19 giugno 2024

# Intelligence report:
# nuovi vettori di attacco e modelli di business del Cybercrime

**Alessio Pennasilico** | CS Clusit
**Marco Lucchina** | Country Manager Italy, Cynet

12.20-13.00 – 19 giugno 2024

# Alessio Pennasilico

Partner, Practice Leader Information & Cyber Security Advisory Team
Security Evangelist & Ethical Hacker

Membro del Comitato Scientifico

Membro del Comitato Direttivo di Informatici Professionisti

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità

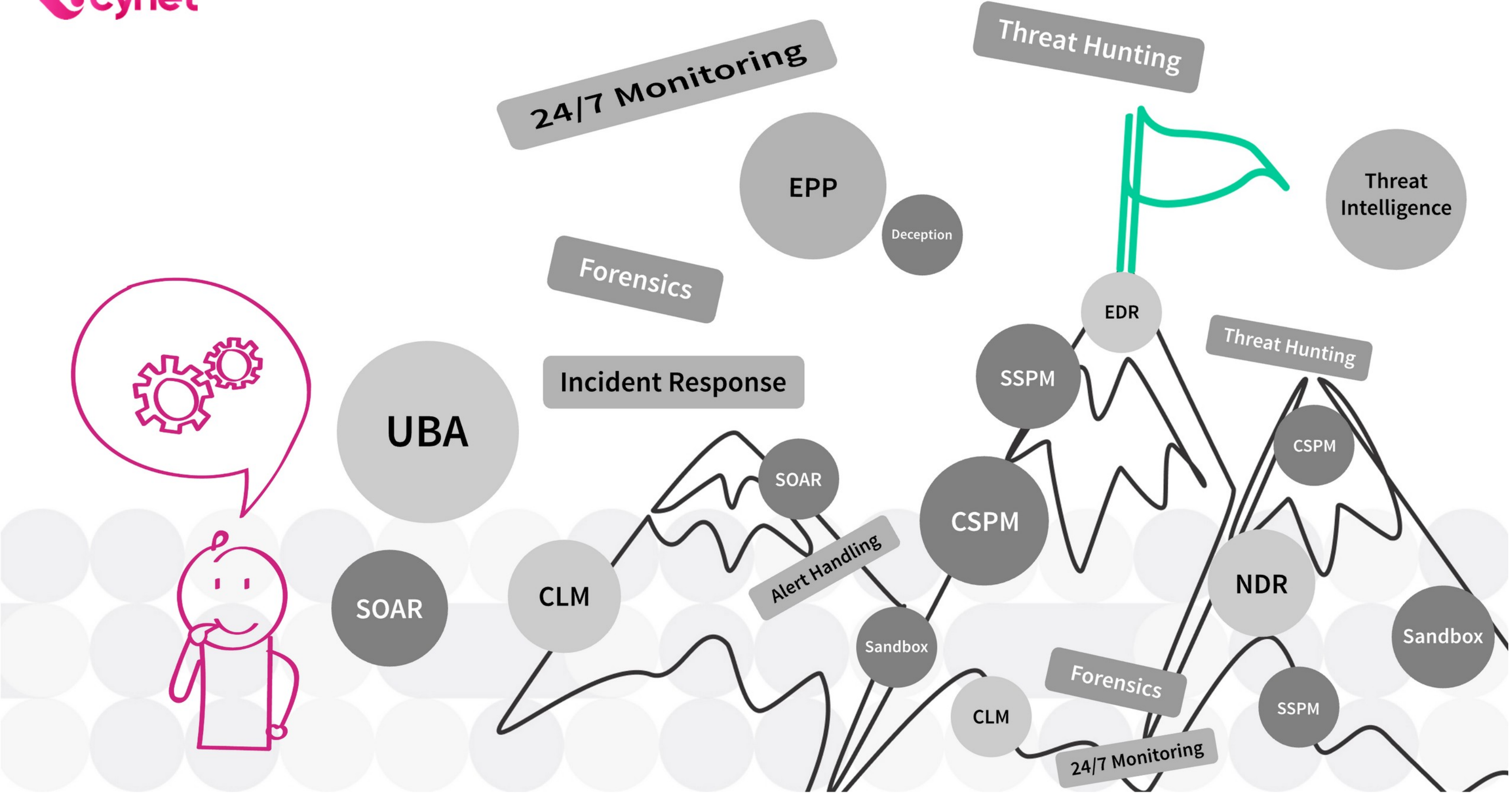
Membro del Comitato di schema

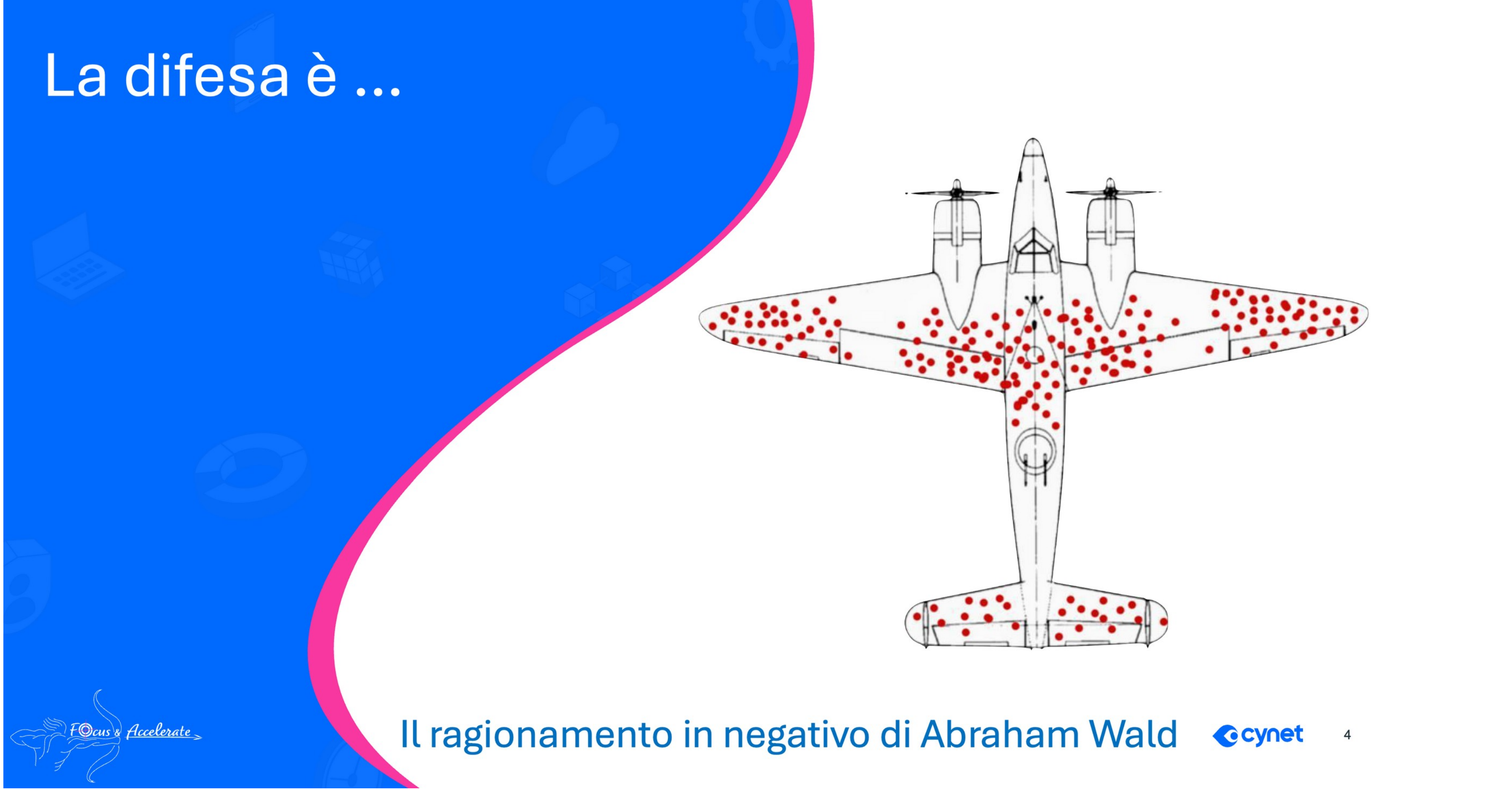
Direttore Scientifico della testata

