CENTRE FOR
CYBER SECURITY
BELGIUM

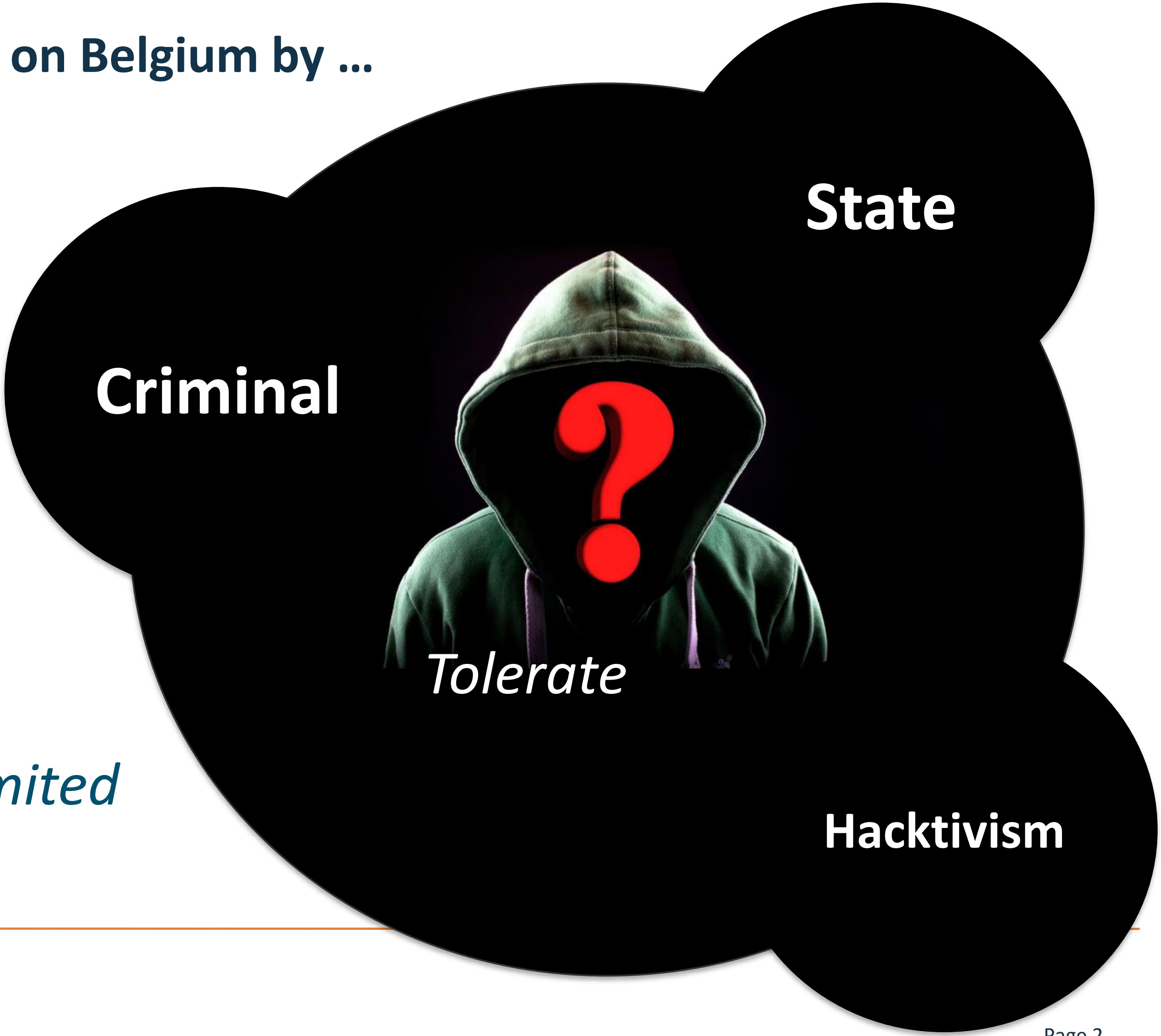
National cyber security impact of Geopolitical tensions

