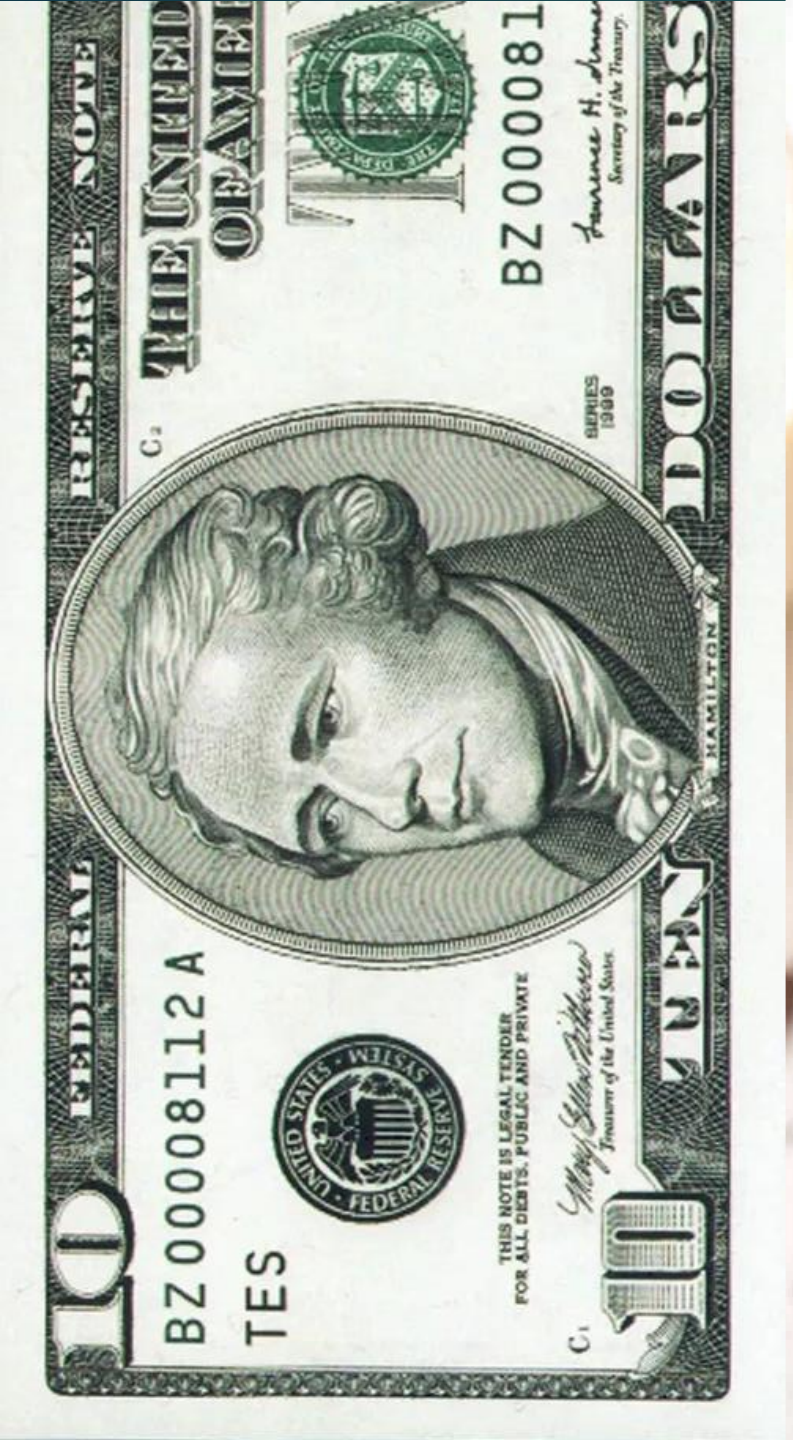


IT-S NOW

10$ for a cookie

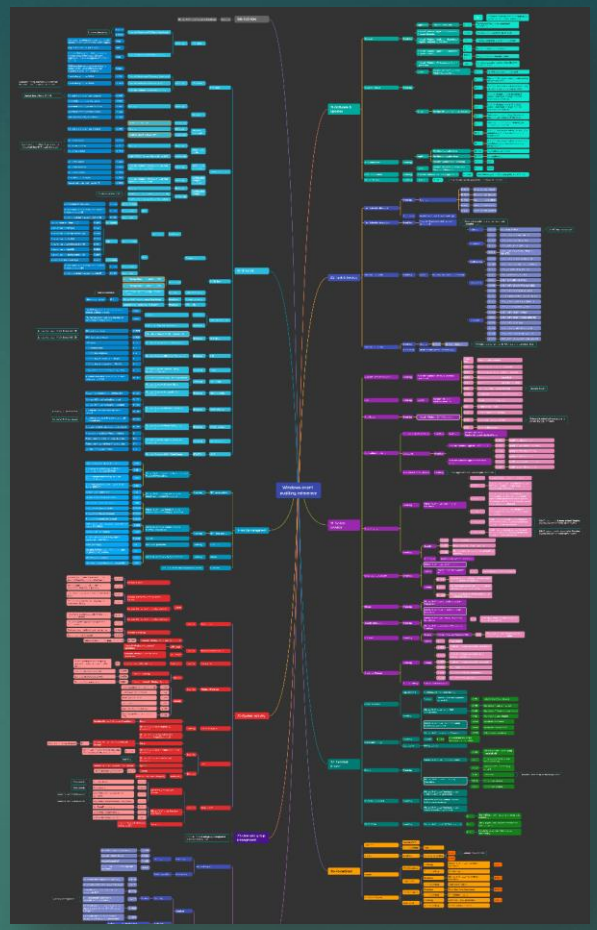
A modern view on the threat detection landscape

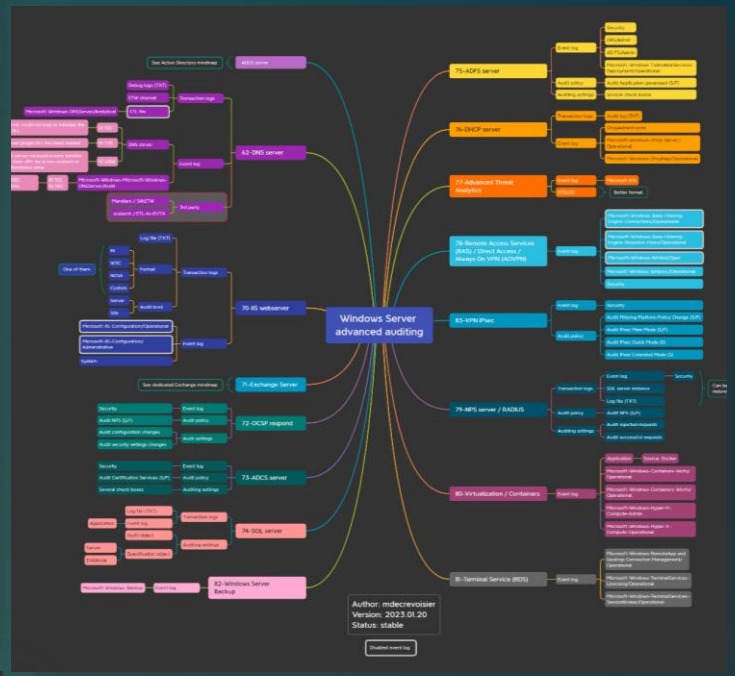
Michel de Crevoisier
SOC / Detection lead
@mdecrevoisier
IT-S NOW 2023

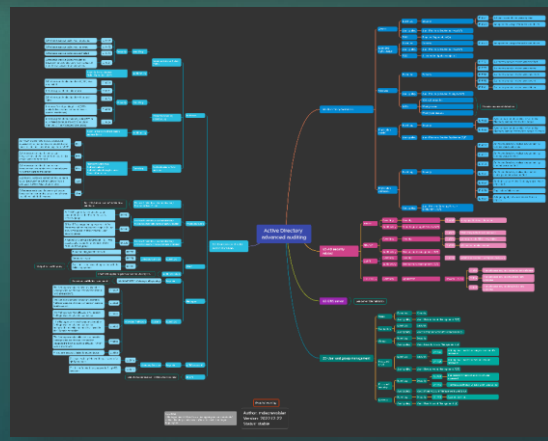
#whoami

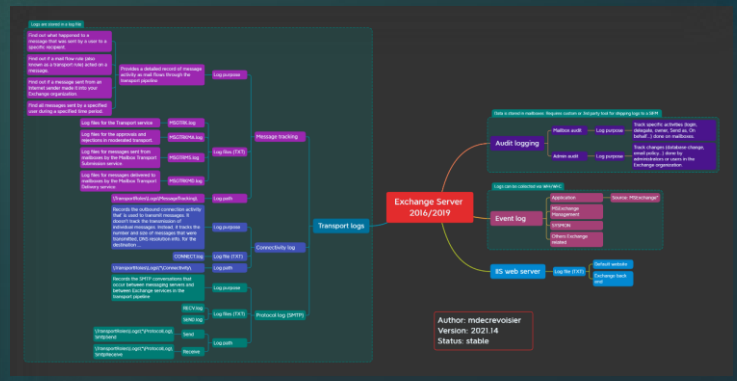
SOC / Detection lead / Senior Security Analyst

- ex Network & System administrator
- Threat bounty developer at SOC PRIME
- Guest contributor at red canary
- Speaker at BSIDES
- Author of several projects:
  - SIGMA-detection-rules (>320 rules)
  - EVTX-to-MITRE-Attack (>270 samples)
  - Microsoft-eventlog-mindmaps









Chained threats

A BRIEF PANORAMA OF THE MODERN THREAT LANDSCAPE

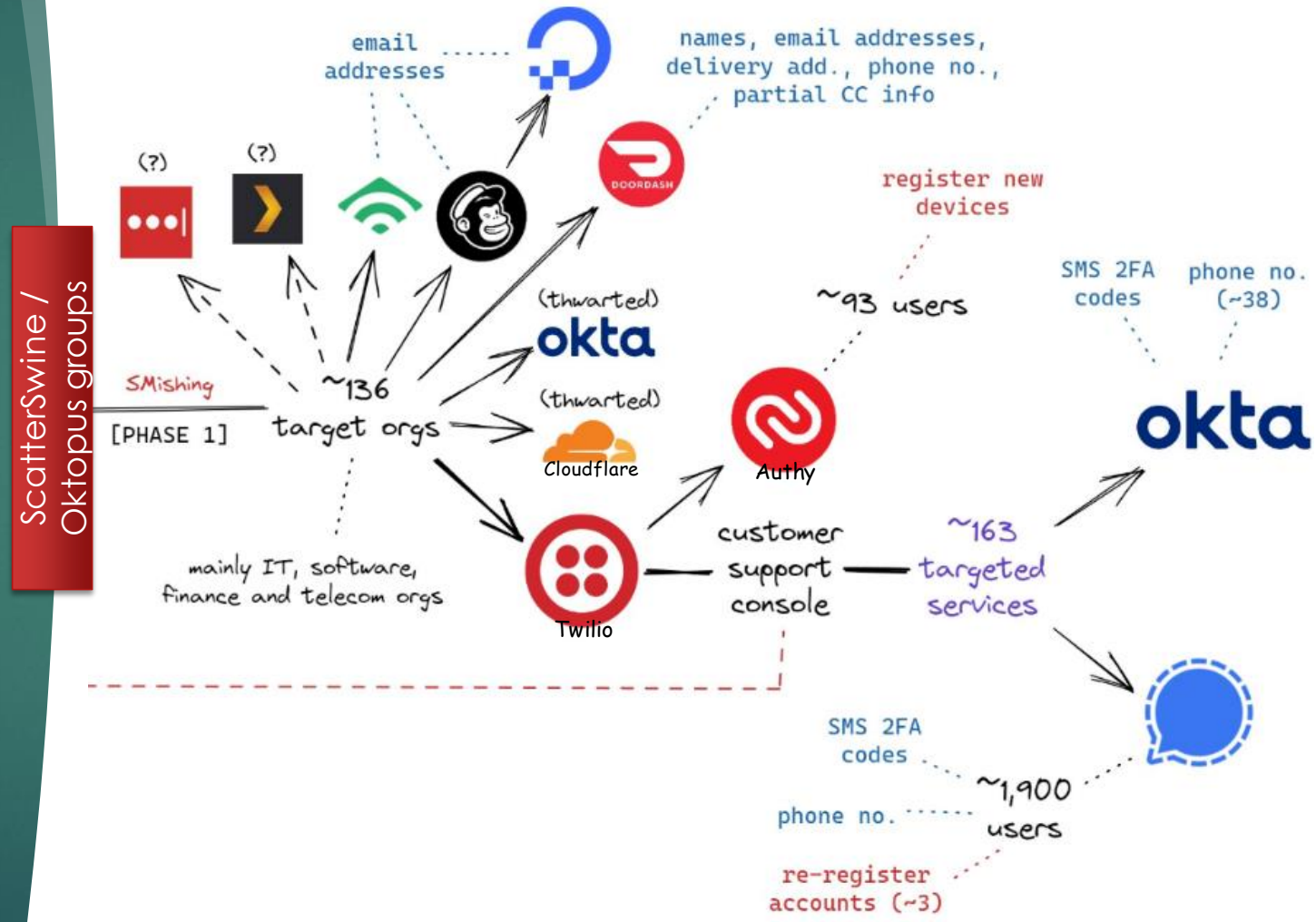
Targeted chained attacks (August 2022)

