Breached by borderless adversaries: Cyber threat actors in the Asia-Pacific

ABHIJITH “ABX” B R

Asia-Pacific ATT&CK Community Workshop
6-7 March 2025 | Singapore

MITRE | Center for Threat Informed Defense™ hosted by citi

https://breachsimrange.io

Who am I?

ABHIJITH “ABX” B R

- I’m a hacker, offensive cyber security specialist, security researcher, red team consultant, trainer and public speaker.
- Over a decade of experience in the offensive cyber security domain
- Founder of **Adversary Village** at DEF CON (https://adversaryvillage.org/)
- An independent Consulting specialist offensive cyber security and currently building **BreachSimRange.io**
- Formerly worked with **Envestnet, Inc**., **Nissan Motor Corporation**, **EY**.
- Actively running **https://tacticaladversary.io** research blog
- Leading DEF CON Group Trivandrum (https://dc0471.org/)

@abhijithbr

Adversary groups landscape in APAC

Threat actors are becoming more sophisticated and frequent

- **Diverse and Sophisticated Adversaries**

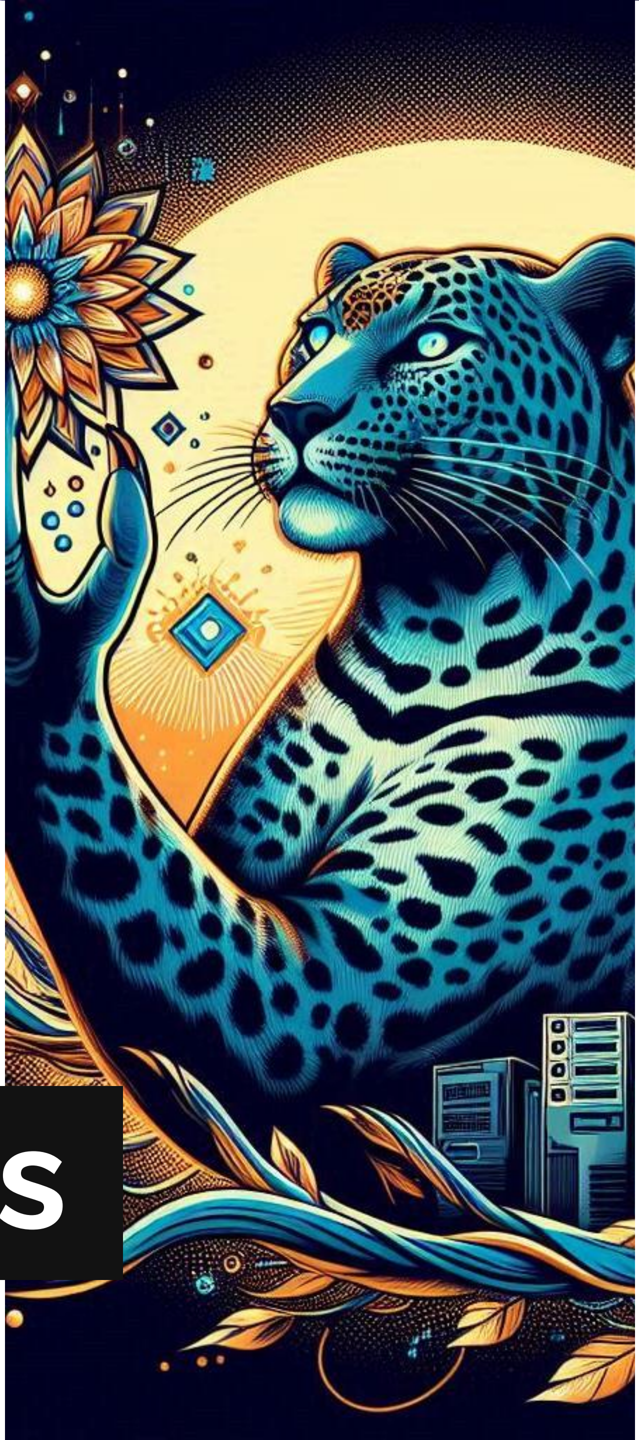
  State-sponsored APT groups like APT41 and APT40, financially motivated ransomware gangs like LockBit and ALPHV

- **Geopolitical Motivations**

  Nation-state actors from adversary countries target APAC nations for espionage, IP theft and political influence

- **Critical Infrastructure Sectors**

  Telecom, Finance, Government, and Defense remain prime targets for adversary groups