I will not tell you anything
you don't already know

Miguel De Bruycker

Managing Director CCB

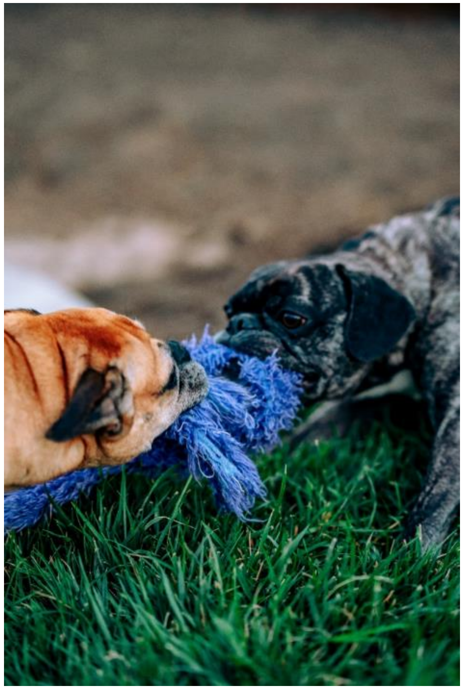
Direct impact on Belgium by …



Cautiously limited

Loss of global trust – emphasis on differences

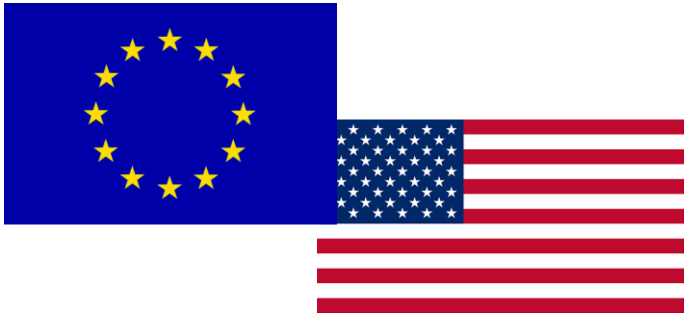
Conflict/war



Tensions

Perception of difference

Ukraine war has changed National cybersecurity permanently



2023 - 2024

- Cyber security as part of the Internet
- Understand what they are capable of … and what not
- The impossible will be done
  - Information sharing amongst trusted partners
  - Identification of TTP’s and infrastructure
  - Filtering

Thank you

info@ccb.belgium.be

CENTRE FOR
CYBER SECURITY
BELGIUM

CENTRE FOR
CYBER SECURITY
BELGIUM

QUARTERLY CYBER THREAT OVERVIEW Q4 2022

@certbe

Be Social: #CCBQCTR

CLARA GRILLET

Cyber Threat Analyst (Threat Research Center)

Team of CyTRIS (Cyber Threat Research & Intelligence Sharing)

CyTRIS is the CTI department of CCB

clara.grillet@cert.be

TLP CLEAR

4 May 2022

Today’s agenda

1

Threats to Belgium

2

Global threats to critical sectors

3

Key APT actor trends

4

Key exploited vulnerabilities

5

Outlook

Threats to Belgium

Ransomware

It’s back and it’s big! 28 ransomware attacks
Multiple actors: **LockBit 3.0**, Play, Ragnar Locker

Same initial access vectors

Phishing, exploited vulnerabilities, leaked credentials, insider threats

Mixed impact depends on each organization’s strategy

3-2-2 backups
MFA on all local and cloud accounts

How to protect against ransomware

https://cert.be/en/alert/several-belgian-municipalities-recently-fell-victim-ransomware

Sale of customer database and network access

Leaked credentials stolen in breaches are sold on underground forums

Concentrated in Exploit.in

RDP access, customer databases, RDWeb access

Spear warnings sent to entities identified by CCB/CyTRIS (names, domains)

Global threats to critical sectors

Risk of data breach, ransomware and DDoS

All critical sectors

Government, healthcare, finance, energy (oil, gas, electricity)

- Global campaign from TAG-52 against government, energy, defense, media and education sectors

Increased activity in the energy sector

Chinese and Russian nexus

Information gathering (future destructive attacks?)