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano

# Marco Lucchina

Country Manager Italy

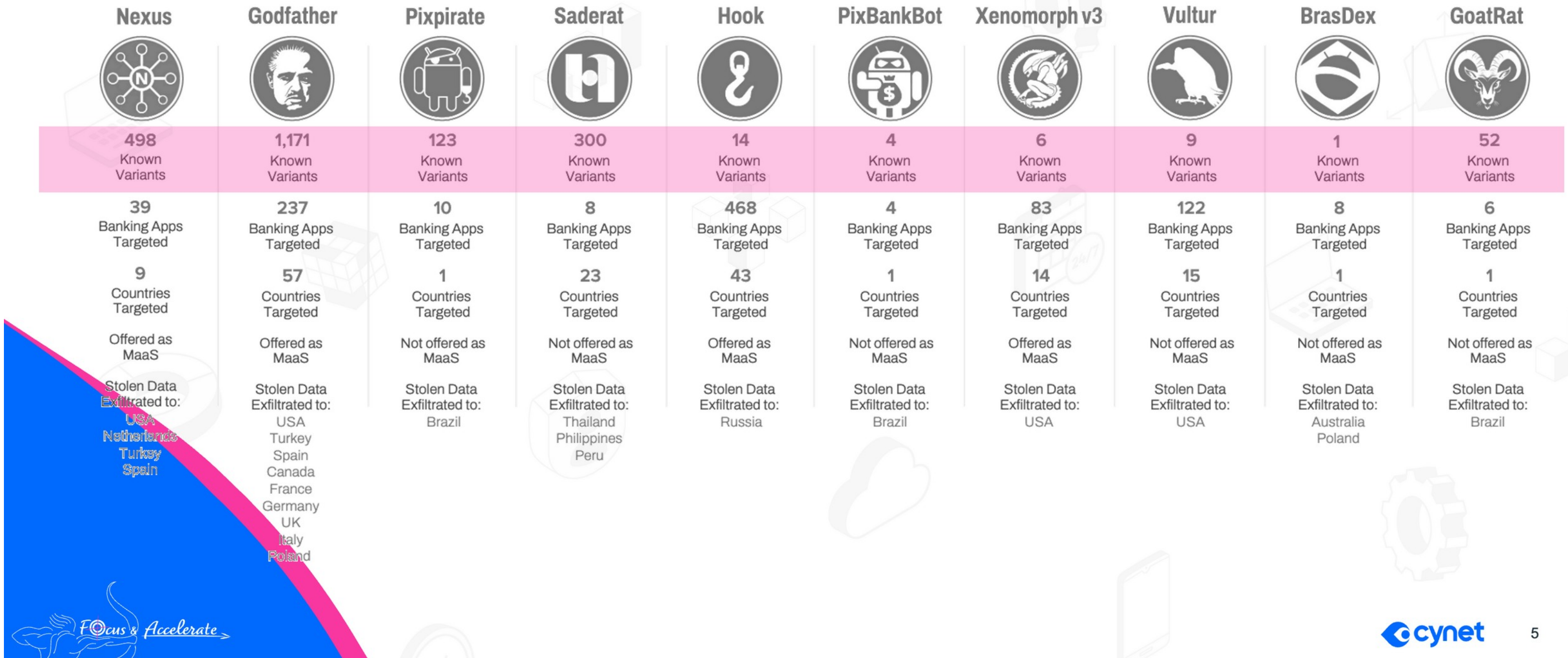

24/7 Monitoring
Threat Hunting
EPP
Deception
Threat Intelligence
Forensics
EDR
SSPM
Threat Hunting
Incident Response
UBA
CSPM
SOAR
CSPM
Alert Handling
NDR
SOAR
CLM
Sandbox
Sandbox
Forensics
CLM
SSPM
24/7 Monitoring