Digital Ocean
- Digital Ocean's **Mailchimp** account was compromised
- Several customers accounts were breached

Twilio
- Internal systems were breached after stealing employee credentials in an SMS phishing attack

Authy
- 93 Authy users were compromised
- Attackers linked new devices for MFA

Signal
- 1900 users were targeted
- SMS verification code were revealed, allowing new accounts registration



Source: Time Passcodes became a corporate liability (Krebs on Security) August 2022

Compromised tokens, keys and cookies (2021-2023)

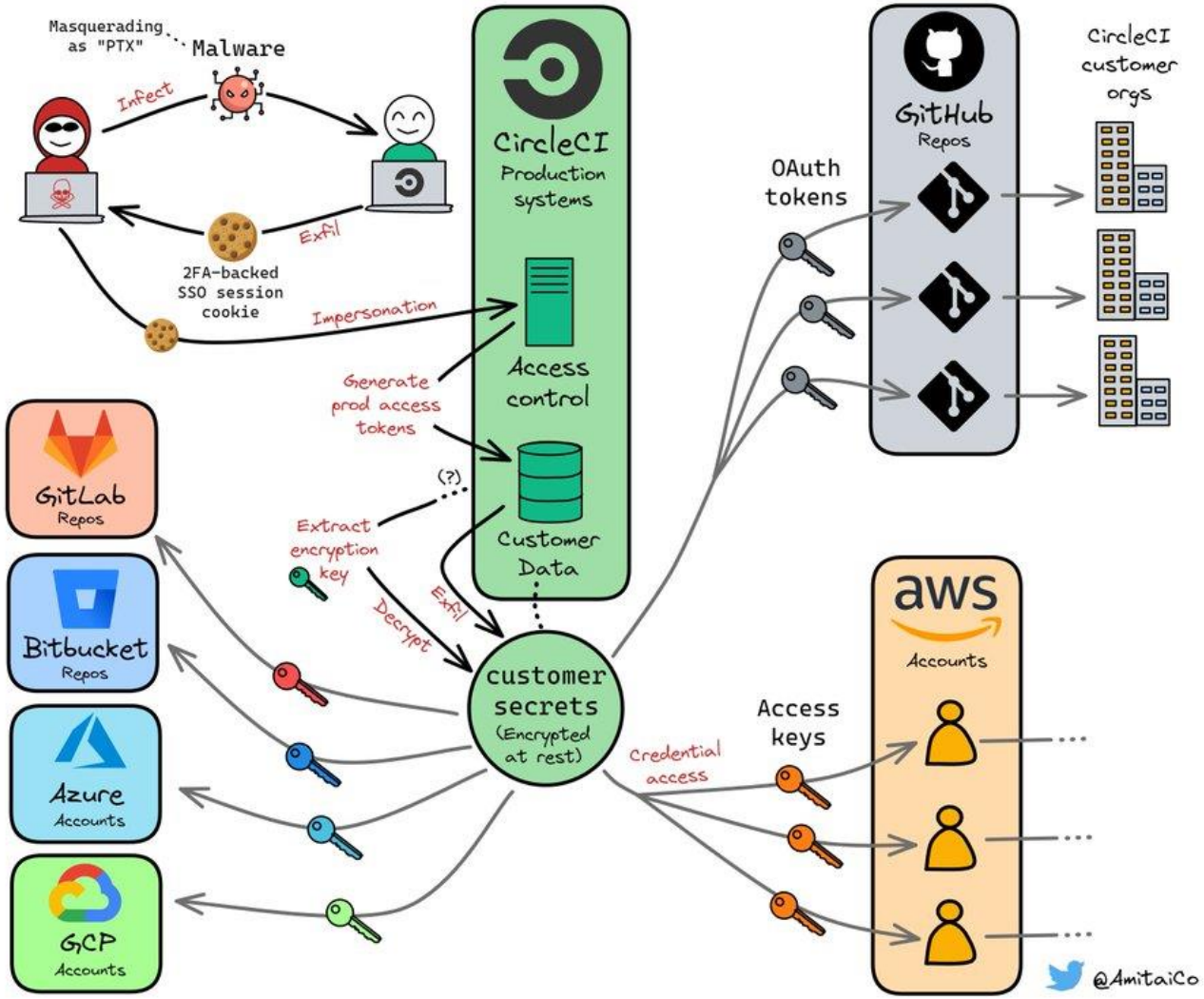
CircleCI December 2022
- Stole 2FA-backed SSO session from a compromised enginer laptop
- Exfiltrated customer tokens and keys

Datadog January 2023
- Signing keys and passphrase were exposed during **CircleCI** breach

Slack January 2023
- Employee's tokens were stolen and misused to gain access to the externally hosted GitHub repository

OKTA March & December 2022
- Private GitHub repositories were hacked
- Lapus$ gained access to admin consoles via 3rd party contractor (Sitel)

Electronic Arts June 2021
- Hack via a10$ stolen cookie from a Slack user
- Requested MFA token to IT support



Source: How CircleCI threat actor *could* have gained access to other orgs @AmitaiCo via Twitter / January 2023

Supply chain attacks on providers

Entrust
August 2022

- Ransomware on giant digital security company
- Breach started 2 months before

Kaseya
2021

- Vulnerability in VSA software used by many MSP

SolarWinds
2019-2020

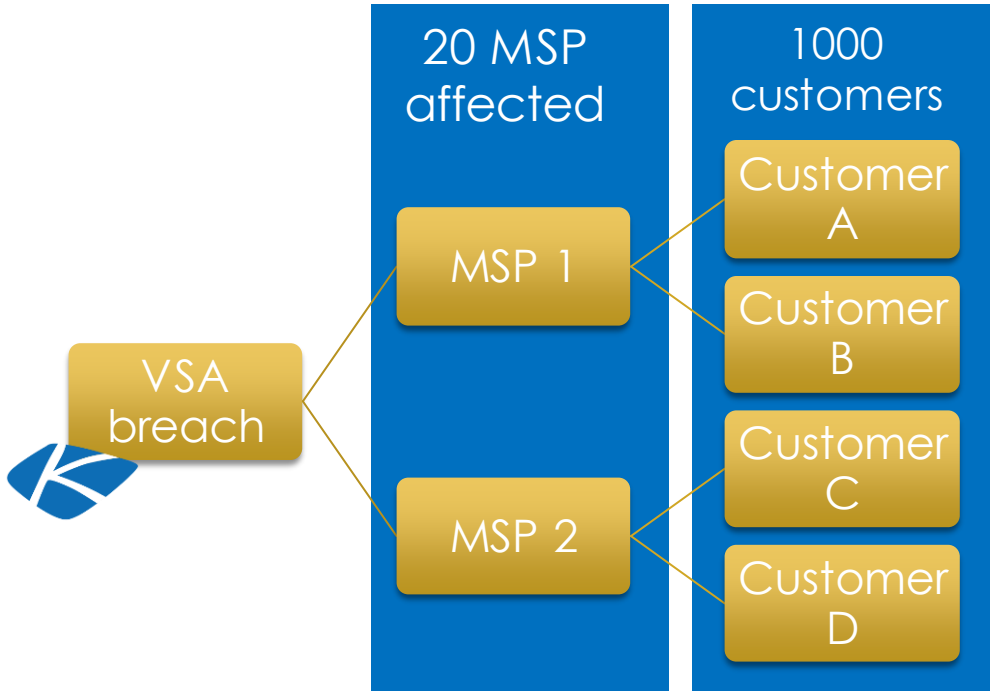
- CI/CD pipeline compromised
- Abused ADFS (Golden SAML) and moved to the cloud

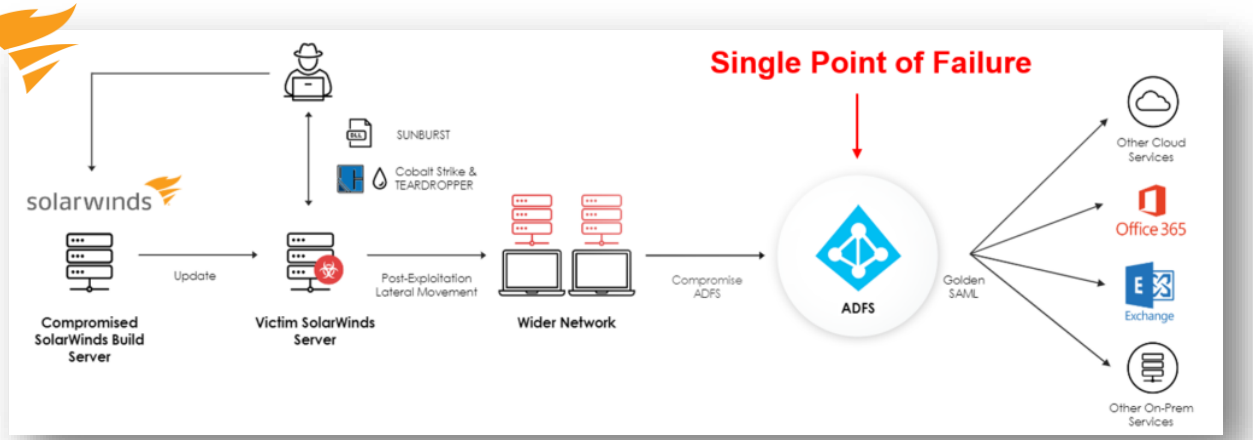
3CX
2022-2023

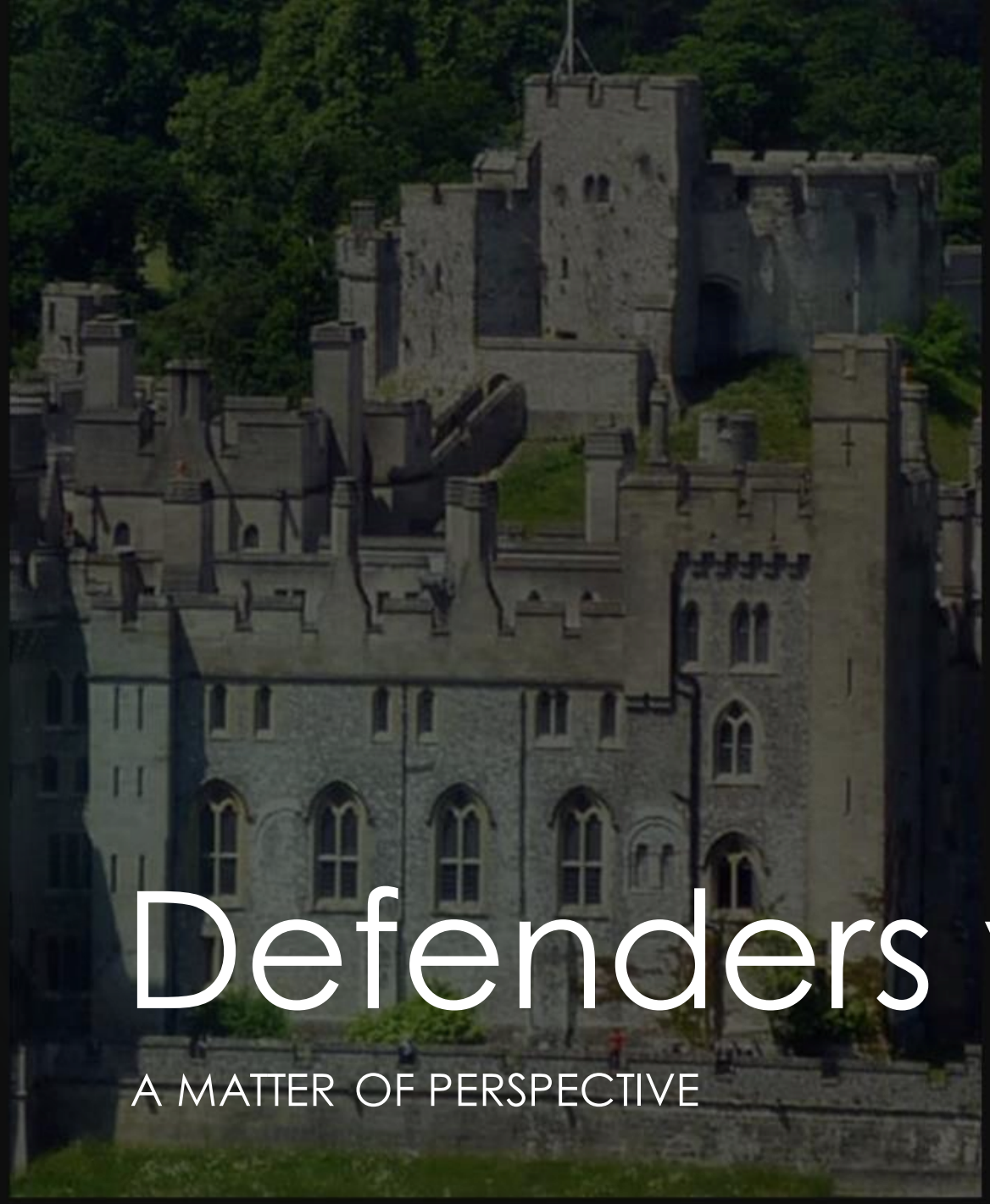
- Trading Tech. Software package breached
- Uses by 3CX to package its software