- Reconnaissance on LNG terminals in the Netherlands

Raspberry Robin

The return of infected USB devices

- Targets European financial institutions

Block USB ports, user awareness

TLP CLEAR

A word on the cyber impacts of the Ukraine-Russia conflict

Renewed activity from Russophone actors

A mix of longstanding, well-known actors and recent hacktivist groups

Gamaredon, Sandworm, KillNet, IT Army of Ukraine, NoName057(16), GhostWriter

Financial crime groups have likely reorganized

Countries perceived to be pro-Ukraine are more targeted

Prestige ransomware attack on Polish and Ukrainian transportation and logistics networks

Geopolitical theme is a recurring **lure** in various campaigns

Beware of hacktivist groups

Ideologically-motivated attacks

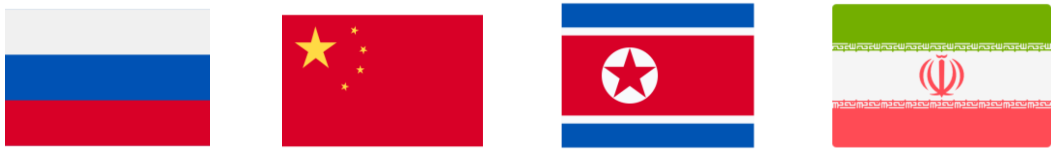
Could target any organization they suspect to be involved with either side

Information war: high visibility, global reach but often low impact

Killnet lauches a DDoS attack against the European Parliament in retaliation for Parliament's decision to designate Russia as state sponsor of terrorism

Key APT actor trends

Their #1 weapon: spear-phishing



Source: flaticon.com

Long-established APTs

Information gathering, disruption and financial gain

Unlike Russia, for China, the UA/RU conflict is just one of multiple focuses

Widening scope: neighboring countries, but also Europe, Latin America, Asia

Chinese activity outside Europe with spearphishing attacks towards government, NGO and research organizations

Shift towards more abuse of legitimate services

Malware delivered via emails from fraudulent Google accounts or malicious Google Drive/Dropbox links

Phishing tests

✓ Use a link instead of an attachment
✓ Customize per department (make it realistic)

Key exploited vulnerabilities

Vulnerabilities in Microsoft Exchange

ProxyNotShell

CVE-2022-41040 and CVE-2022-41082

Mitigations before a patch became available a month later

OWASSRF

CVE-2022-41080

Bypasses ProxyNotShell mitigations

Used by Play ransomware

Older vulnerabilities are still being actively exploited (Log4j)

Other vulnerabilities

Fortinet

- CVE-2022-40684
- CVE-2022-42475

Zimbra

- CVE-2022-41352

Apache "Text4Shell"

- CVE-2022-42889

VMWare

- CVE-2021-39144

OpenSSL

- CVE-2022-3602 and CVE-2022-3786

Citrix

- CVE-2022-27518

Oracle

- CVE-2021-35587

Outlook

Ransomware will continue to rise

- Primarily for financial gain
- Also for destructive or disruptive operations
- OT, industrial systems and critical infrastructure
- Increased specialization, extortion-only groups

Continued influence of Ukraine-Russia conflict

- Hacktivism and APTs, upskilling
- Geopolitical targeting: government, logistics, media, energy
- Phishing lure

Increased speed of exploitation

- Prioritize!
- Beware of external access
- Good practice: MFA on cloud and local accounts, back-ups

- **Inform CCB about possible threats or compromises to your organization/sector**
- Increase overall security posture
  - https://cyberguide.ccb.belgium.be/en
- Know your environment & look for anomalies!
- User awareness!!!
- Periodical threat hunt
- Protect your entry points
  - Vulnerability Management
- Protect supply chain
  - Zero-Trust network
- PREPARE for the attack!
  - Crisis communication
  - Incident Response plan

Questions?