# La difesa è ...

Il ragionamento in negativo di Abraham Wald

# Malware as a service



| Nexus | Godfather | Pixpirate | Saderat | Hook | PixBankBot | Xenomorph v3 | Vultur | BrasDex | GoatRat |
|---|---|---|---|---|---|---|---|---|---|
| 498<br>Known Variants | 1,171<br>Known Variants | 123<br>Known Variants | 300<br>Known Variants | 14<br>Known Variants | 4<br>Known Variants | 6<br>Known Variants | 9<br>Known Variants | 1<br>Known Variants | 52<br>Known Variants |
| 39<br>Banking Apps Targeted | 237<br>Banking Apps Targeted | 10<br>Banking Apps Targeted | 8<br>Banking Apps Targeted | 468<br>Banking Apps Targeted | 4<br>Banking Apps Targeted | 83<br>Banking Apps Targeted | 122<br>Banking Apps Targeted | 8<br>Banking Apps Targeted | 6<br>Banking Apps Targeted |
| 9<br>Countries Targeted | 57<br>Countries Targeted | 1<br>Countries Targeted | 23<br>Countries Targeted | 43<br>Countries Targeted | 1<br>Countries Targeted | 14<br>Countries Targeted | 15<br>Countries Targeted | 1<br>Countries Targeted | 1<br>Countries Targeted |
| Offered as MaaS | Offered as MaaS | Not offered as MaaS | Not offered as MaaS | Offered as MaaS | Not offered as MaaS | Offered as MaaS | Not offered as MaaS | Not offered as MaaS | Not offered as MaaS |
| Stolen Data Exfiltrated to:<br>USA<br>Netherlands<br>Turkey<br>Spain | Stolen Data Exfiltrated to:<br>USA<br>Turkey<br>Spain<br>Canada<br>France<br>Germany<br>UK<br>Italy<br>Poland | Stolen Data Exfiltrated to:<br>Brazil | Stolen Data Exfiltrated to:<br>Thailand<br>Philippines<br>Peru | Stolen Data Exfiltrated to:<br>Russia | Stolen Data Exfiltrated to:<br>Brazil | Stolen Data Exfiltrated to:<br>USA | Stolen Data Exfiltrated to:<br>USA | Stolen Data Exfiltrated to:<br>Australia<br>Poland | Stolen Data Exfiltrated to:<br>Brazil |

cynet 5

Focus & Accelerate

## Cloud9: Chrome Extension Enables Remote Device Control

Late in the fall of 2022, the zLabs team discovered a malicious, potentially extremely dangerous extension to the Chrome browser. Dubbed Cloud9, this malware has the ability to steal information available during browser sessions. In addition, it can install malware that enables malicious actors to gain control over the infected device. This malware is distributed in a number of ways, including sideloading through fake executables and malicious websites purporting to provide users with Adobe Flash Player updates.

## Schoolyard Bully: Trojan Credential Stealer Afflicts 300,000 Victims

Late in 2022, zLabs discovered a new Android threat campaign, the Schoolyard Bully Trojan. These trojans have been found in numerous apps that were downloaded from the Google Play Store and third-party app stores. The trojans are hidden within seemingly legitimate educational apps. Claiming more than 300,000 victims, the malware is focused on stealing an individual's Facebook credentials. While these malicious apps have been removed from the Google Play store, they remain on numerous third-party app sites.

## Dark Herring: Scamware Exceeds 100 Million Installations

Last year's report featured an Android Trojan attack known as GriftHorse, outlining how it infected 10 million devices in over 70 countries. Unfortunately, since that time, the scamware threat only became more widespread. Early in 2022, zLabs discovered Dark Herring, another scamware campaign. Dark Herring has targeted more than 100 million victims globally. This campaign exploits direct carrier billing to scam money from unsuspecting users, with losses estimated to have reached hundreds of millions of dollars.

TeaBot campaign. TeaBot is a banking trojan that was first detected by Cleafy in 2021.[33] This malware is designed to steal victims' credentials and SMS messages. In late 2021 and early 2022, the number of malware samples grew substantially. Ultimately, more than 400 malicious apps were detected.