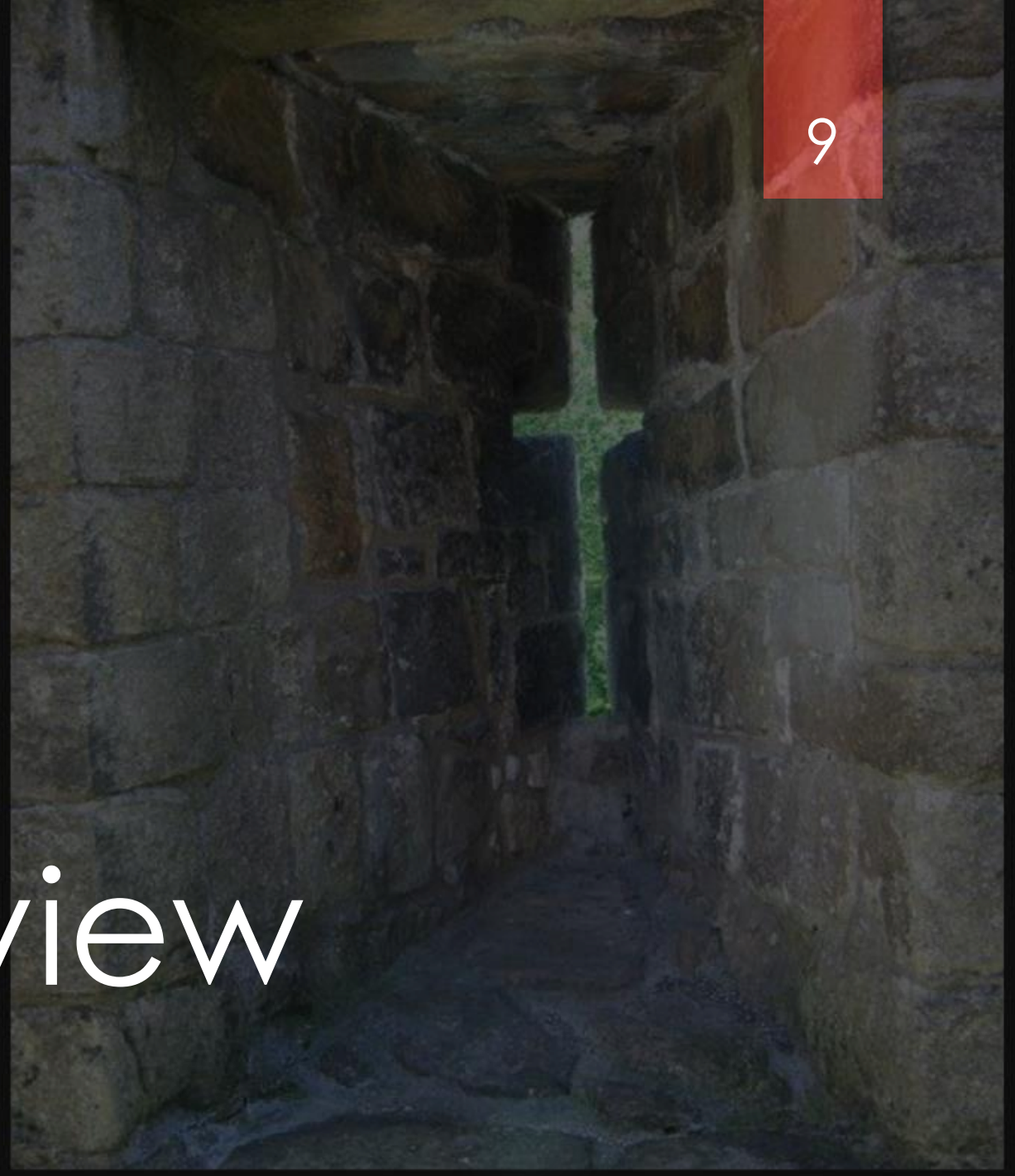
Others

- CodeCov
- ClickStudio (PAM solution)
- Autodesk (via SolarWinds)









Defenders view

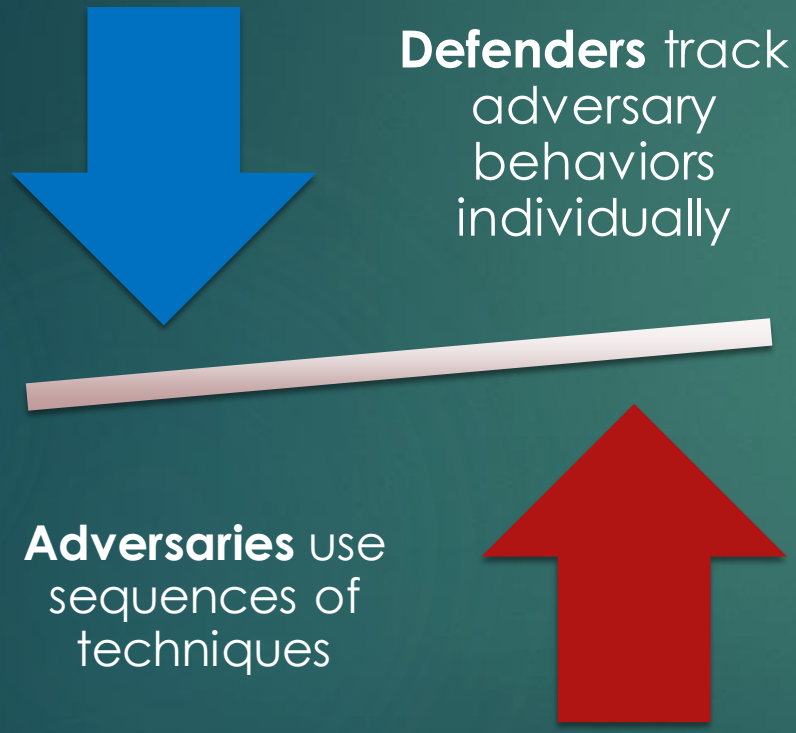
A MATTER OF PERSPECTIVE

The **graph** approach

▶**Source:** John Lambert (@JohnLaTwc) / Microsoft - April 2015

*"**Defenders** think in lists.*
***Attackers** think in graphs.*
As long as this is true, attackers win."

The **sequential** approach



Defenders track adversary behaviors individually

Adversaries use sequences of techniques

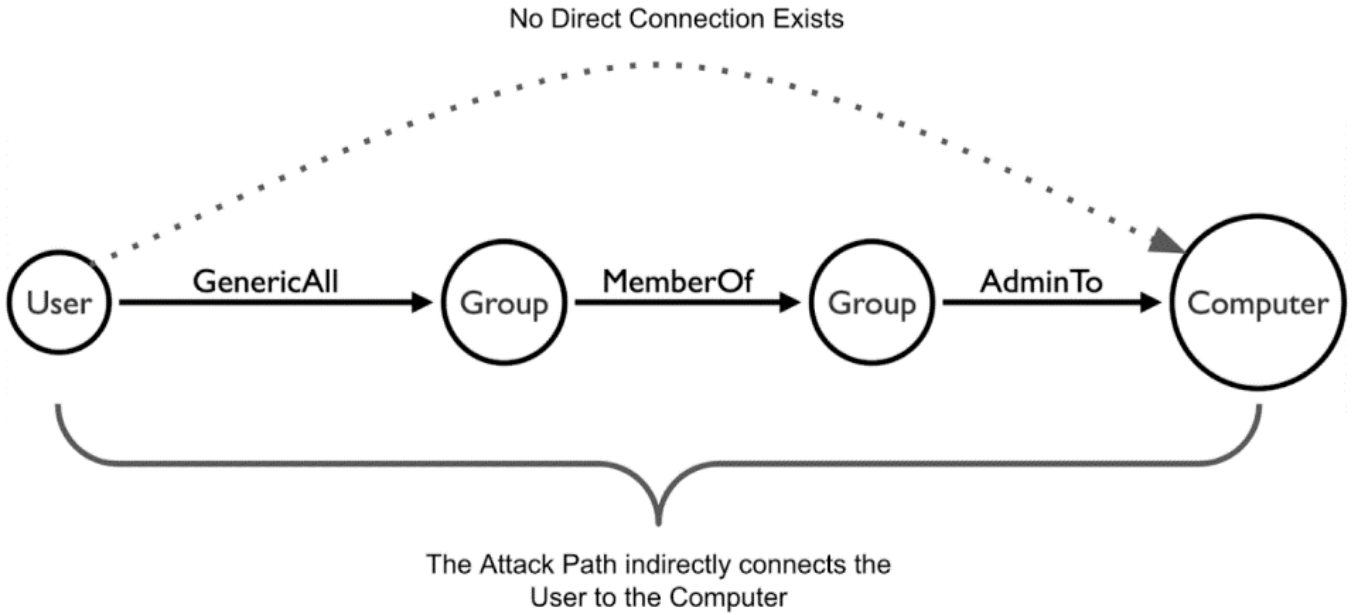
"An attack flow is a machine-readable representation of a sequence of actions and assets, plus knowledge properties"

Source: Attack Flow – Beyond Atomic Behaviors / Steve LUKE - MITRE Engenuity - June 2022

The **attack path** approach

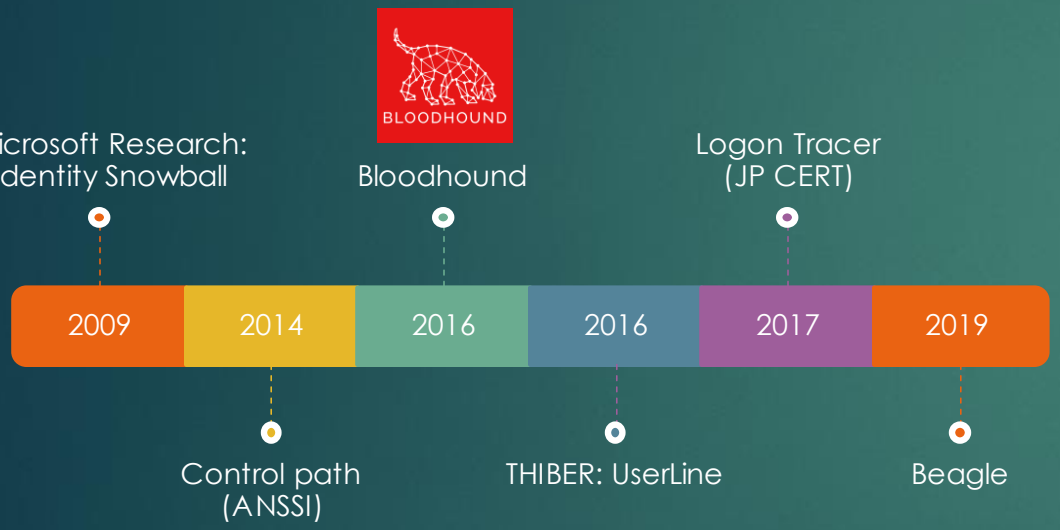
"**Identity snowball attacks** leverage the users logged in to a first compromised host to launch additional attacks with those users' privileges on other hosts."