Contact details:

- CTI questions: ews@cert.be
- Incident reports: cert@cert.be

in https://www.linkedin.com/company/centre-for-cybersecurity-belgium/

@certbe

CLARA GRILLET
Analyst at Threat Research Centre, CyTRIS
clara.grillet@ccb.belgium.be
clara.grillet@cert.be

TLP CLEAR

рахмат
danke
謝謝
ngiyabonga
Баярлалаа
spas
mersi
kia ora
barka
welalin
tack
teşekkür ederim
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
kiitos
dankie
nanni
nandri
dhanyavad
thank you
gracias
хвала
asante
manana
obrigada
tenki
enkosi
bedankt
bayarlalaa
gracie
hvala
mauruuru
köszönöm
akun
dankon
aciu
djiere dieuf
tau
mochchakkeram
murakoze
chokrane
dziękuję
дякую
mamnun
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
sobodi
dekuji
obrigado
sagolun
sukriya
kop khun krap
taiku
arigatô
takk
dakujem
trugarez
mèsi
didi madloba
najis tuke
ありがとう
tanemirt
rahmet
grazie
diolch
dhanyavadagalu
shukriya
merce
мерси
kam sah hamnida
rahmat
terima kasih
তোমাকে ধন্যবাদ
감사합니다
xièxie
ευχαριστώ
merci

How can we prioritize vulnerabilities?

Know

Know your environment!

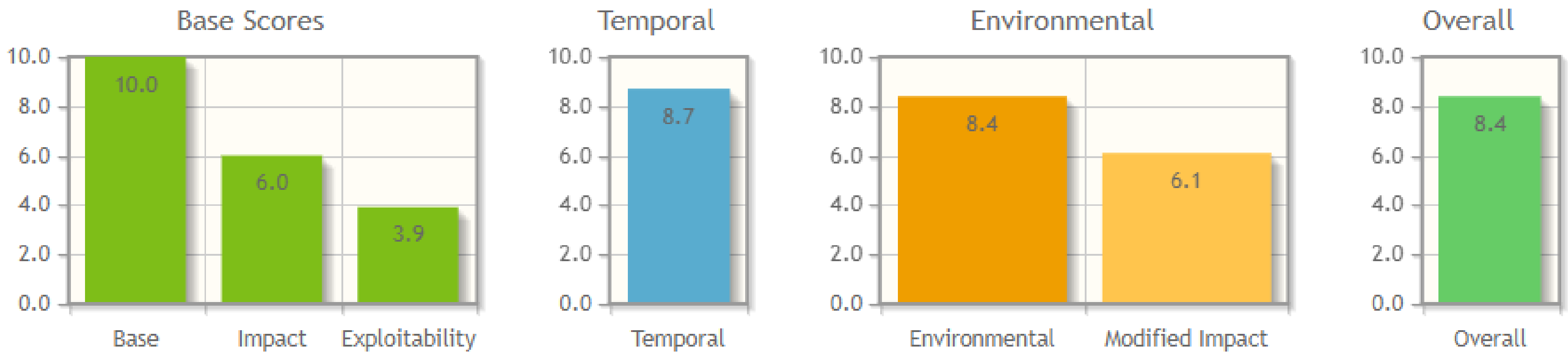
Scan internally & externally

Patch

Patch management:

- Prioritize!
- Fix exploited vulnerabilities first
- Don’t neglect internal applications

- Common Vulnerability Scoring System (CVSS v3.1)
- Apply to your own environment
  - Impact on crown jewels
  - Where in the network does the vulnerability exist?
  - Possibility to move laterally?
- Exploit sought in Underground / researched publicly / disclosed publicly?
- Exploit weaponized?
  - Exploit used by Activity Groups targeting your organization/sector?