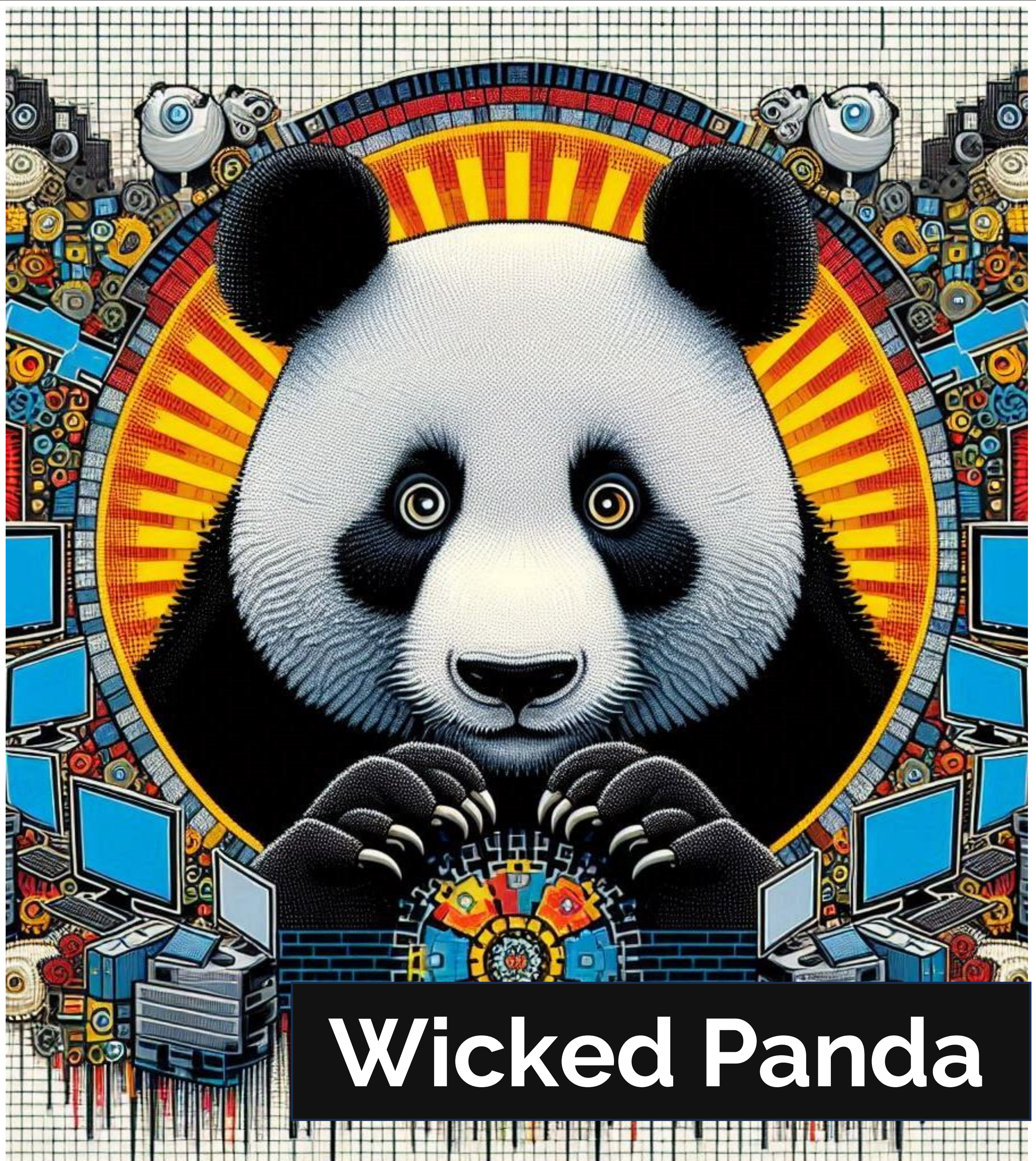


Adversary Groups

https://breachsimrange.io

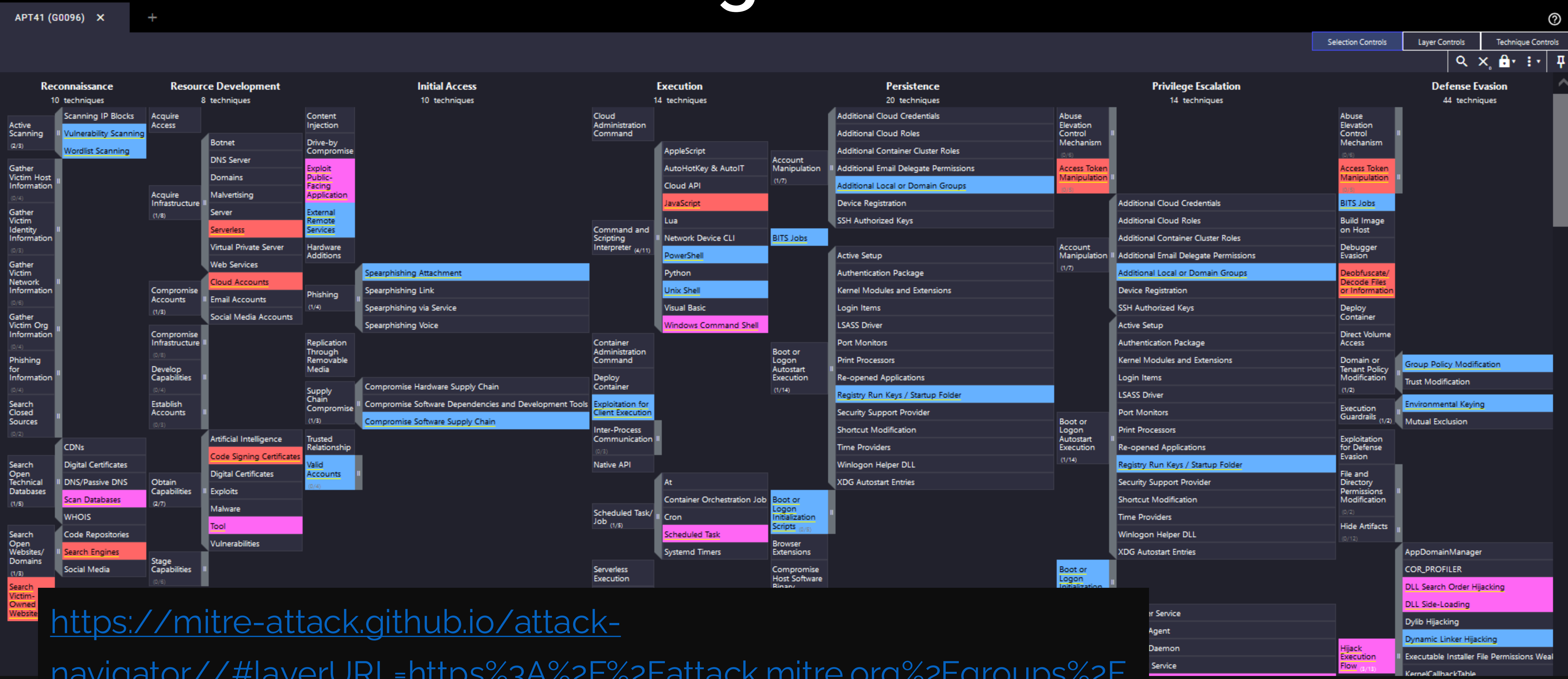
[Wicked Panda | APT41 | BARIUM]

- A state sponsored threat actor whose goals include cyber espionage and financial gain, active since at least 2007
- Also known as BARIUM, Winnti, WICKED SPIDER, WICKED PANDA, Blackfly, Suckfly
- APT41 compromised and gained various levels of access to at least 14 organizations worldwide.
- The group's targets include government and private organizations based in the **India, US, Taiwan, Thailand, China, Hong Kong, Mongolia, Indonesia, Vietnam, Bangladesh, Ireland, Brunei,** and **UK.**



Wicked Panda

MITRE ATT&CK Navigator



Reconnaissance 10 techniques

- Active Scanning (2/3)
  - Scanning IP Blocks
  - Vulnerability Scanning
  - Wordlist Scanning
- Gather Victim Host Information (0/4)
- Gather Victim Identity Information (0/3)
- Gather Victim Network Information (0/6)
- Gather Victim Org Information (0/4)
- Phishing for Information (0/4)
- Search Closed Sources (0/2)
- Search Open Technical Databases (1/5)
  - CDNs
  - Digital Certificates
  - DNS/Passive DNS
  - Scan Databases
  - WHOIS
- Search Open Websites/ Domains (1/3)
  - Code Repositories
  - Search Engines
  - Social Media
- Search Victim-Owned Website

Resource Development 8 techniques

- Acquire Access
- Acquire Infrastructure (1/8)
  - Botnet
  - DNS Server
  - Domains
  - Malvertising
  - Server
  - Serverless
  - Virtual Private Server
  - Web Services
- Compromise Accounts (1/3)
  - Cloud Accounts
  - Email Accounts
  - Social Media Accounts
- Compromise Infrastructure (0/8)
- Develop Capabilities (0/4)
- Establish Accounts (0/3)
- Obtain Capabilities (2/7)
  - Artificial Intelligence
  - Code Signing Certificates
  - Digital Certificates
  - Exploits
  - Malware
  - Tool
  - Vulnerabilities
- Stage Capabilities (0/6)

Initial Access 10 techniques

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (1/4)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
  - Spearphishing Voice
- Replication Through Removable Media
- Supply Chain Compromise (1/3)
  - Compromise Hardware Supply Chain
  - Compromise Software Dependencies and Development Tools
  - Compromise Software Supply Chain
- Trusted Relationship
- Valid Accounts (0/4)

Execution 14 techniques

- Cloud Administration Command
- Command and Scripting Interpreter (4/11)
  - AppleScript
  - AutoHotKey & AutoIT
  - Cloud API
  - JavaScript
  - Lua
  - Network Device CLI
  - PowerShell
  - Python
  - Unix Shell
  - Visual Basic
  - Windows Command Shell
- Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- Inter-Process Communication (0/3)
- Native API
- Scheduled Task/ Job (1/5)
  - At
  - Container Orchestration Job
  - Cron
  - Scheduled Task
  - Systemd Timers
- Serverless Execution

Persistence 20 techniques

- Account Manipulation (1/7)
  - Additional Cloud Credentials
  - Additional Cloud Roles
  - Additional Container Cluster Roles
  - Additional Email Delegate Permissions
  - Additional Local or Domain Groups
  - Device Registration
  - SSH Authorized Keys
- BITS Jobs
- Boot or Logon Autostart Execution (1/14)
  - Active Setup
  - Authentication Package
  - Kernel Modules and Extensions
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- Compromise Host Software Binary