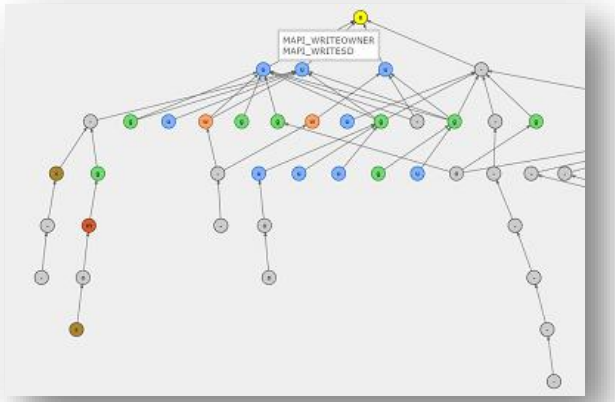
Source: Combating identity snowball attacks using machine learning, combinatorial optimization and attack graphs - Microsoft Research 2009



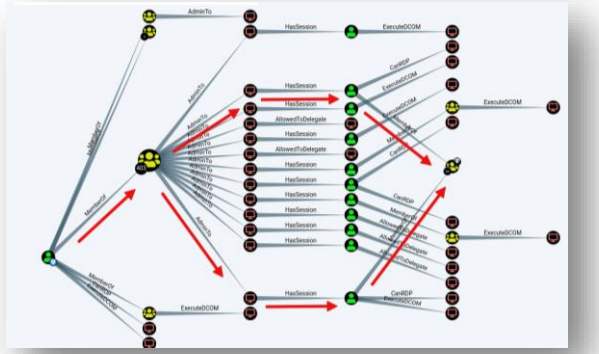
Source: Bloodhound Enterprise website

The **attack path** evolution

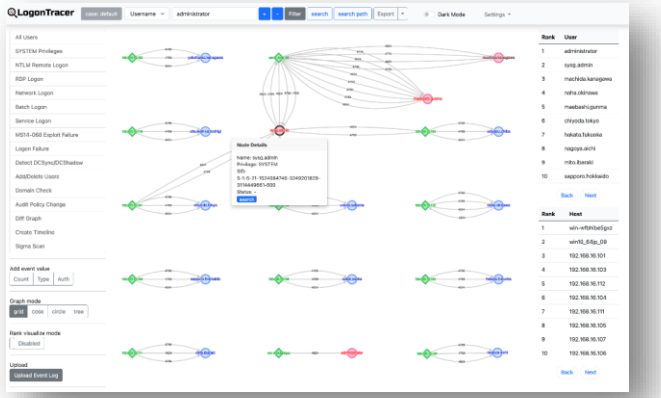




Control path



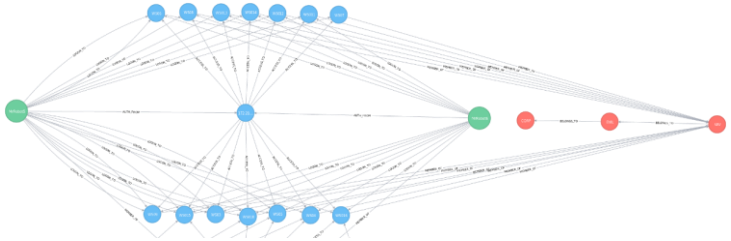
Bloodhound



Logon tracer

UserLine

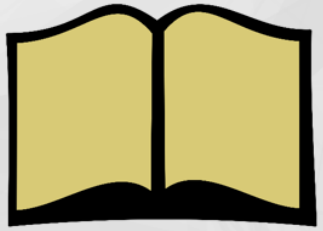
Beagle

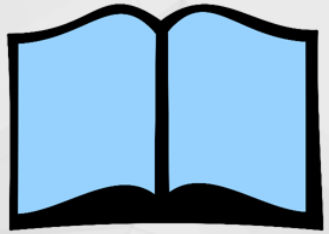


Defenders mindset

A CONTINUOUSLY EVOLVING ROLE

Traditional vs Modern defenders

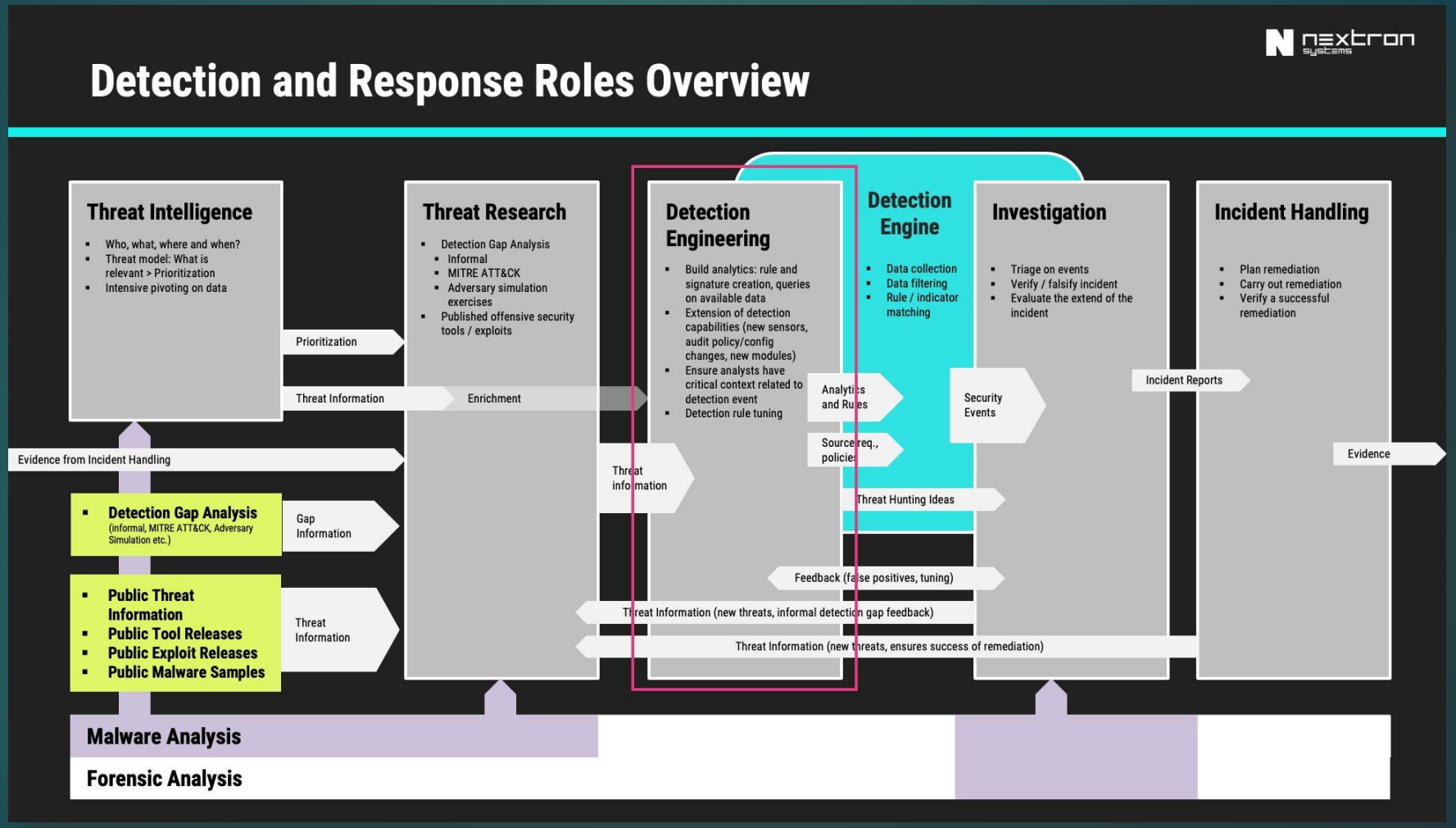




Traditional Defenders	Modern Defenders
Defend a list of assets	Defend a graph of assets
Manage incidents	Manage adversaries
Minimize risks by keeping incidents secret	Maximize learning by sharing incidents with trusted outside peers
View pentest results as a report card	View pentest results as an input
Think about stopping attacks	They think about increasing attacker requirements

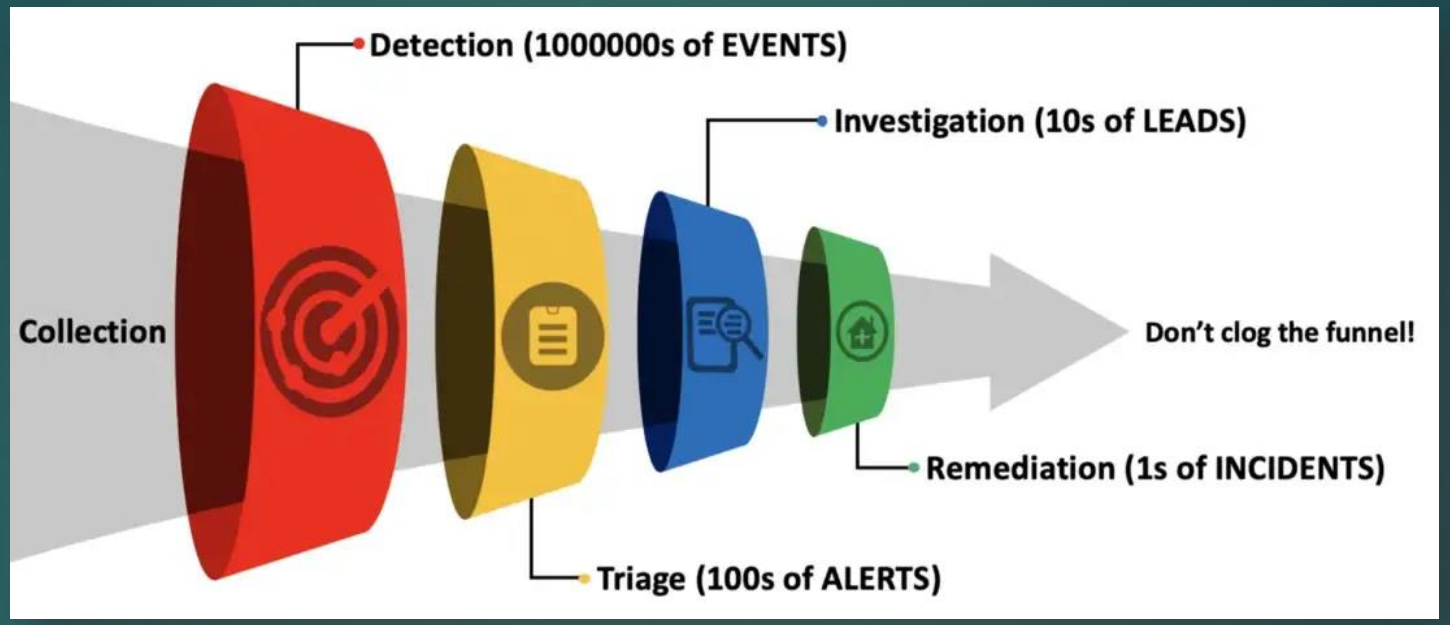
Source: MITRE ATT&CKcon 2018 keynote / John Lambert (@JohnLaTwc)
Microsoft - 2018

Modern defenders roles



Source: Florian ROTH (@cyb3rops) - NEXTRON – June 2021

The defender funnel



Source: Funnel of fidelity - Jared Atkinson / SpecterOps - 2019

SOAR
(Security Orchestration, Automation and Response

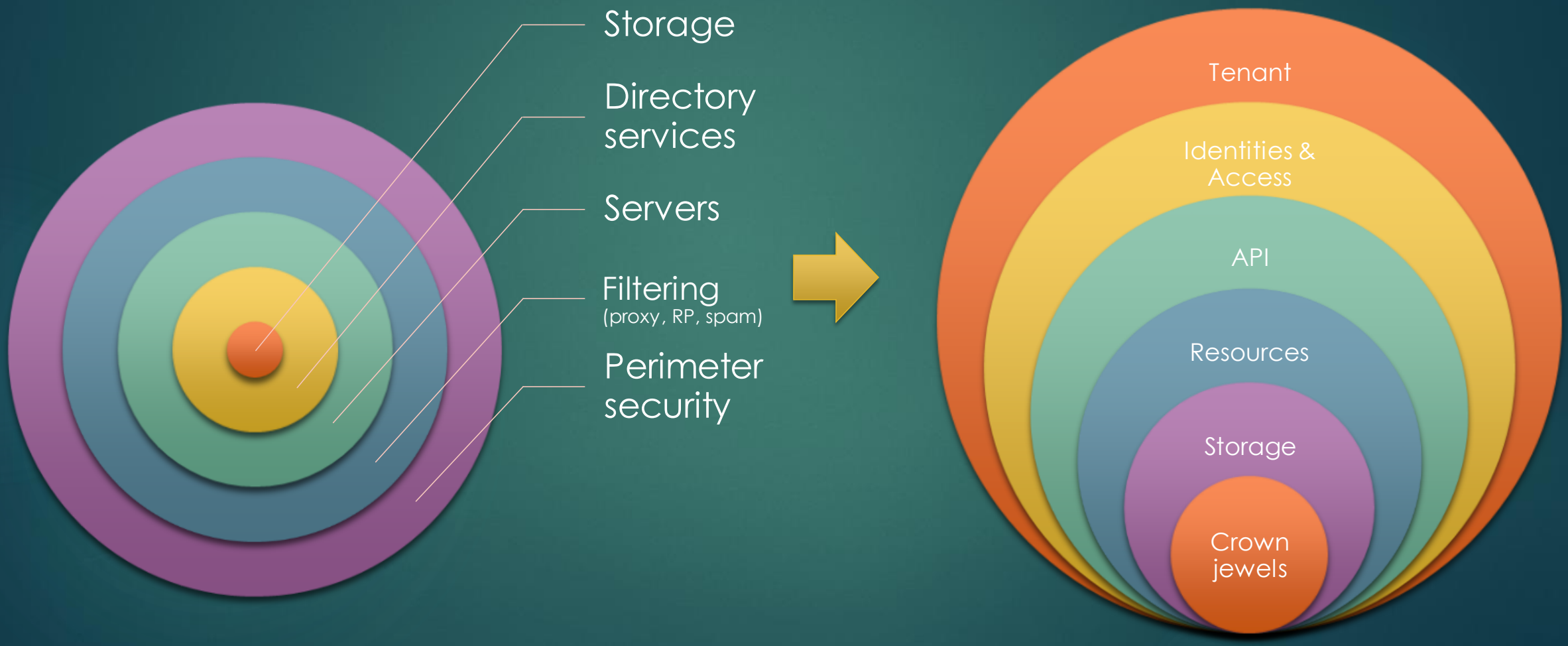
Collection	Detection	Triage	•Investigation	•Remediation
• **Role**: Data Engineer • **Input**: Data Sensors • **Output**: Events	• **Role**: Detection Engineer • **Input**: Events • **Output**: Alerts	• **Role**: SOC Analyst (T1/2) • **Input**: Alerts • **Output**: Leads	• **Role**: SOC (T2/3) or Forensic Analyst • **Input**: Leads • **Output**: Incidents	• **Role**: Incident Responder • **Input**: Incident • **Output**: N/A