CVSS Base Score: 10.0

Impact Subscore: 6.0

Exploitability Subscore: 3.9

CVSS Temporal Score: 8.7

CVSS Environmental Score: 8.4

Modified Impact Subscore: 6.1

Overall CVSS Score: 8.4

Crisis communication

- Be prepared for an incident: https://youtu.be/-cHcTidmT1Y
  - Create a cyber emergency plan + add crisis communication plan
- How to communicate?
  - Be open and honest
  - Communicate pro-actively, take control of the story
  - Rule: “We know, We do, We care”
    1. We know about the incident and acknowledge the problem
    2. We do the following steps to fix the problem ASAP
    3. We care about the incidents, our clients, and vendors who are impacted by it
- Have a cyber emergency plan with a contact list on paper in a secure place
- Ask help at to the CCB!
- Major incident: hire a professional crisis communication expert

censys

Think Like an Attacker

The Importance of Attack Surface Management in Cloud Security

Nick Miles | Director Partner Channel, EMEA
nmiles@censys.io

January, 2023

State of Security

The fundamentals of security are the same

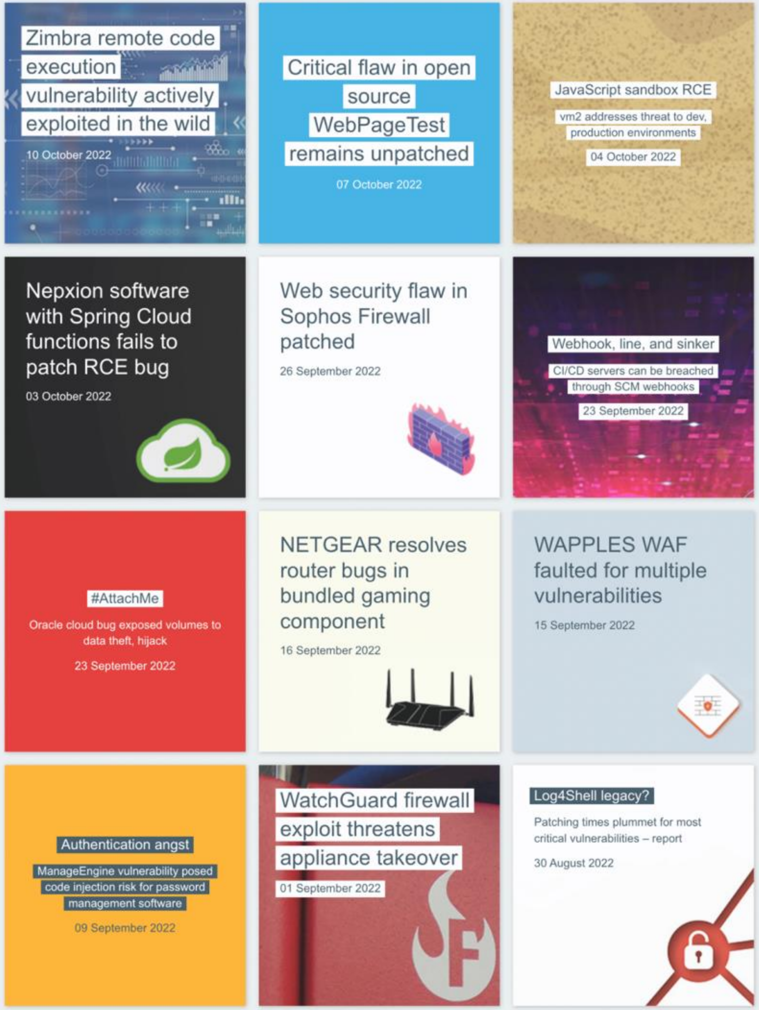
- Inventory all of the assets
- Prioritize and remediate risks
- Prevent breaches

But the IT ecosystem has become more complex

- Multi-cloud adoption
- More people, offices, assets, services…
- More vulnerabilities and exposures
- Shift from ‘What’s mine?’ to ‘What’s Exposed?’