Dark Herring campaign. Early in 2022, Zimperium discovered this malware campaign which successfully targeted more than 105,000,000 victims around the world.[32] This campaign exploits direct carrier billing to scam money from unsuspecting users, and losses are estimated to have reached hundreds of millions of dollars.

RatMilad campaign. In the fall of 2022, the Zimperium zLabs team issued a warning about RatMilad, an Android spyware campaign targeting individuals in the Middle East.[34] The spyware was hidden within a phone number spoofing app and was distributed under the guise of enabling users to independently verify a social media account. Once users installed the app, malicious actors could gain control over their mobile devices, including the ability to view contacts, phone call logs, media, and files.

## MoneyMonger: Malware Disguised by Flutter

Near the end of 2022, zLabs announced the discovery of MoneyMonger. Disguised as an app enabling individuals to get loans, this malware campaign enables malicious actors to steal private data. MoneyMonger was discovered in a Flutter app. Flutter is an open-source software kit for developing cross-platform apps. Through Flutter, teams can develop and maintain one codebase while delivering native mobile apps on multiple device platforms. By taking advantage of Flutter's framework, the threat actors behind MoneyMonger were able to obfuscate malicious features so they're not detected by legacy mobile security products.

## Dirty RatMilad: Android Spyware

Mobile spyware is no longer just the domain of sophisticated government surveillance teams and nation states. RatMilad is just one example of how this type of spyware is being employed by smaller organizations. This malware (which has various spyware capabilities such as data exfiltration techniques) has taken various forms. The original variant of RatMilad was hidden within a phone number spoofing app called Text Me, an app that purported to help users verify a social media account by phone. In the fall of 2022, zLabs discovered a live sample of RatMilad hidden within an app called NumRent, which is a renamed, updated version of Text Me. These apps are distributed through links in messages and social media posts.

cynet 6

# The Godfather

- Anti-emulator
- Collect victim's device info
- Unstructured Supplementary Service Data
- Call forwarding
- Push notifications
- Smishing
- Steal SMSs
- Record the screen
- VNC
- Start/Kill the malware
- Cache cleaner

Mobile

BANCO BPM

# Predator Spyware

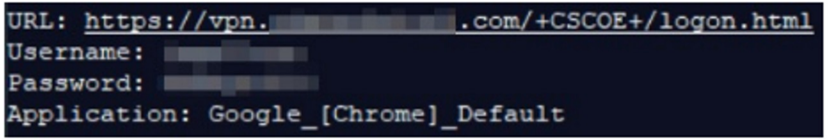
Cost: unknown

Ttps: unknown

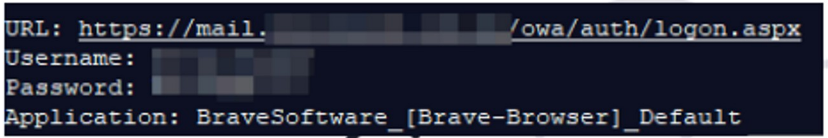
Attack Vector: SMS/MSG

Capabilities: HPPT zero-click injection

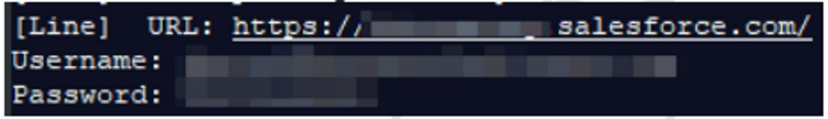
Stealth mode



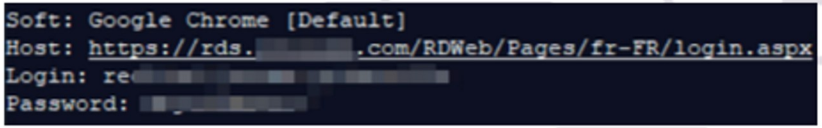
```
URL: https://vpn.[redacted].com/+CSCOE+/logon.html
Username: [redacted]
Password: [redacted]
Application: Google_[Chrome]_Default
```