And the cloud came…

Azure

aws

Onion layer principle evolution



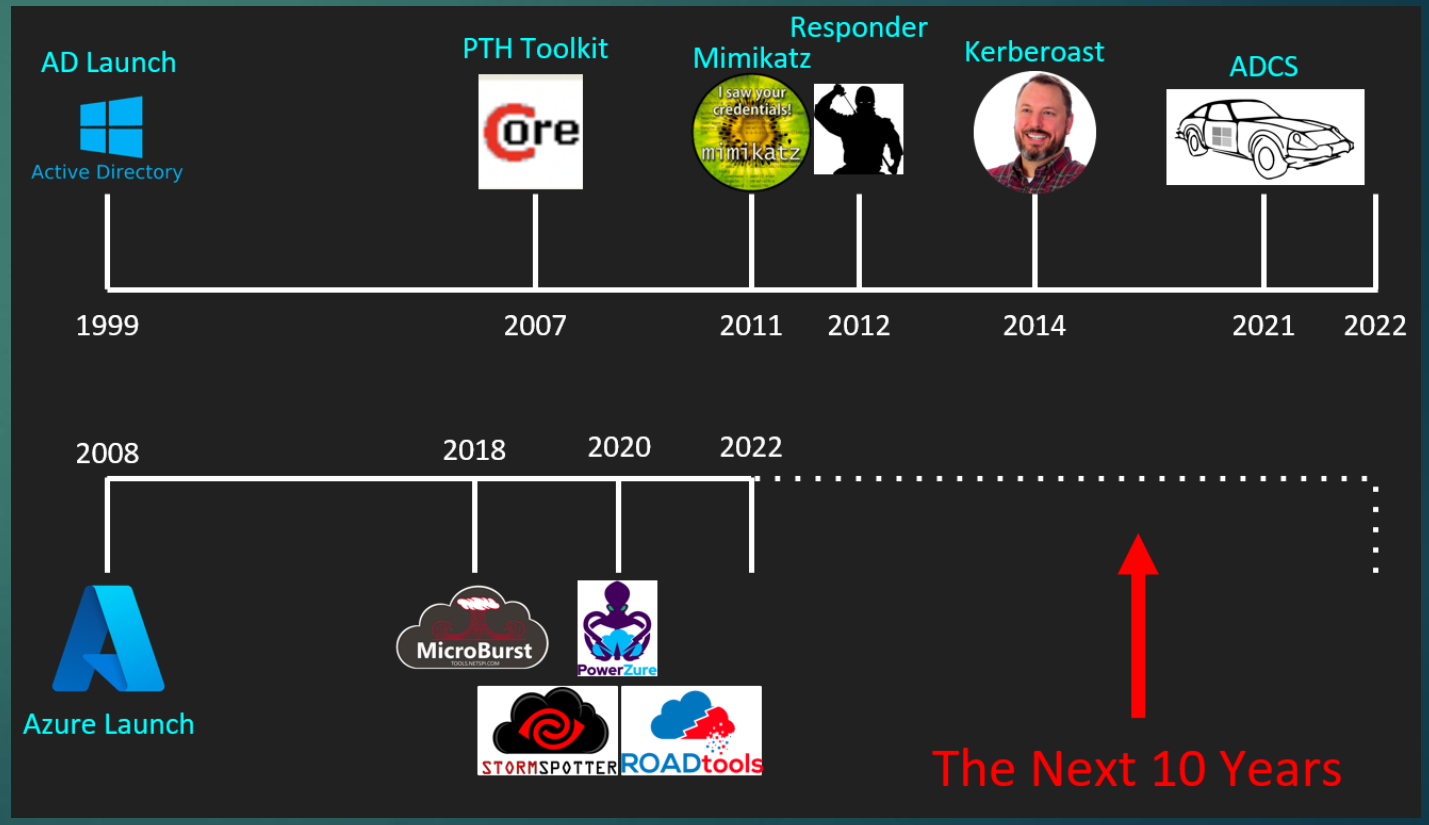
Attacking the cloud

From on premise to Cloud

Server	→	Services
Domain	→	Subscriptions
Domain Admin	→	Subscription Admin
Pass the Hash	→	Credential Pivot
Private IPs	→	Public IPs
ACLs	→	NSGs
RDP/SSH	→	Management APIs

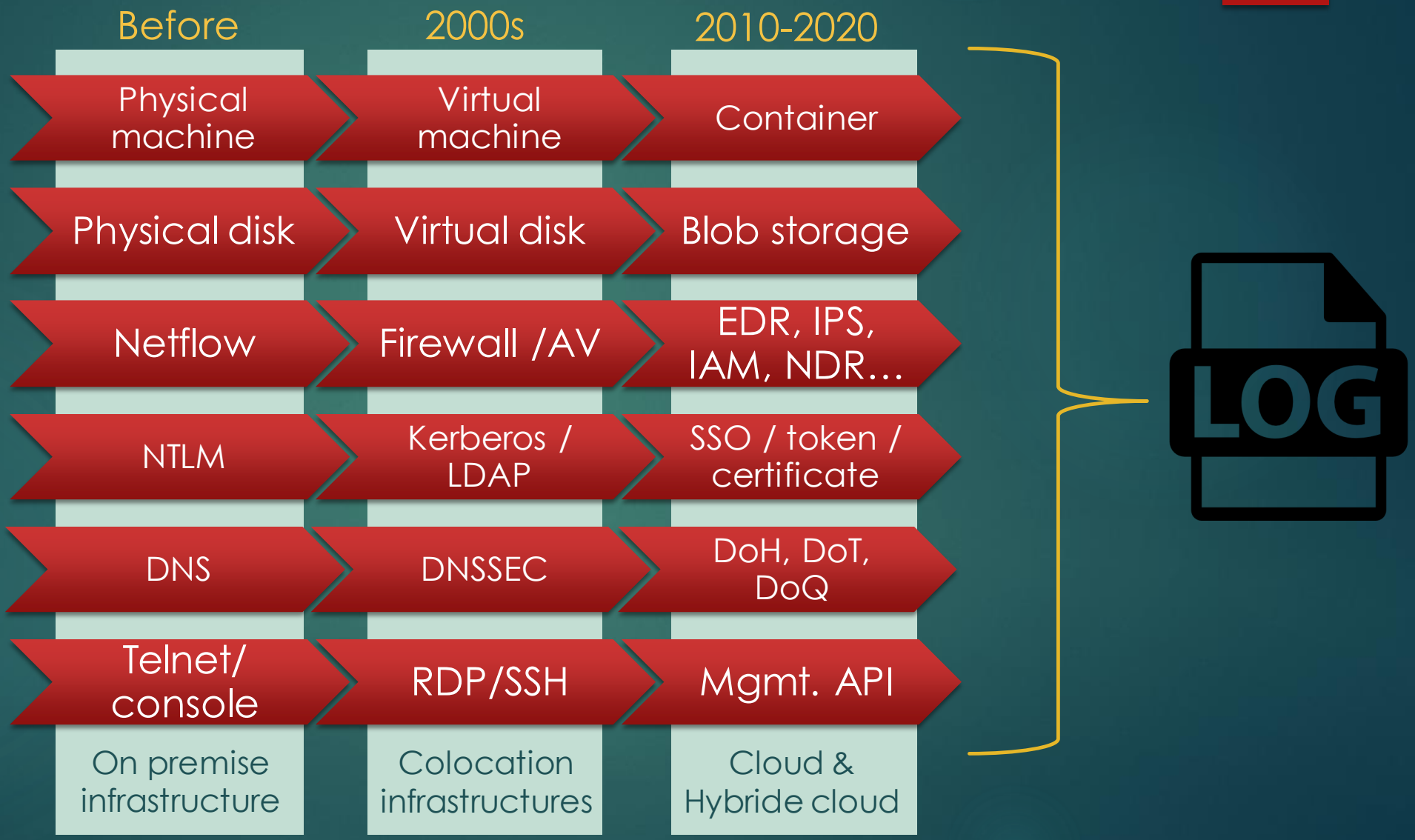
Source: original from Sean Metcalf in 2017, updated by @maarten_goet in 2019

Tools evolution



Source: Attacking and defending Azure - SpecterOps

Digital investigation complexification



The log source challenge

Log source assessment

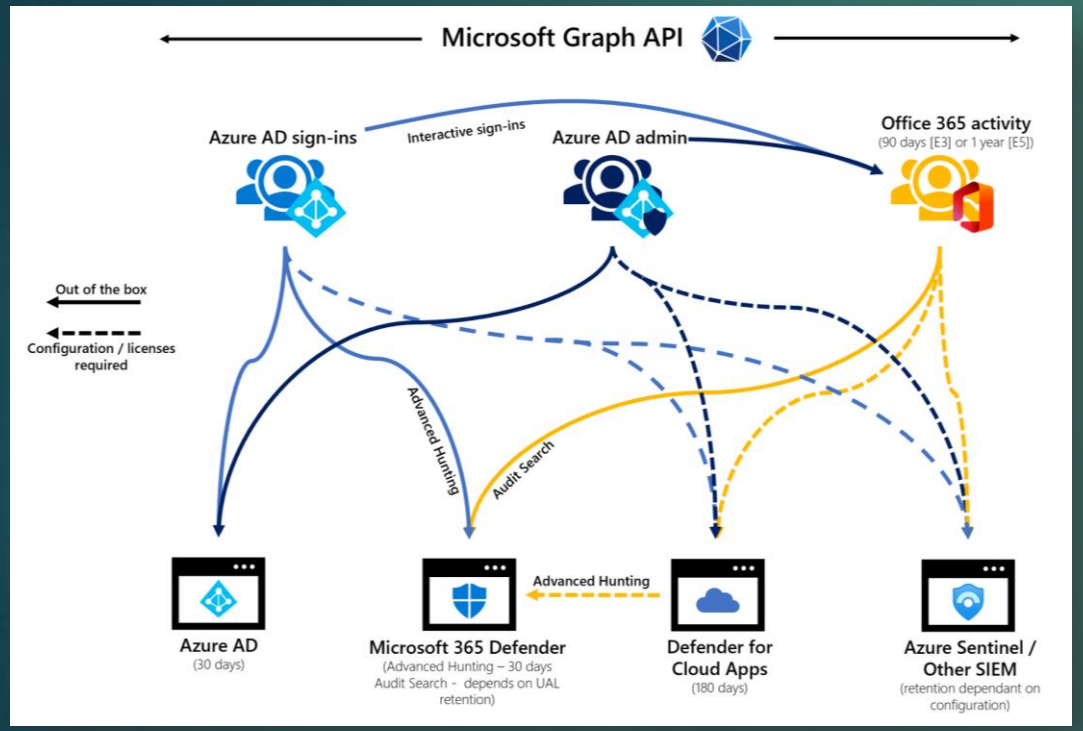
Log Source	Volume[11]	IOC Matching	Threat Hunting	Audit Trail[9]	APT Detection[10]
Antivirus	Low	-	++[3]	+	+++
Windows & Sysmon	Medium[8]	++[1]	+++[4]	++	++
Proxy	Medium	++[2]	+[5]	++	+
NIDS/NSM[7]	Medium	+[2]	+	+	+
DNS	High	++[2]	+[5]	+	+
Mail[6]	Medium	+	-	+	-
Firewall	High	+[2]	-	++	-
Linux (auditd)	Medium	-	+	+	-