Existing security solutions weren't built for this challenge

- Tools miss unknown assets and risks are fractured across multiple platforms and products
- Too many alerts and not enough context to effectively prioritize and fix critical risks



Zimbra remote code execution vulnerability actively exploited in the wild

10 October 2022

Critical flaw in open source WebPageTest remains unpatched

07 October 2022

JavaScript sandbox RCE

vm2 addresses threat to dev, production environments

04 October 2022

Nepxion software with Spring Cloud functions fails to patch RCE bug

03 October 2022

Web security flaw in Sophos Firewall patched

26 September 2022

Webhook, line, and sinker

CI/CD servers can be breached through SCM webhooks

23 September 2022

#AttachMe

Oracle cloud bug exposed volumes to data theft, hijack

23 September 2022

NETGEAR resolves router bugs in bundled gaming component

16 September 2022

WAPPLES WAF faulted for multiple vulnerabilities

15 September 2022

Authentication angst

ManageEngine vulnerability posed code injection risk for password management software

09 September 2022

WatchGuard firewall exploit threatens appliance takeover

01 September 2022

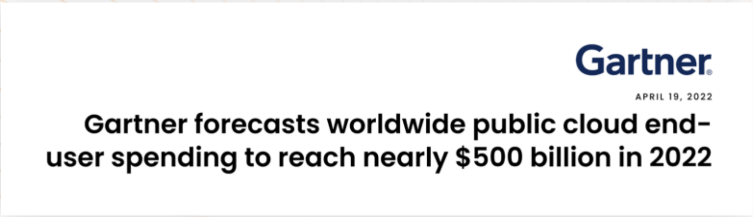
Log4Shell legacy?

Patching times plummet for most critical vulnerabilities – report

30 August 2022

Why Attack Surface Management

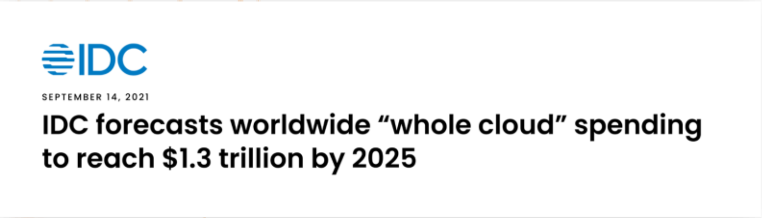
Security pros are unable to comprehensively discover, manage, and protect their rapidly growing attack surface



Gartner.

APRIL 19, 2022

Gartner forecasts worldwide public cloud end-user spending to reach nearly $500 billion in 2022

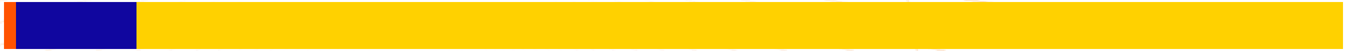


IDC

SEPTEMBER 14, 2021

IDC forecasts worldwide "whole cloud" spending to reach $1.3 trillion by 2025

1 Security FOR EVERY 10 DevOps FOR EVERY 100 Devs



110%

y/y attack surface growth

80%

Internet facing assets were impacted in 80% of security breaches

– 2022 DBIR

43%

of assets are potentially unknown

60%

of exposures on the Internet are misconfigurations

– 2022 SOTIR

Attack Surface definition:

“the set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from.”

– NIST

Attacker’s Perspective

The “**think like an attacker**” perspective is a unique but essential point of view; it’s important for organizations to secure not only the assets they know about, but to **secure the unknown ones** as well, as those are some of the **most vulnerable assets**.

Attackers are crawling the Internet and the cloud constantly, looking for any vulnerabilities to exploit:

80%
Of security incidents involved external cloud assets in 2022

69%
Of organizations experience a cyber attack that started with unknown assets

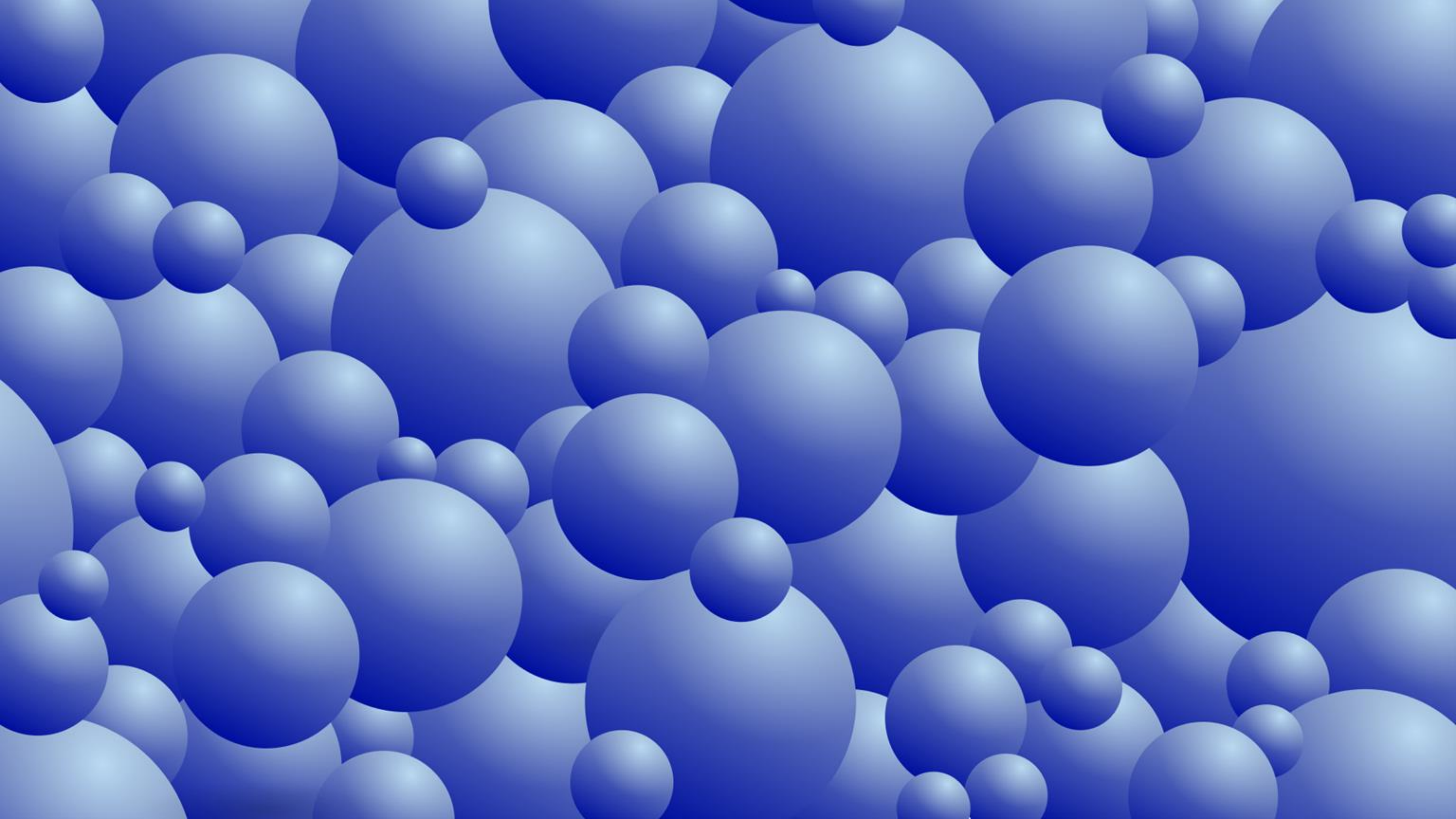
110%
Attack Surface growth year-over-year

43%
on average of any company’s assets are unknown

65%
of High and Critical risks live in the Cloud

9%
of all hosts with services on the Internet are AWS, Azure, Google, and Oracle

Security starts
with visibility.



Unsanctioned Cloud Assets
Supply Chain Assets
Externally Facing On-Prem Assets
Internet Facing Assets
Internet-Facing Assets
IoT & Mobile Devices
Cloud Environments
Cloud Environments
Cloud
Cloud
Cloud
Cloud
Cloud
M&A
M&A
M&A
Supply Chain Assets
Internet Facing Assets
Externally Facing On-Prem Assets
Cloud
M&A
Cloud

1000's of Cloud Projects & Accounts

(& 100's that you *don't* know about)

ATTACK SURFACE PROBLEM

Unable to comprehensively discover, manage, and protect the rapidly growing and complex attack surface.