Privilege Escalation 14 techniques

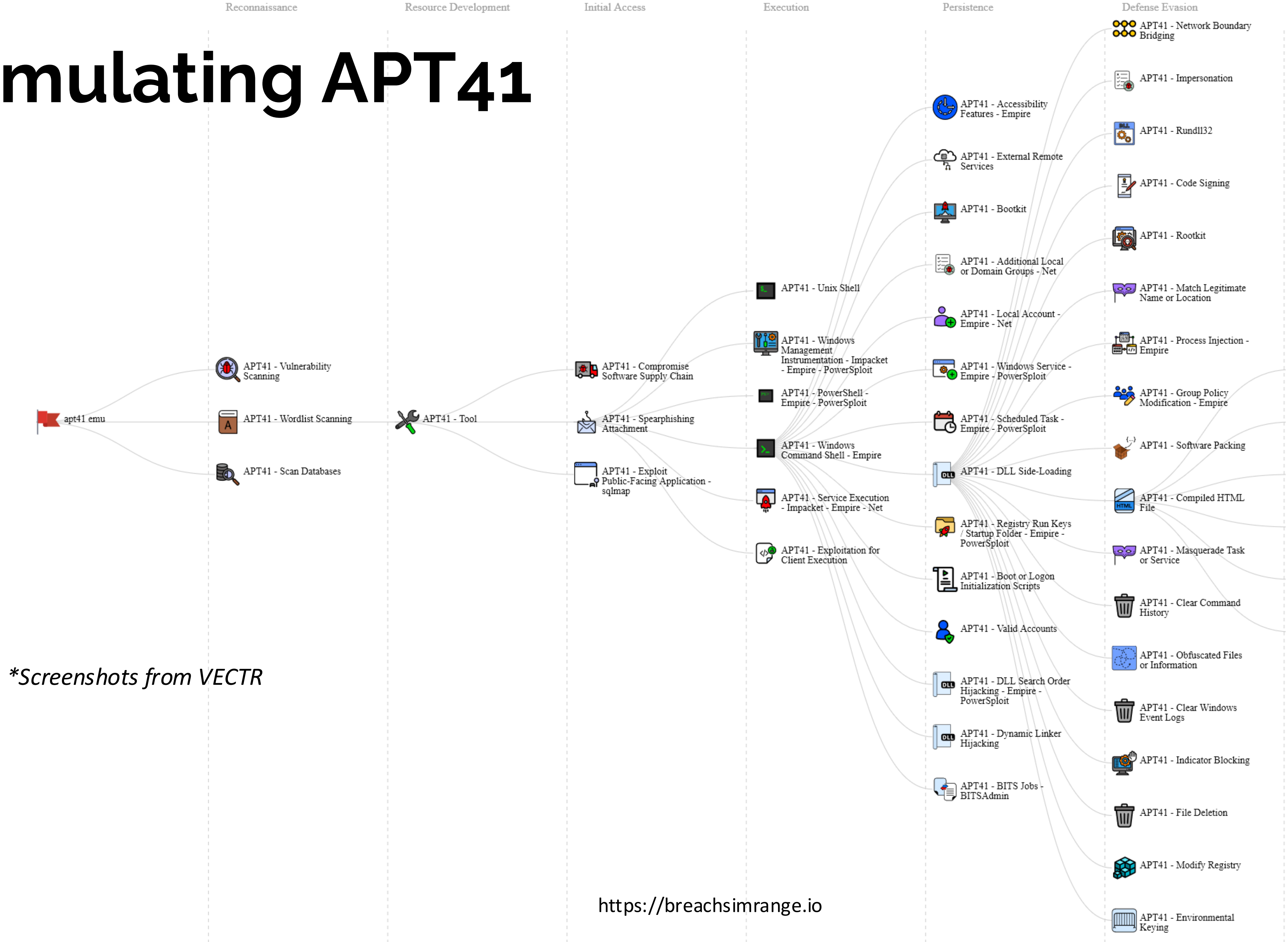
- Abuse Elevation Control Mechanism (0/6)
- Access Token Manipulation (0/5)
- Account Manipulation (1/7)
  - Additional Cloud Credentials
  - Additional Cloud Roles
  - Additional Container Cluster Roles
  - Additional Email Delegate Permissions
  - Additional Local or Domain Groups
  - Device Registration
  - SSH Authorized Keys
- Boot or Logon Autostart Execution (1/14)
  - Active Setup
  - Authentication Package
  - Kernel Modules and Extensions
  - Login Items
  - LSASS Driver
  - Port Monitors
  - Print Processors
  - Re-opened Applications
  - Registry Run Keys / Startup Folder
  - Security Support Provider
  - Shortcut Modification
  - Time Providers
  - Winlogon Helper DLL
  - XDG Autostart Entries
- Boot or Logon Initialization
  - r Service
  - Agent
  - Daemon
  - Service

Defense Evasion 44 techniques

- Abuse Elevation Control Mechanism (0/6)
- Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/ Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification (1/2)
  - Group Policy Modification
  - Trust Modification
- Execution Guardrails (1/2)
  - Environmental Keying
  - Mutual Exclusion
- Exploitation for Defense Evasion
- File and Directory Permissions Modification (0/2)
- Hide Artifacts (0/12)
- Hijack Execution Flow (3/13)
  - AppDomainManager
  - COR_PROFILER
  - DLL Search Order Hijacking
  - DLL Side-Loading
  - Dylib Hijacking
  - Dynamic Linker Hijacking
  - Executable Installer File Permissions Weal
  - KernelCallbackTable

https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0096%2FG0096-enterprise-layer.json