High
Priority
Low

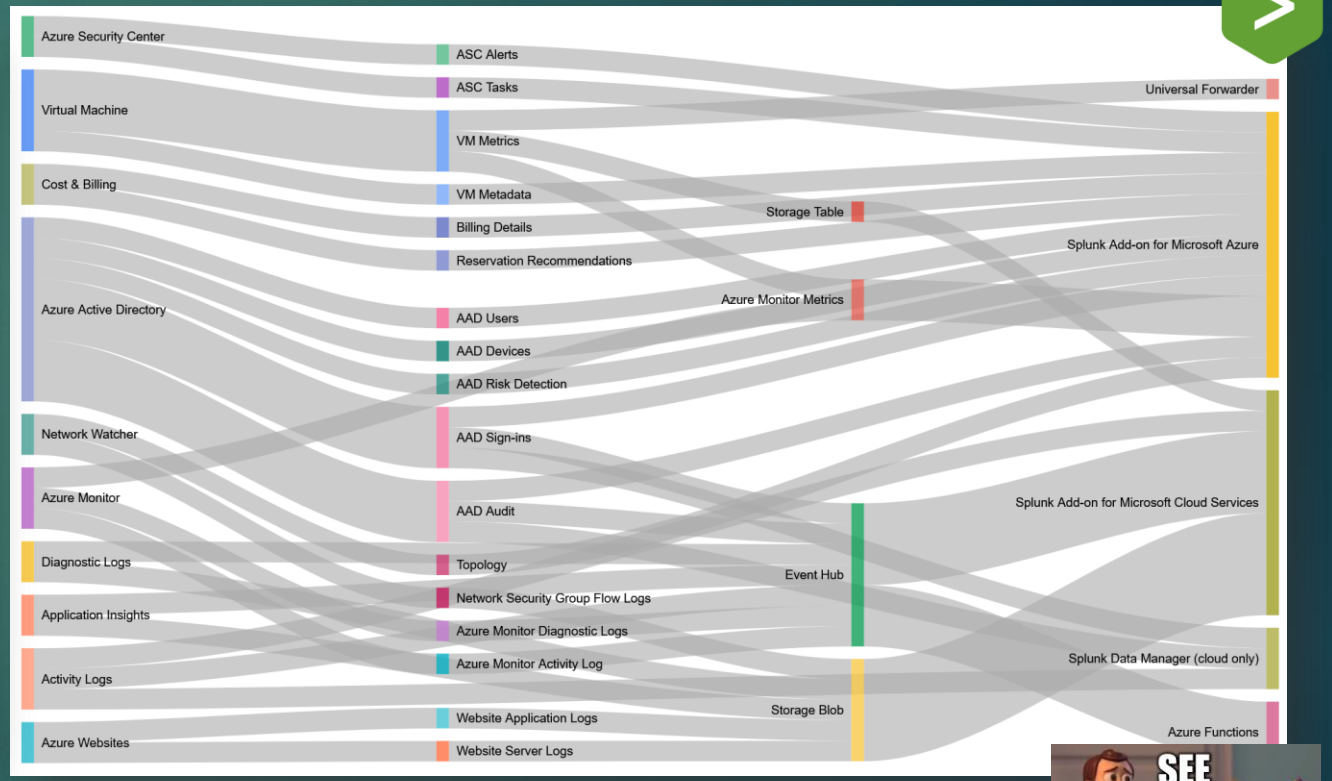
1 – File hash values (MD5, SHA1, SHA256)
2 – C2 IPs oder domain names
3 – see „Antivirus Event Analysis Cheat Sheet"
4 – Sigma can help a lot
5 – Patterns (URL, hostname), suspicious TLDs
6 – No personal experience with this log source but highly recommended by others
7 – Suricata, Zeek or alike
8 – Depends mainly on audit policy (use Microsoft Baseline) and Sysmon config
9 – Usefullness in reconstruction of events
10 – How useful are these logs in the detection of persistent threats (reconnaissance, backdoors, lateral movement)
11 – Depends on audit policy and filters (rule of thumb)

Source: Florian ROTH (@cyb3rops) – Tweet posted in January 2020

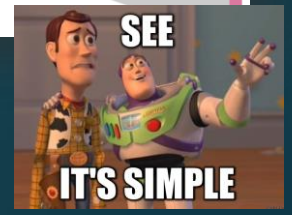
You said « grab cloud logs » ?



Source: Forensic artifacts in Office 365 and where to find them – Microsoft 2022



Source: Splunk Azure GDI from Jason Conger



Data gathering with a SIEM

Logging strategy challange

Requirements	Auditing	Cache	Collecting
•TTPs •DFIR •Compliance •Detection use cases	•What is required to be audited on the systems •Which logs are required to be enabled	•Which log file size •3rd party agent local cache usage	•What needs to be collected in regards of the requirements •Noise reduction
Which inputs to read ?	Which audit settings ?	For how long ?	What to allow or deny ?

No real complete toolset available, from requirements definition to agent configuration.

EDR under attack

A NEW KEY PLAYER / FOCUS ON EVASION OPERATIONS

EDR evasion operations

Avoiding the EDR

- This can be accomplished by operating from VPN, proxying traffic, or compromising only targets not equipped with EDRs.

Blending into the environment

- Executing operations abusing tools and actions commonly observed in the target network (eg: RDP, remote control tools, Teams, Process Monitor …)

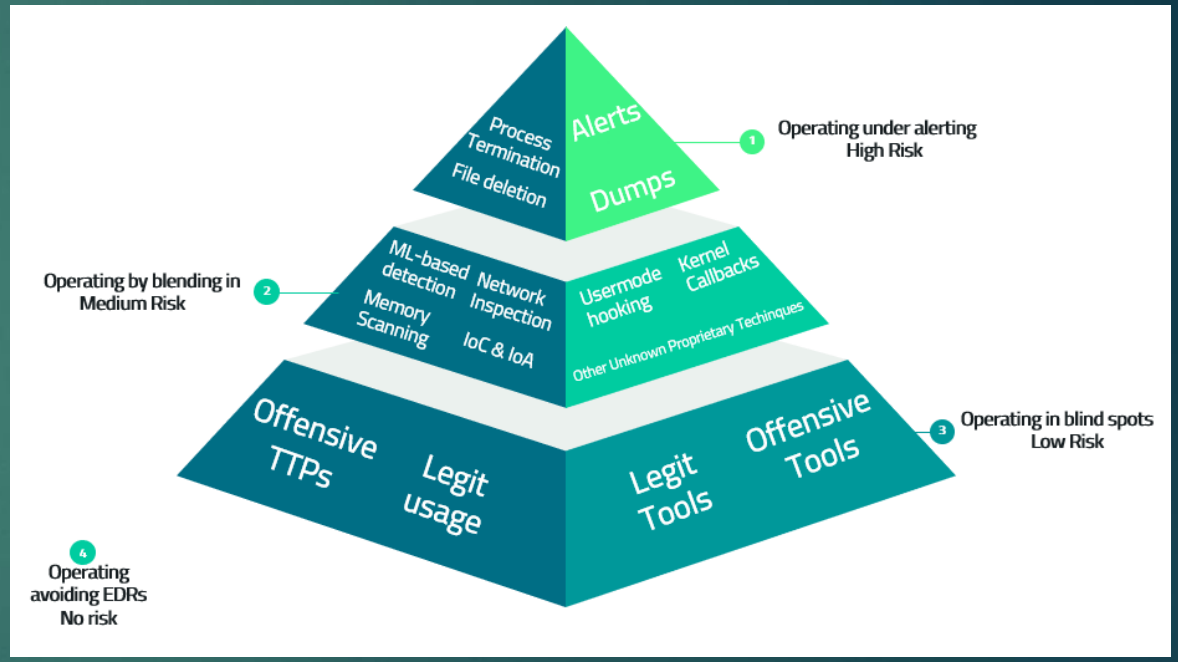
EDR tampering

- This category involves disabling or limiting EDR's features or visibility in order to perform tasks without triggering an EDR response or without sending alerts.

Operating in blind spots

- EDR have finite resources and finite visibility, so blind spots are always present.

Attacker's pyramid of pain - Mapping risk levels to EDR evasion category



Source: Living-Off-the-Blindspot - Operating into EDRs' blindspot – September 2022

EDR tampering

Techniques

- ★BYOVD
- ETW bypass
- AMSI bypass
- NG wiper
- LOLBINS
- WSL (Subsystem for Linux)
- DLL side loading
- User mode hooking
- Kernel routines removal
- Kernel callbacks
- […]

MITRE ATT&CK™ T1068-Priv. escalation

Bring Your Own [Vulnerable] Driver

2023 Terminator	• Driver signed by Zamana antimalware solution *zamguard64.sys* (source)
2022 Sunlogin driver	•Sunlogin remote control utility (from Oray company) - CNVD-2022-10270 / CNVD-2022-03672 (ASEC)
2022 AMD driver	•AMD's Ryzen master driver v17 (GitHub) •CPU overclocking control
2022 Scattered Spider	•Intel Ethernet diagnostic drivers *iqvw64.sys* - CVE-2015-2291 (Crowdstricke)
2022 BurntCigar malware	•Signed with a legitimate WHCP certificate (Sophos)
2021 Lazarus group	•Dell DBUtil drivers - CVE-2021-21551 (ESET)
2021 Cuba ransomware	•Avast driver *aswArPot.sys* (AON)
2019 BlackByte ransomware	•Micro-Star's MSI AfterBurner •Graphics card overclocking utility *RTCore[32/64].sys* (Sophos)

EDR tampering

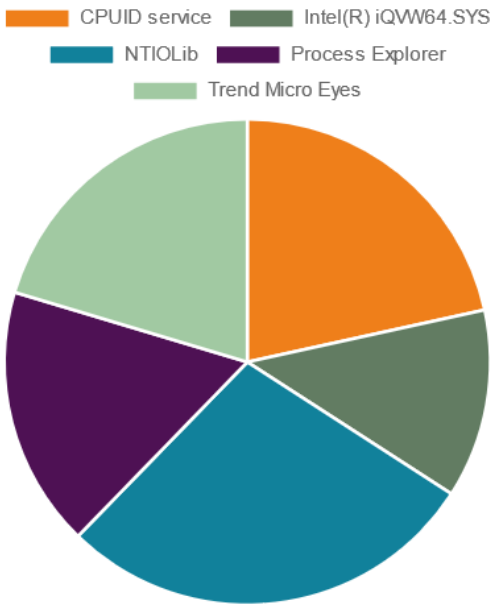
Techniques

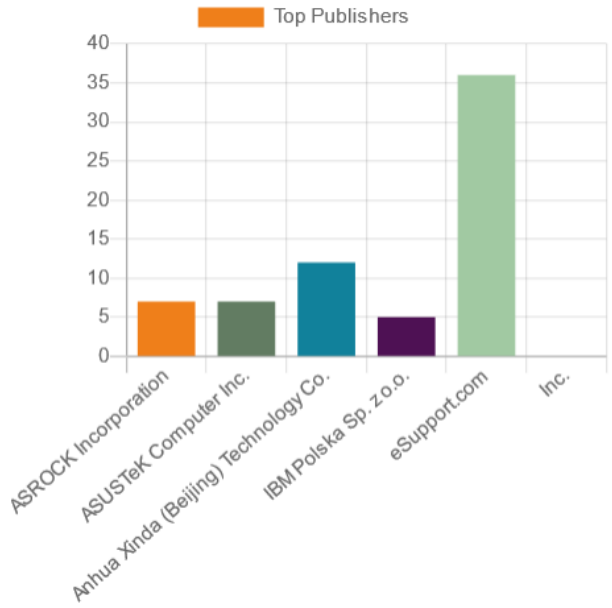
- ★BYOVD
- ETW bypass
- AMSI bypass
- NG wiper
- LOLBINS
- WSL (Subsystem for Linux)
- DLL side loading
- User mode hooking
- Kernel routines removal
- Kernel callbacks
- […]