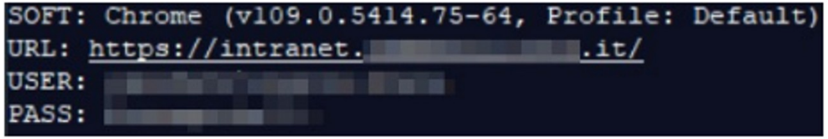
```
URL: https://mail.[redacted]/owa/auth/logon.aspx
Username: [redacted]
Password: [redacted]
Application: BraveSoftware_[Brave-Browser]_Default
```



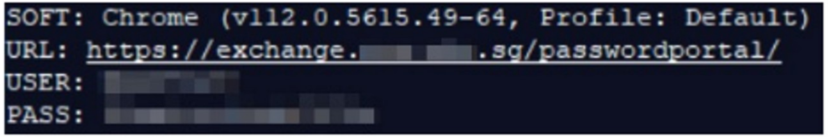
```
[Line]  URL: https://[redacted] salesforce.com/
Username: [redacted]
Password: [redacted]
```



```
Soft: Google Chrome [Default]
Host: https://rds.[redacted].com/RDWeb/Pages/fr-FR/login.aspx
Login: re[redacted]
Password: [redacted]
```



```
SOFT: Chrome (v109.0.5414.75-64, Profile: Default)
URL: https://intranet.[redacted].it/
USER: [redacted]
PASS: [redacted]
```



```
SOFT: Chrome (v112.0.5615.49-64, Profile: Default)
URL: https://exchange.[redacted].sg/passwordportal/
USER: [redacted]
PASS: [redacted]
```

# New Cybercrime

Qakbot: 700k+ (Botnet)

Genesis market: 1,5M+ host infected (credentials)

Raid forum: 800M+ records
Russian market:

ChatGPT/Gemini 20x
Ransomware: +63% paid

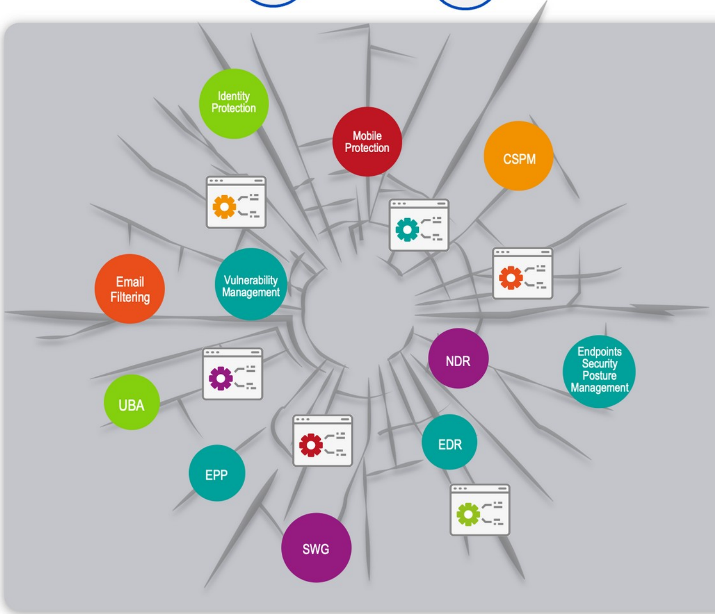
Affiliate program: +200%

Adavanced tactics and technics: 138 ATP groups

# Cybercrime predictions

# When Cyberdefense fails

TIME COMPLEXITY SKILLS BUDGET

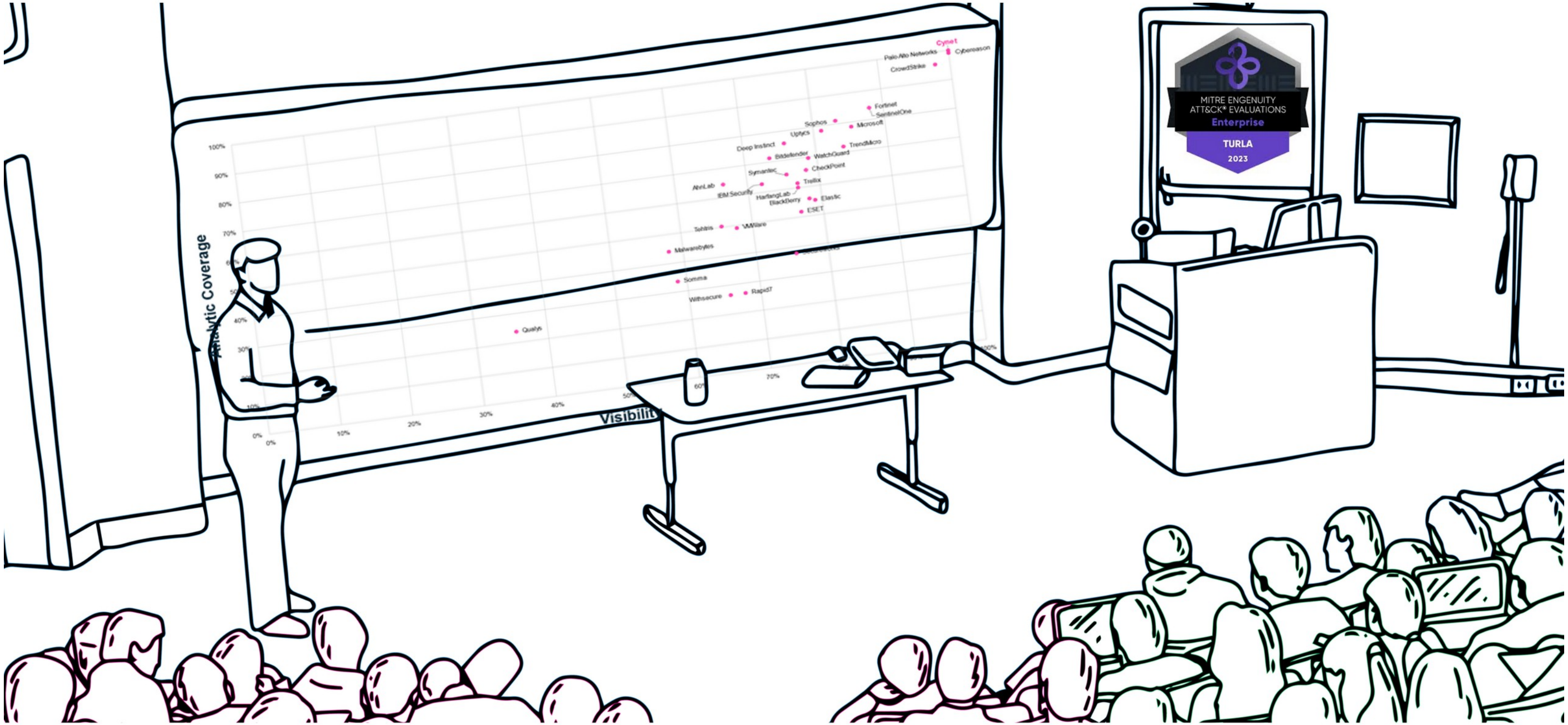


## Business goals

- Achieve full cybersecurity **coverage**
- **Simplify** Cybersecurity
- Make cybersecurity more **cost-effective**
- Activate **24/7 monitoring**
- Ensure **compliance**, qualify for **cyber insurance**
- **Automate** security operations
- Accelerate **incident response**
- Elevate security **effectiveness**

cynet

cynet


Cynet
Palo Alto Networks
Cybereason
CrowdStrike
Fortinet
SentinelOne
Sophos
Microsoft
Uptycs
Deep Instinct
TrendMicro
Bitdefender
WatchGuard
CheckPoint
Symantec
AhnLab
Trellix
IBM Security
HarfangLab
BlackBerry
Elastic
ESET
Tehtris
VMWare
Malwarebytes
Somma
Withsecure
Rapid7
Qualys
Analytic Coverage
100%
90%
80%
70%
60%
50%
40%
30%
10%
0%
Visibility
0%
10%
20%
30%
40%
50%
60%
70%
100%
MITRE ENGENUITY
ATT&CK® EVALUATIONS
Enterprise
TURLA
2023

cynet

*<- My LinkedIN*