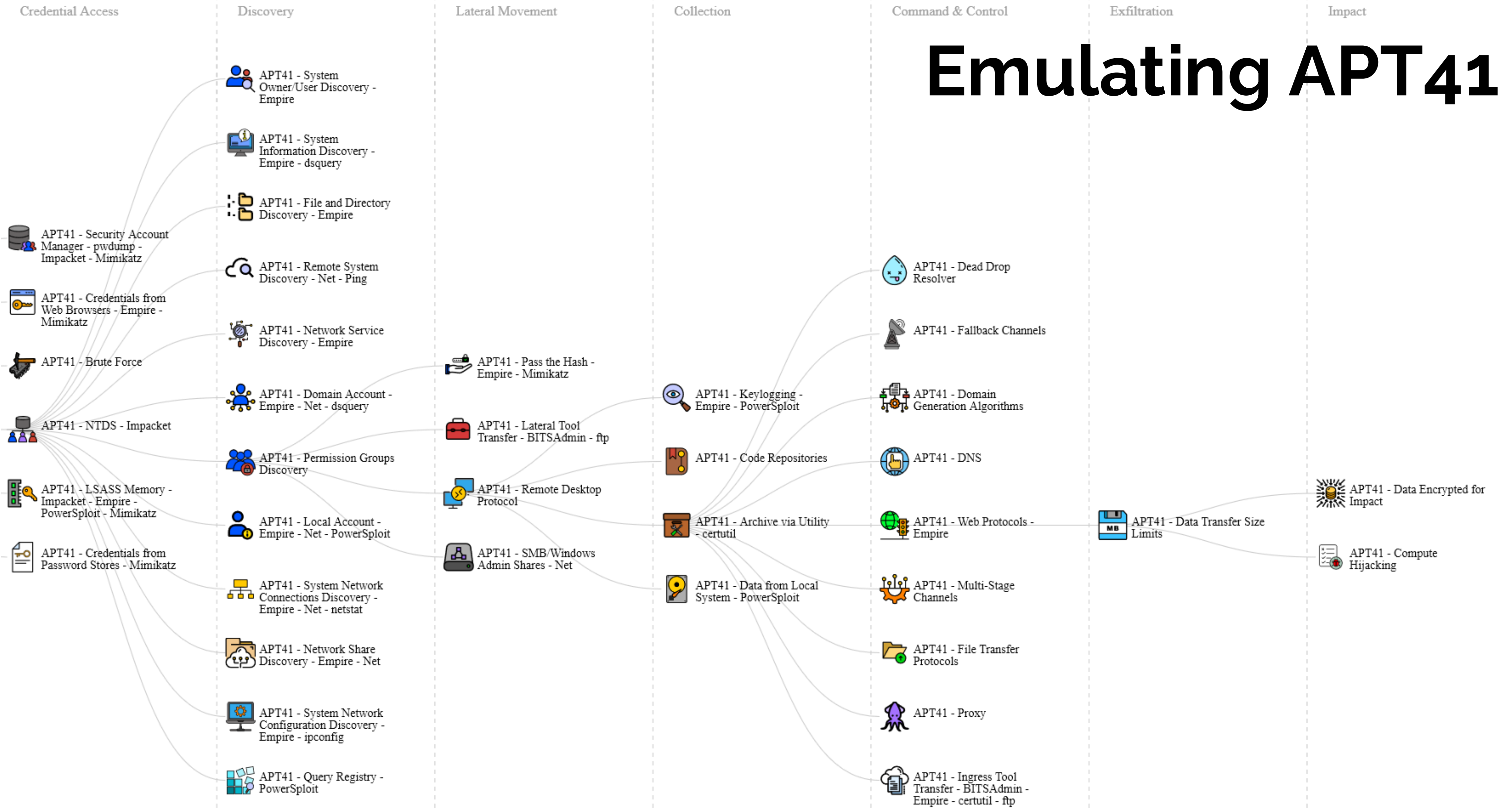
Emulating APT41


Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Defense Evasion
apt41 emu
APT41 - Vulnerability Scanning
APT41 - Wordlist Scanning
APT41 - Scan Databases
APT41 - Tool
APT41 - Compromise Software Supply Chain
APT41 - Spearphishing Attachment
APT41 - Exploit Public-Facing Application - sqlmap
APT41 - Unix Shell
APT41 - Windows Management Instrumentation - Impacket - Empire - PowerSploit
APT41 - PowerShell - Empire - PowerSploit
APT41 - Windows Command Shell - Empire
APT41 - Service Execution - Impacket - Empire - Net
APT41 - Exploitation for Client Execution
APT41 - Accessibility Features - Empire
APT41 - External Remote Services
APT41 - Bootkit
APT41 - Additional Local or Domain Groups - Net
APT41 - Local Account - Empire - Net
APT41 - Windows Service - Empire - PowerSploit
APT41 - Scheduled Task - Empire - PowerSploit
APT41 - DLL Side-Loading
APT41 - Registry Run Keys / Startup Folder - Empire - PowerSploit
APT41 - Boot or Logon Initialization Scripts
APT41 - Valid Accounts
APT41 - DLL Search Order Hijacking - Empire - PowerSploit
APT41 - Dynamic Linker Hijacking
APT41 - BITS Jobs - BITSAdmin
APT41 - Network Boundary Bridging
APT41 - Impersonation
APT41 - Rundll32
APT41 - Code Signing
APT41 - Rootkit
APT41 - Match Legitimate Name or Location
APT41 - Process Injection - Empire
APT41 - Group Policy Modification - Empire
APT41 - Software Packing
APT41 - Compiled HTML File
APT41 - Masquerade Task or Service
APT41 - Clear Command History
APT41 - Obfuscated Files or Information
APT41 - Clear Windows Event Logs
APT41 - Indicator Blocking
APT41 - File Deletion
APT41 - Modify Registry
APT41 - Environmental Keying

**Screenshots from VECTR*

https://breachsimrange.io

Emulating APT41



Credential Access

- APT41 - Security Account Manager - pwdump - Impacket - Mimikatz
- APT41 - Credentials from Web Browsers - Empire - Mimikatz
- APT41 - Brute Force
- APT41 - NTDS - Impacket
- APT41 - LSASS Memory - Impacket - Empire - PowerSploit - Mimikatz
- APT41 - Credentials from Password Stores - Mimikatz

Discovery

- APT41 - System Owner/User Discovery - Empire
- APT41 - System Information Discovery - Empire - dsquery
- APT41 - File and Directory Discovery - Empire
- APT41 - Remote System Discovery - Net - Ping
- APT41 - Network Service Discovery - Empire
- APT41 - Domain Account - Empire - Net - dsquery
- APT41 - Permission Groups Discovery
- APT41 - Local Account - Empire - Net - PowerSploit
- APT41 - System Network Connections Discovery - Empire - Net - netstat
- APT41 - Network Share Discovery - Empire - Net
- APT41 - System Network Configuration Discovery - Empire - ipconfig
- APT41 - Query Registry - PowerSploit

Lateral Movement

- APT41 - Pass the Hash - Empire - Mimikatz
- APT41 - Lateral Tool Transfer - BITSAdmin - ftp
- APT41 - Remote Desktop Protocol
- APT41 - SMB/Windows Admin Shares - Net

Collection

- APT41 - Keylogging - Empire - PowerSploit
- APT41 - Code Repositories
- APT41 - Archive via Utility - certutil
- APT41 - Data from Local System - PowerSploit

Command & Control

- APT41 - Dead Drop Resolver
- APT41 - Fallback Channels
- APT41 - Domain Generation Algorithms
- APT41 - DNS
- APT41 - Web Protocols - Empire
- APT41 - Multi-Stage Channels
- APT41 - File Transfer Protocols
- APT41 - Proxy
- APT41 - Ingress Tool Transfer - BITSAdmin - Empire - certutil - ftp

Exfiltration

- APT41 - Data Transfer Size Limits

Impact

- APT41 - Data Encrypted for Impact
- APT41 - Compute Hijacking

**Screenshots from VECTR*

https://breachsimrange.io

[Volt Typhoon | Vanguard Panda]

- Volt Typhoon is an allegedly Chinese state-sponsored cyber espionage group, primarily targeting critical infrastructure and government entities
- The group is known for using "living-off-the-land" binaries and techniques to avoid detection
- In 2024, accused of breaching Singapore Telecommunications (SingTel)
- Targeted organizations across the APAC region, including telecom, energy, and maritime sectors, often aligning with political interest

[ALPHV | BlackCat Ransomware]

- ALPHV, also known as BlackCat, is a highly advanced ransomware-as-a-service (RaaS) operation, first observed in late 2021
- The group is believed to be based in a CIS country, with strong links to earlier ransomware groups like DarkSide and BlackMatter
- ALPHV uses Rust-based ransomware, to target multiple operating systems, including Windows and Linux
- BlackCat has targeted a wide range of industries worldwide, including organizations in the APAC region, focusing on finance, healthcare, and critical infrastructure

Mythic Leopard

[Mythic Leopard | APT36 | Transparent Tribe]

- Pak based APT group which has specifically targeted employees of Indian government organizations.
- Initial access: Malvertising, and credential phishing attacks | Limepad for exfiltration
- The threat actor used new domains hosting websites masquerading as the **official Kavach app download portal.**
- Abused the Google Ads paid search feature to push the malicious domains to the top of Google search results for Indian users
- Credential harvesting attacks were used to spoof the NIC Kavach login page