MITRE ATT&CK™ T1068-Priv. escalation

Bring Your Own [Vulnerable] Driver

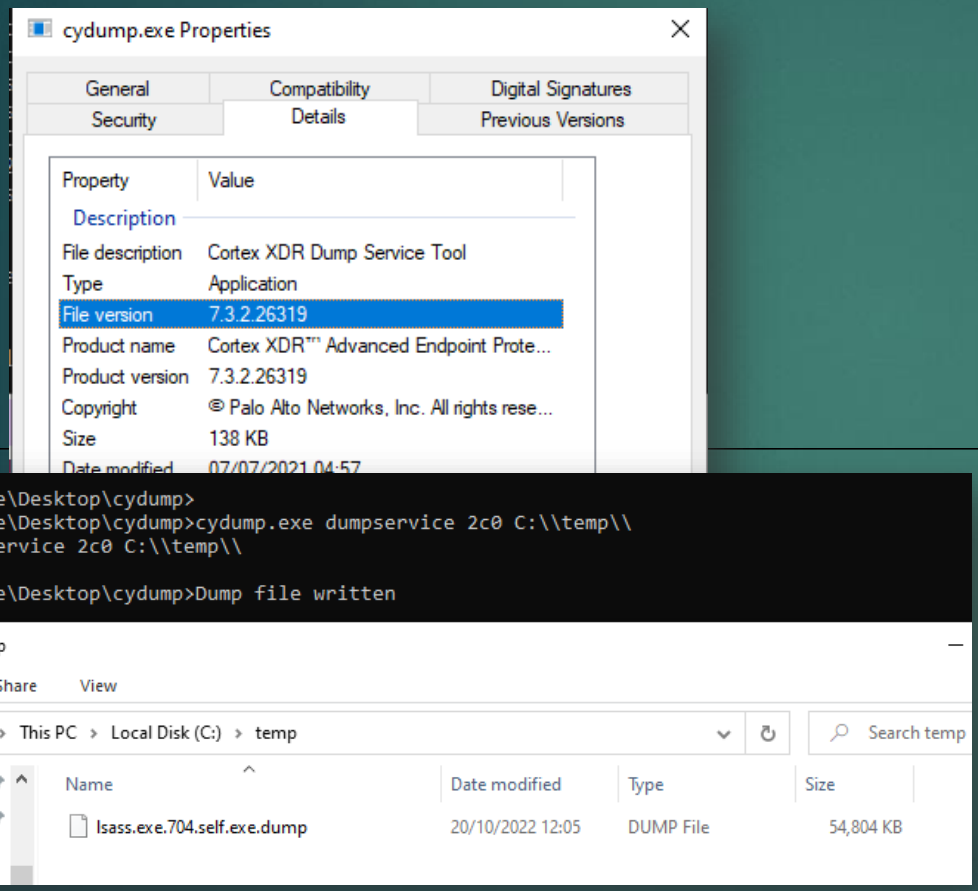
Top Products





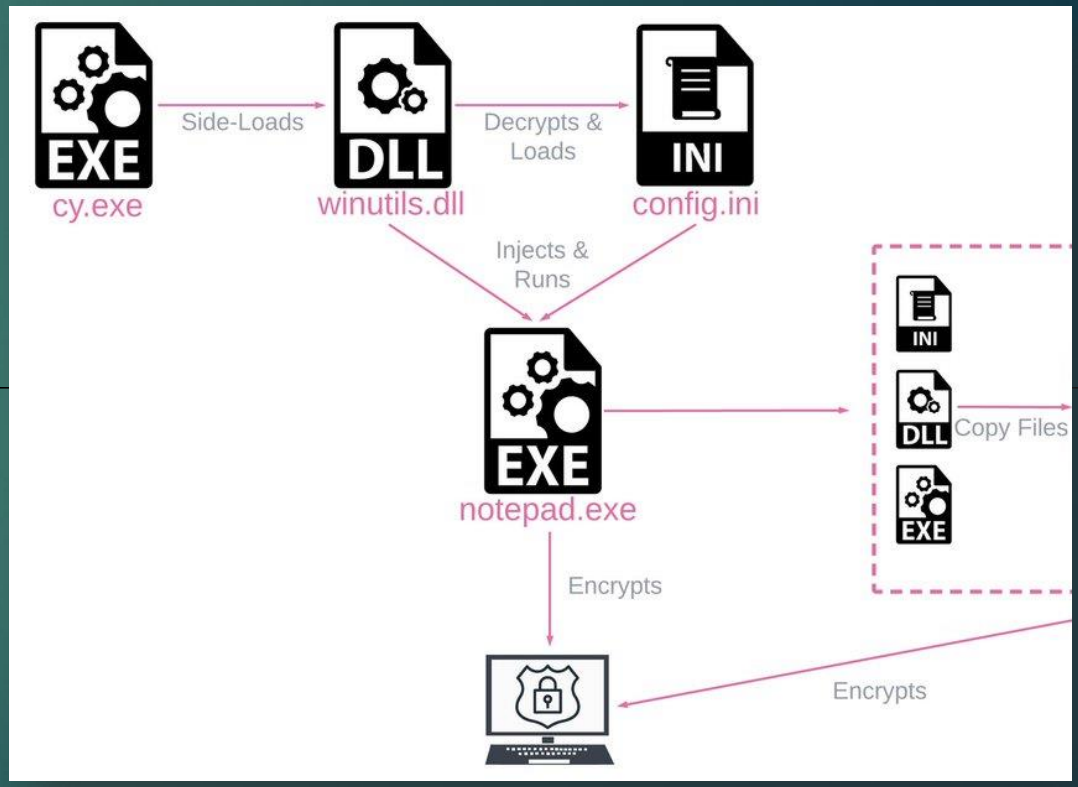
EDR FAIL

Dumping LSASS with **Palo Alto Cortex XDR** "cydump.exe" tool (patched in July 2021)



Source: Randsec – July 2022

DLL sideloading with **Palo Alto Cortex XDR** "cy.exe" tool



Source: "Rorschach: a new sophisticated ransomware" - Checkpoint – April 2023

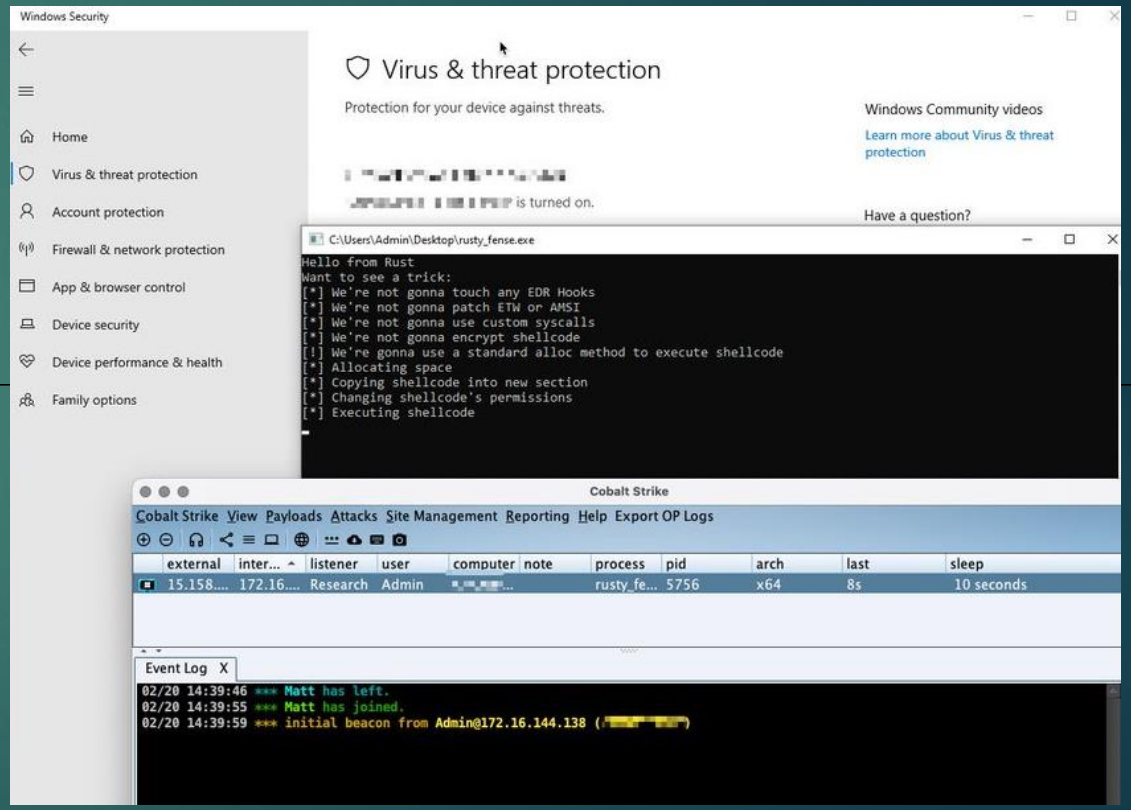
EDR FAIL

OKTA breach: LAPSUS downloaded "Process Hacker" and terminated the **FireEye HX** service agent.
(was tamper protection on ?)

Date (UTC)	Event	Attack Phase
2022-01-16 00:33:23	First logon event from [SYSTEM NAME REDACTED]. Logon to [SYSTEM NAME REDACTED] from [SYSTEM NAME REDACTED] (10.112.137.64)	Initial Compromise
2022-01-19 19:19:47	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Initial Compromise
2022-01-19 19:45:39	Bing search for Privilege escalation tools on Github by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01 19:47:58	UserProfileSvcEop.exe downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:31:19	Account [ACCOUNT NAME REDACTED] created on [SYSTEM NAME REDACTED]	Maintain Presence
2022-01-20 18:32:32	RDP logon by [ACCOUNT NAME REDACTED] from LOCAL to [SYSTEM NAME REDACTED]	Move Laterally
2022-01-20 18:39:43	Bing search for Process Explorer by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:40:04	Process Explorer executed by [ACCOUNT NAME REDACTED]	Internal Recon
2022-01-20 18:43:51	Bing search for Process Hacker by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:01	Process Hacker downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:44:17	Process Hacker execution by [ACCOUNT NAME REDACTED]	Establish Foothold
2022-01-20 18:46:22	FireEye Endpoint Agent service terminated on [SYSTEM NAME REDACTED]	Establish Foothold
2022-01-20 18:46:55	Bing search for Mimikatz by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:48:28	Mimikatz downloaded from hxxps://github.com by [ACCOUNT NAME REDACTED]	Escalate Privileges
2022-01-20 18:50:10	Mimikatz executed by [ACCOUNT NAME REDACTED] on [SYSTEM NAME REDACTED]	Escalate Privileges

Source: @BillDemirkapi - January 2022

Offensive Rust – More and more ransomware groups are abusing it since 2022
(cross platform, LLVM base, bypass static analysis…)



Source: A closer look at rust based malware - February 2023

EDR configuration extraction

MITRE ATT&CK™ | T1518.001 - Software Discovery: Security Software Discovery

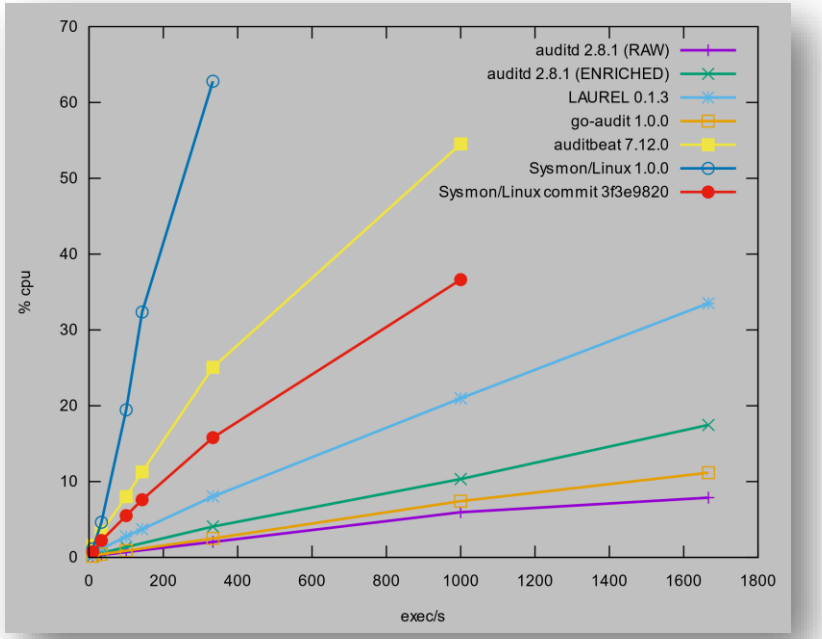
- •Uninstall Password Hash & Salt
- •Excluded signed Names
- •DLL Security Exclusions & Settings
- •Office Files Security Exclusions & Settings
- •Credential Gathering Module Exclusions
- •Webshell Protection Module Exclusions
- •Childprocess Executionchain Exclusions
- •Behavorial Threat Module Exclusions
- •Local Malware Scan Module Exclusions
- •Memory Protection Module Status
- •Global Hash Exclusions
- •Ransomware Protection Module Modus & Settings

Detection tools

A COMPLEMENTARY DETECTION APPROACH

Modern host detection tools

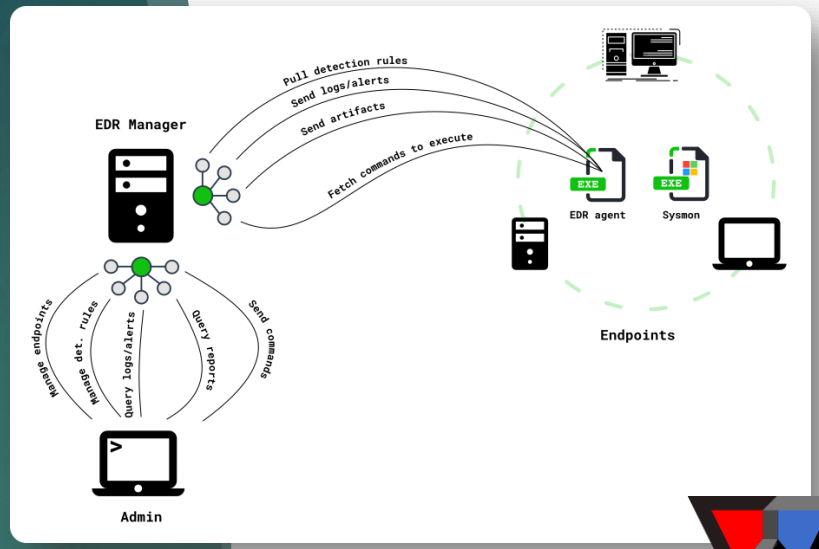
Auditd	From RedHat
OS Query	Released in 2014 To combine with fleet
Audit-beat	Released in 2017
Symon	Released in 2021 Relies on eBPF
Laurel	Released in 2021 Post-processing event plugin for auditd

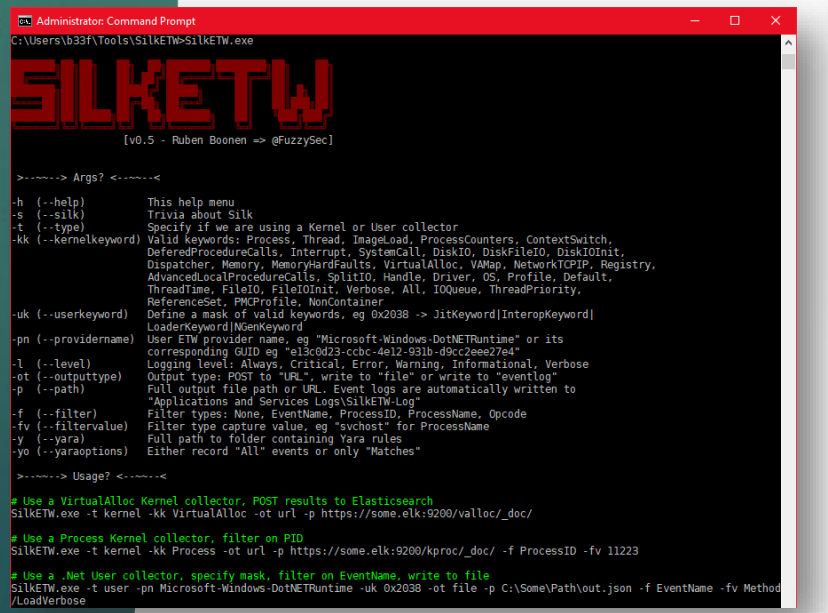


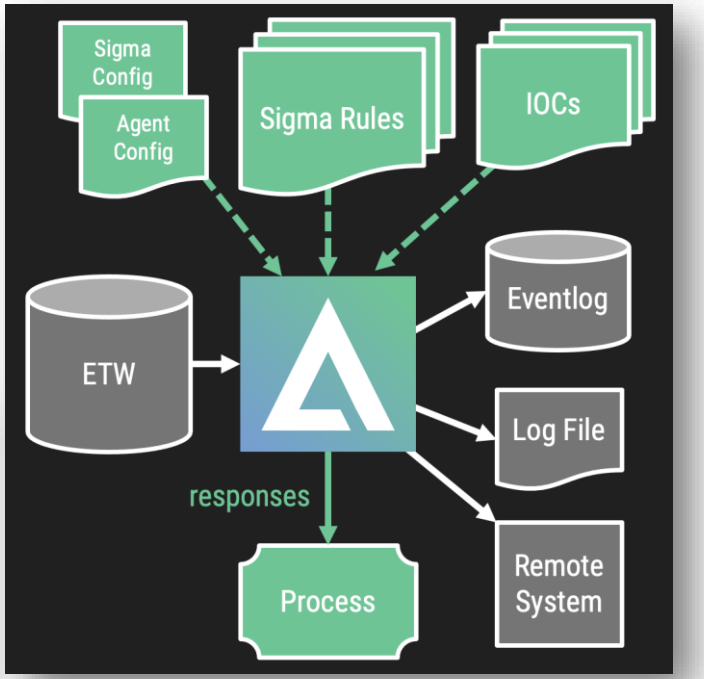
Source: Laurel's Github – October 2021

Modern host detection tools

Native logs	Breaking change in event logging infrastructure following Windows Vista release in 2007
SYSMON	Released in 2014 Kernel driver base
WHIDS	Released on 2018 Based on ETW and SYSMON API to control agents config (including SYSMON)
SilkETW	Released in 2019 by Mandiant
Aurora	Release in 2021 by Nextron EDR based on ETW & use SIGMA rules Capacity to respond to threats







Expecting the unexpected

WHAT/WHO CAN WE TRUST ?

Trust your security partners

On 10 May 2021, Hospital C asked Hospital C's cybersecurity solutions provider whether they should be concerned about Cobalt Strike alerts. They were advised by Hospital C's cybersecurity solutions provider that since the threat had been remediated by their antivirus software, their risk was low.[54] Hospital C did not initiate a cyber incident response investigation.

Conti cyber attack on the HSE

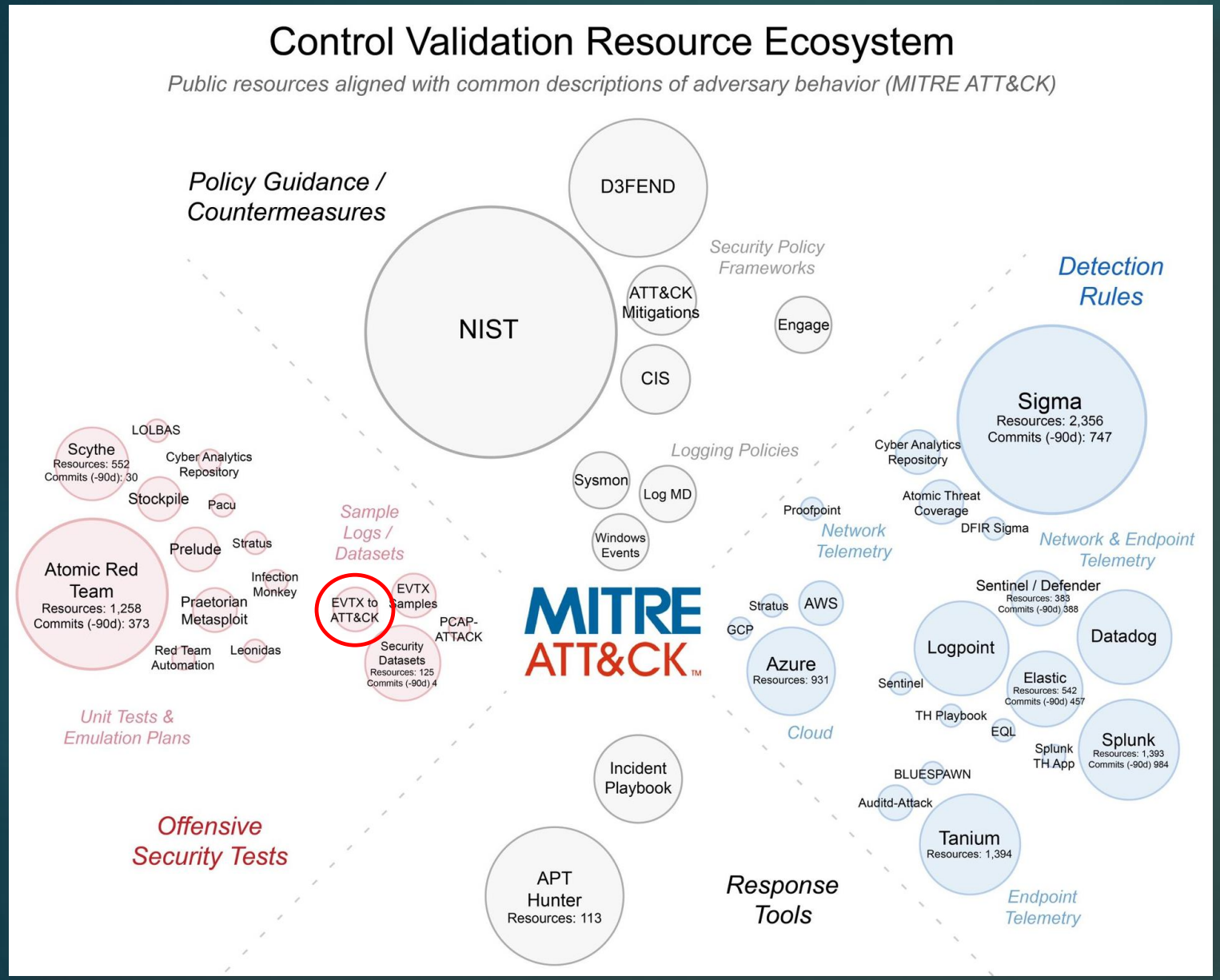
Independent Post Incident Review

Source: Conti attack on the HSE (Health Service Executive) – Ireland Public post incident report from PwC - 2021

Detection validation

ASSESSING YOUR DEFENSES

Control validation resource ecosystem



Source: Control Compass – May 2022

EDR assessment tools

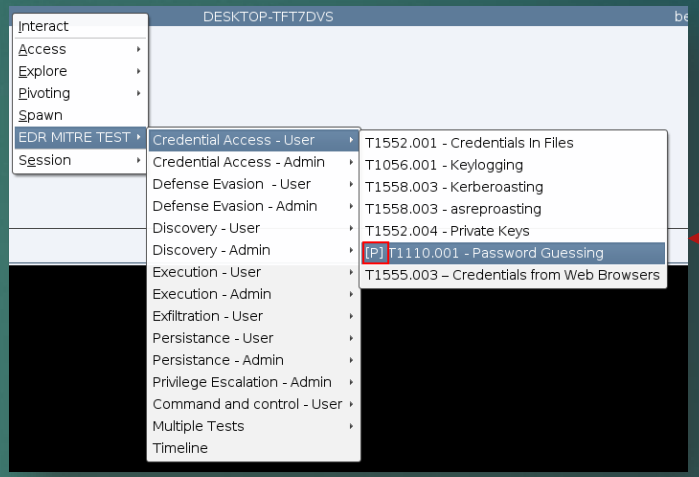
Atomic Red team (Red Canary)

Attack range (Splunk)

APT Simulator (Nextron)

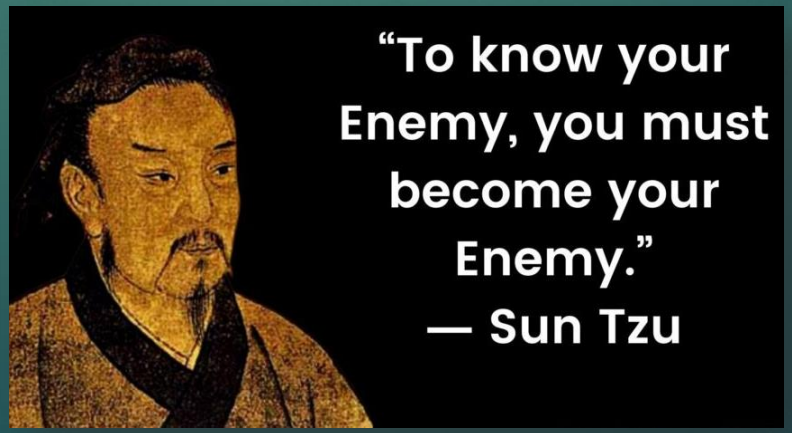
Caldera (MITRE)

Threatest (Datadog)



EDR-test

- A good alternative to Atomic Red Team not using PowerShell



Pyramid

- Perform offensive tasks by leveraging Python evasion techniques

Holistic and combined approach

Audit for tampering

Audit for EDR tampering

Read and forward logs

Check log agent status → EDR alert (not via your log agent)

Thank you!