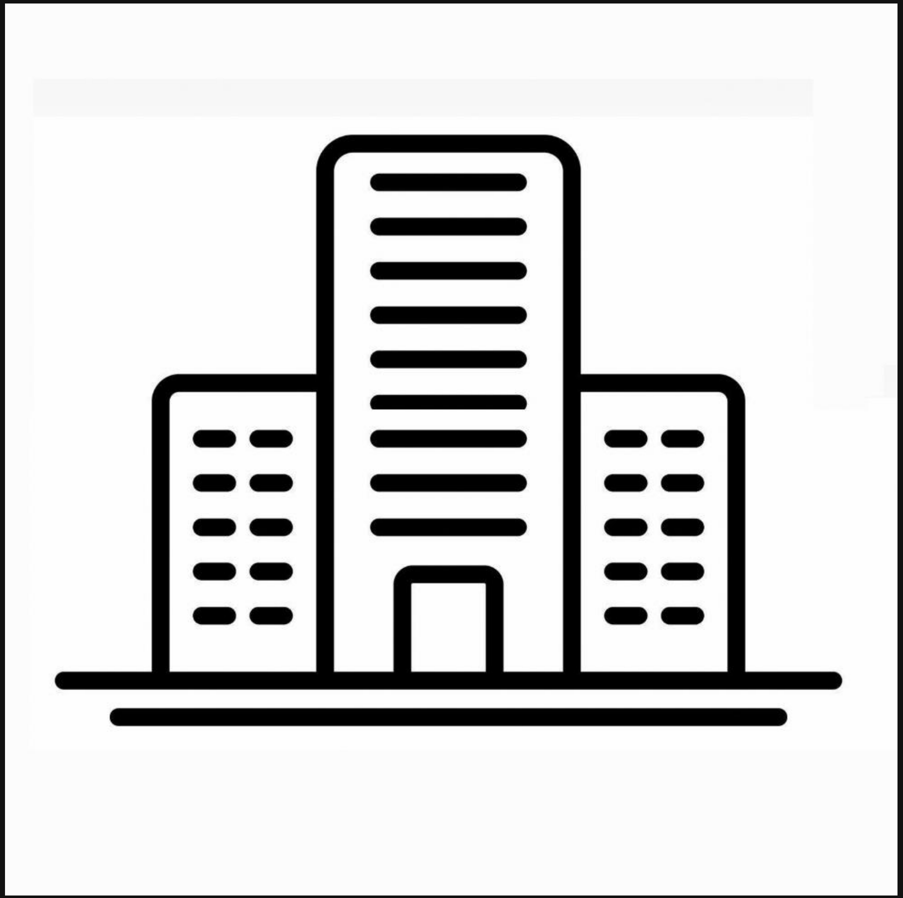
https://breachsimrange.io

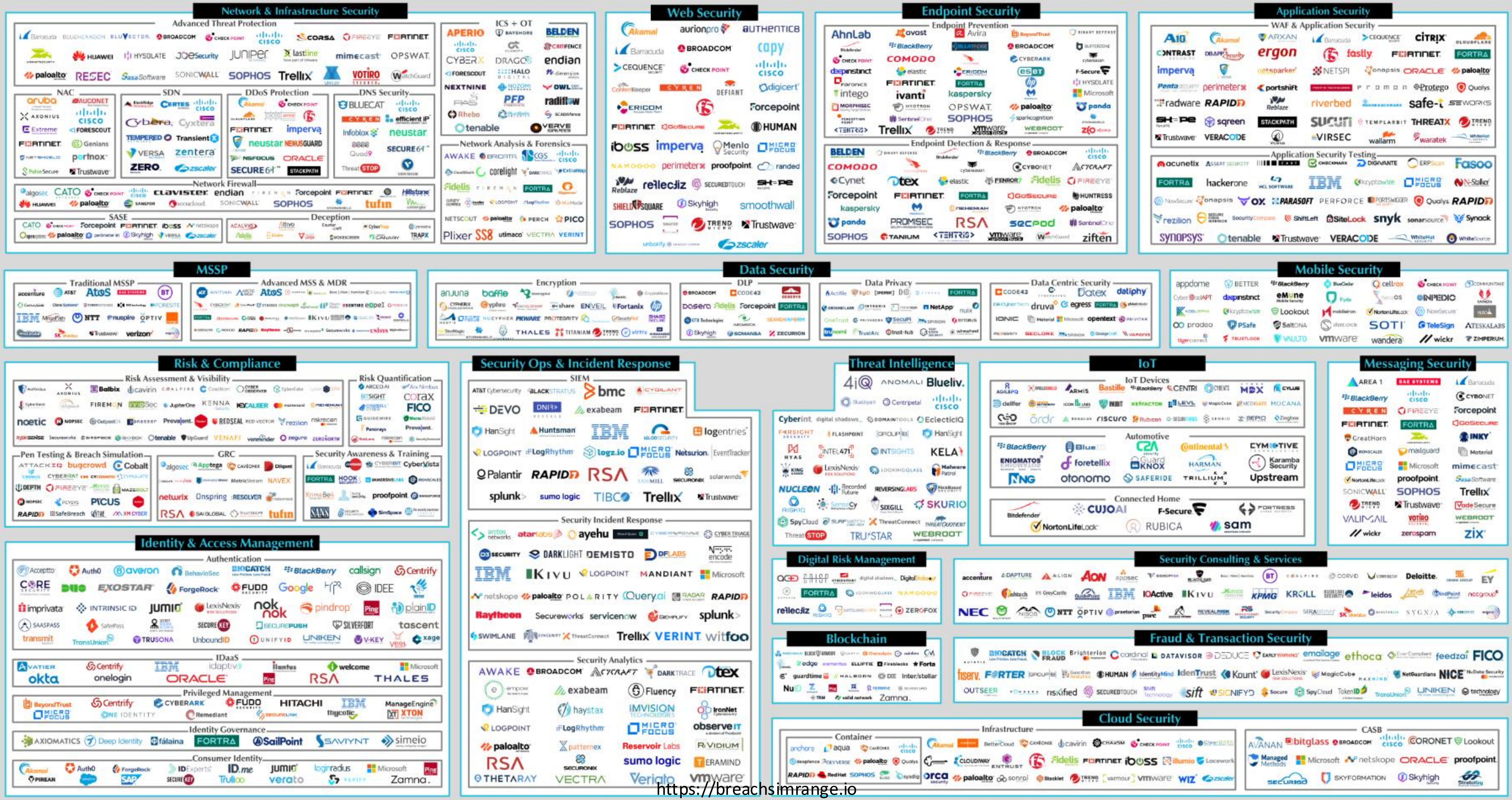
Let’s talk about the targets!

https://breachsimrange.io

Defense level: 9

Target 1:
The Enterprises!





Network & Infrastructure Security

Advanced Threat Protection

ICS + OT

NAC

SDN

DDoS Protection

DNS Security

Network Analysis & Forensics

Network Firewall

SASE

Deception

Web Security

Endpoint Security

Endpoint Prevention

Endpoint Detection & Response

Application Security

WAF & Application Security

Application Security Testing

MSSP

Traditional MSSP

Advanced MSS & MDR

Data Security

Encryption

DLP

Data Privacy

Data Centric Security

Mobile Security

Risk & Compliance

Risk Assessment & Visibility

Risk Quantification

Pen Testing & Breach Simulation

GRC

Security Awareness & Training

Security Ops & Incident Response

SIEM

Security Incident Response

Security Analytics

Threat Intelligence

IoT

IoT Devices

Automotive

Connected Home

Messaging Security

Identity & Access Management

Authentication

IDaaS

Privileged Management

Identity Governance

Consumer Identity

Digital Risk Management

Security Consulting & Services

Blockchain

Fraud & Transaction Security

Cloud Security

Container

Infrastructure

CASB

https://breachsimrange.io

Enterprises [with no budget constraints]

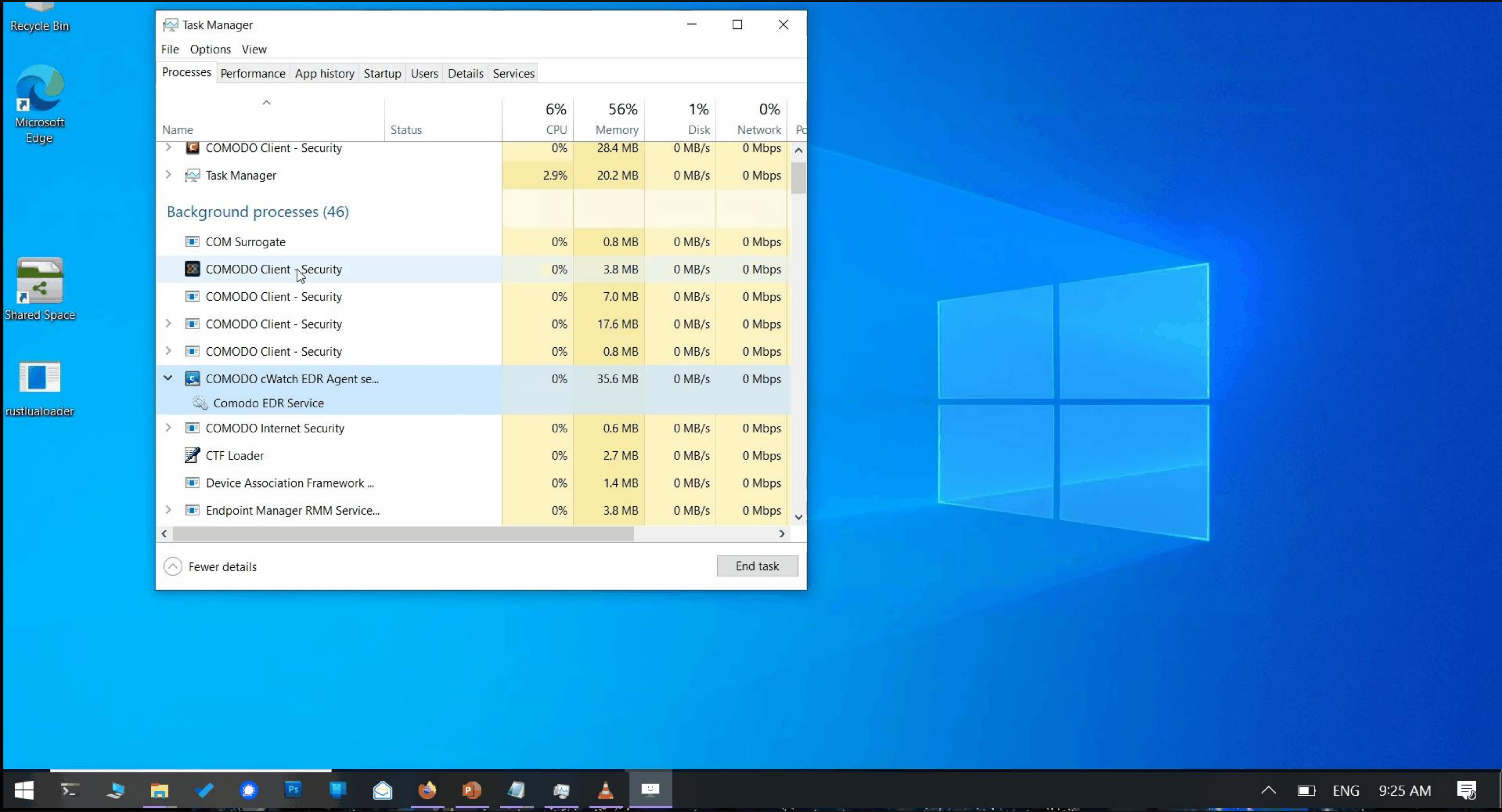
All kind of security products | Let’s take an end-user laptop as an example

- **Multiple agents installed**
- Anti-Virus, EDR [Endpoint detection and response], XDR
- EPM [Endpoint privilege manager]
- Webproxies
- DLP [Data loss prevention]
- SIEM agents
- IP monitoring, user analytics, and other user telemetry collection
- SCCM, Zero trust agents and many others….

Demo 1

What would an adversary or a red teamer do?

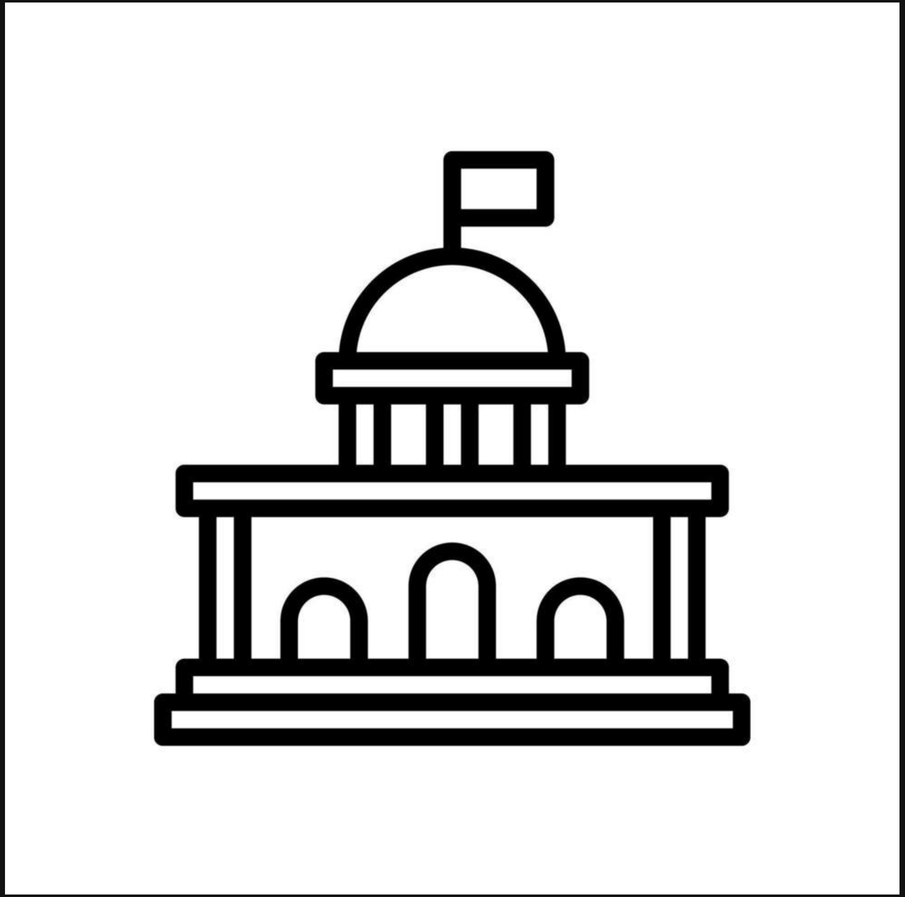
[Breaching enterprise defenses]



Name	Status	6% CPU	56% Memory	1% Disk	0% Network
COMODO Client - Security		0%	28.4 MB	0 MB/s	0 Mbps
Task Manager		2.9%	20.2 MB	0 MB/s	0 Mbps
Background processes (46)					
COM Surrogate		0%	0.8 MB	0 MB/s	0 Mbps
COMODO Client - Security		0%	3.8 MB	0 MB/s	0 Mbps
COMODO Client - Security		0%	7.0 MB	0 MB/s	0 Mbps
COMODO Client - Security		0%	17.6 MB	0 MB/s	0 Mbps
COMODO Client - Security		0%	0.8 MB	0 MB/s	0 Mbps
COMODO cWatch EDR Agent se...		0%	35.6 MB	0 MB/s	0 Mbps
Comodo EDR Service					
COMODO Internet Security		0%	0.6 MB	0 MB/s	0 Mbps
CTF Loader		0%	2.7 MB	0 MB/s	0 Mbps
Device Association Framework ...		0%	1.4 MB	0 MB/s	0 Mbps
Endpoint Manager RMM Service...		0%	3.8 MB	0 MB/s	0 Mbps

Defense level: 8

Target 2:
Govt. Organizations



Govt. organizations

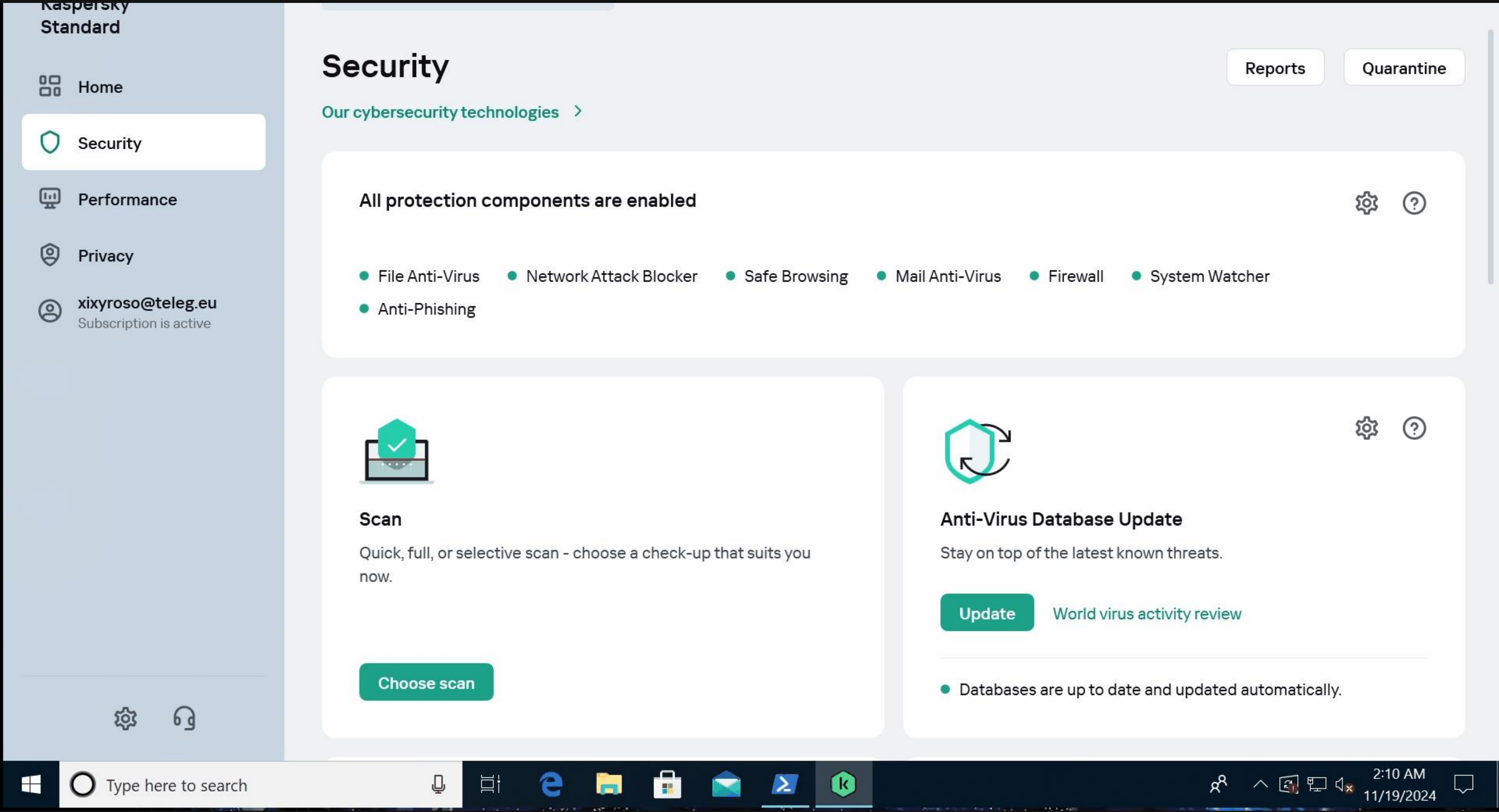
No budget constraints, but a lot of difficulties due to red tape
Let’s take an end-user laptop as an example

- **Multiple agents installed**
- Anti-Virus
- EDR [Endpoint detection and response]
- Webproxies, but mostly firewall based outbound traffic control systems
- SIEM agents
- Not including the detailed list due to the obvious reasons
- Focused on the limiting access and traffic

Demo 2

What would a nation-state threat actor typically do?

[Bypassing enterprise defenses]



Security

Our cybersecurity technologies >

All protection components are enabled

- File Anti-Virus
- Network Attack Blocker
- Safe Browsing
- Mail Anti-Virus
- Firewall
- System Watcher
- Anti-Phishing

Scan

Quick, full, or selective scan - choose a check-up that suits you now.

Choose scan

Anti-Virus Database Update

Stay on top of the latest known threats.

Update

World virus activity review

- Databases are up to date and updated automatically.

Defense level: 2

Target 3:
The general public

General public | Home users

Let’s take a home user laptop as an example

- Mostly Windows Defender preloaded
- Commercial home edition Anti-Virus products
- Linux home users, Mostly no Anti-Virus at all
- What else?
- You tell me!

Demo 3

What would a ransomware gang typically do?

[Breaching home-security products]

https://breachsimrange.io

Cyber Threat Actors doesn’t have

Guard Rails!

Not Exactly.

We are prepared,

https://breachsimrange.io

Until
We are not.

How would you defend against such evolving and motivated Adversaries?

https://breachsimrange.io

Thinking like an attacker might help?

https://tacticaladversary.io/

Story time

Offensive X Defensive

= Collaboration

Improving your organization's defensive tradecraft?

Or Offensive?

Dynamic Simulation of Defense Evasion TTPs

There are 100+ open-source EDR bypass tools and loaders available in GitHub.

Your offensive team ever tried to collect and dynamically simulate those tools against your endpoint-security controls?

Case study

Threat Intel powered Internet Vulnerability Research Team

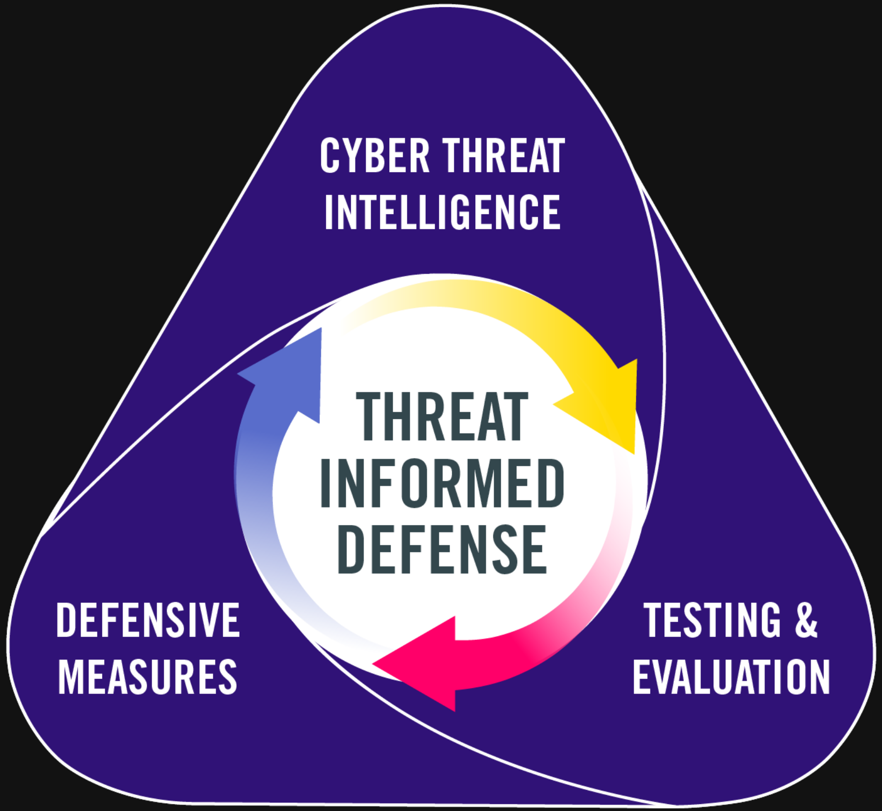
- A dedicated OR shared team with the involvement of all security teams
- Threat Intel, Internet vulnerability research and tactical response
- Prioritize vulnerabilities based on exploitability, map it against the assets inventory
- Validate exploitability, deploy complimentary security controls even if a patch was not announced
- Convert deep technical findings to business impact
- *Bridge the gaps in enterprise vulnerability scanners and threat intel feeds*
- Communicate Communicate Communicate

Threat-Intel Powered
Adversary Emulation?
The Game Changer.

Threat-Informed Defense

Threat Intel Powered Breach and Attack Simulation

MITRE Center for Threat-Informed Defense



- Purple teaming and adversary simulation are critical components of threat-informed defense
- Enable continuous validation and improvement of security posture
- Threat-informed defense is about improving security program efficiency and effectiveness

https://center-for-threat-informed-defense.github.io/m3tid/getting-started/

https://breachsimrange.io

Is this approach effective for Organizations in Private and Government sector?

Enterprise Organizations

Government Organizations

{Actionable Threat Intel}

+

{Continuous Security Control Validation}

+

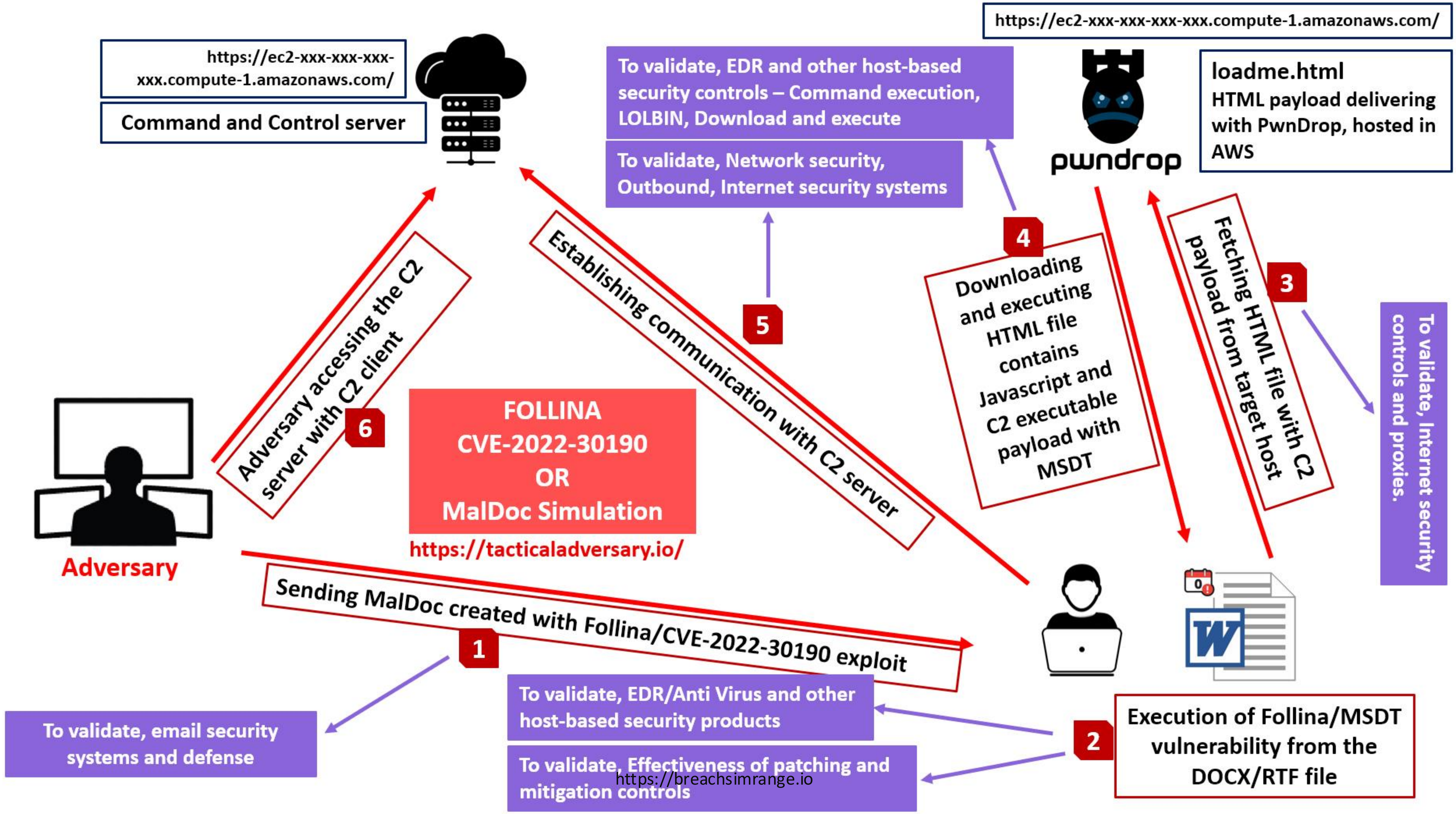
{Continuous Defense Improvement}

Year 1

Start with Open-source tools and frameworks

Year 2

Move to commercial



FOLLINA
CVE-2022-30190
OR
MalDoc Simulation

https://tacticaladversary.io/

Adversary

https://ec2-xxx-xxx-xxx-xxx.compute-1.amazonaws.com/

Command and Control server

https://ec2-xxx-xxx-xxx-xxx.compute-1.amazonaws.com/

pwndrop

loadme.html
HTML payload delivering with PwnDrop, hosted in AWS

1 Sending MalDoc created with Follina/CVE-2022-30190 exploit

To validate, email security systems and defense

2 Execution of Follina/MSDT vulnerability from the DOCX/RTF file

To validate, EDR/Anti Virus and other host-based security products

To validate, Effectiveness of patching and mitigation controls

3 Fetching HTML file with C2 payload from target host

To validate, Internet security controls and proxies.

4 Downloading and executing HTML file contains Javascript and C2 executable payload with MSDT

To validate, EDR and other host-based security controls – Command execution, LOLBIN, Download and execute

5 Establishing communication with C2 server

To validate, Network security, Outbound, Internet security systems

6 Adversary accessing the C2 server with C2 client

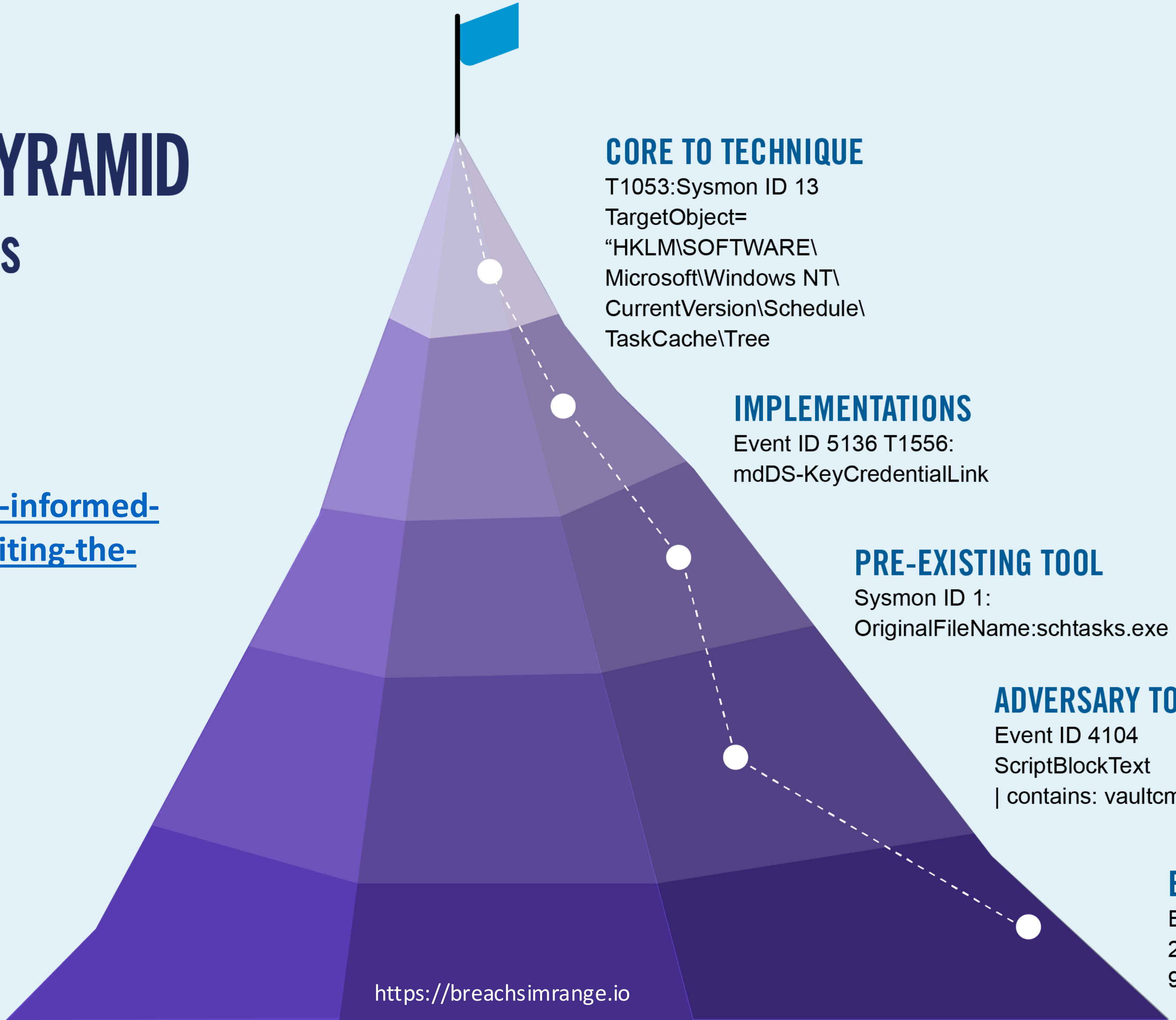
Continuous Security Control validation

- **Using Adversary Emulation to assess endpoint security products:**
- Anti-Virus
- EDR products
- Web proxies
- Firewalls / WAF / IPS/IDS systems
- Privileges user management (EPM)
- DLP Systems
- Email security products and controls
- Cloud security products
- Using Adversary Simulation to assess SOC/SIEM systems
- Security Operations Centre
- Detection engineering
- What other security products are there?
- **Bring maximum ROI on security products**

SUMMITING THE PYRAMID

Level Up Your Analytics

https://center-for-threat-informed-defense.github.io/summiting-the-pyramid/



CORE TO TECHNIQUE

T1053:Sysmon ID 13
TargetObject=
“HKLM\SOFTWARE\
Microsoft\Windows NT\
CurrentVersion\Schedule\
TaskCache\Tree

IMPLEMENTATIONS

Event ID 5136 T1556:
mdDS-KeyCredentialLink

PRE-EXISTING TOOL

Sysmon ID 1:
OriginalFileName:schtasks.exe

ADVERSARY TOOL

Event ID 4104
ScriptBlockText
| contains: vaultcmd

EPHEMERAL

Event ID 4688
22dc9f0490f5ae
9f014d1acb7ed5641

MITRE ENGENUITY | Center for Threat Informed Defense

Now, how do you help the general public?

Public-Private Partnership might be a good idea?

https://breachsimrange.io

What is next?

Conclusion

- **Adversarial Exposure Validation**
- Breaking defenses from an attacker's perspective getting easier
- Targets could be Govt., Enterprises and the general public with different Defense levels.
- Some breaches, organizations doesn't even know how the initial access happened.
  It is still a huge concern.
- Breach and Attack Simulation, Adversary Emulation, Purple Teaming exercises can make a huge impact on the security posture of your organization
- Threat-Informed Defense has a well-defined path to attain this goal
- Extend your simulation scenarios to each security products and services then create full attack sim scenarios to assess the full attack chain
- **Emulate-Emulate-Emulate-Simulate-Simulate-Red Team**

Would you expect something like this?

Expect the Unexpected
Simulate the Unknown!

https://breachsimrange.io

Keep in touch!

BLOG: https://tacticaladversary.io/blog

https://x.com/abhijithbr

https://in.linkedin.com/in/abhijith-b-r

Abx#1337

Thank You!

https://breachsimrange.io