Challenges with existing solutions:

Vendor Risk Management

No visibility into suppliers' cloud configurations

Vulnerability Management

No visibility into Shadow IT

Digital Risk Protection

No visibility into unknown attacker-facing Internet assets

Cloud Security Posture Mgmt

No visibility into unknown cloud accounts and weaknesses in other critical Internet assets, like SaaS

> We have 14,000 unread warnings from Wiz. We don’t know which are about assets exposed to the Internet.
>
> \- McKinsey

Current challenges organizations face

1. Vulnerability Management
2. Cloud Misconfiguration
3. Internet of Things (IoT)
4. Unknown/Unmanaged Assets
5. Shadow IT Groups
6. Identifying Public-Facing Assets
7. Home Networks for Remote Workers
8. IT Asset Inventory

FORRESTER®

> “
>
> Censys discovered **80% more cloud assets** than what we previously believed were online.
>
> - New World Development

An Attack Surface Management Platform Provides:

Comprehensive Visibility

Get total visibility into your Internet and cloud exposure

Actionable Insights & Investigation

Explore context-rich attack surface results to prioritize and address your riskiest Internet weaknesses

Rapid Response & Remediation

Operationalize your attack surface insights across your critical security investments for efficiency across the organization

Critical infrastructure

Energie Sector & Utilities

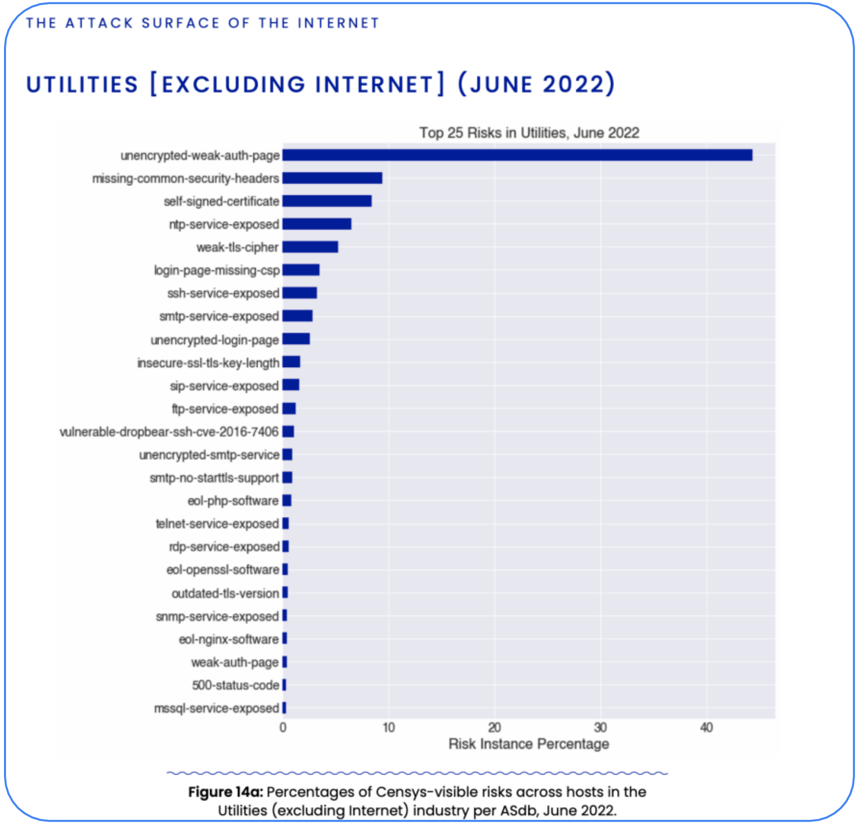
censys

Top Risks in Utilities and Energy Sector

From Censys State of the internet Report

The risk profile of the **Utilities industry** stands out because so much of it is driven by **unencrypted weak authentication pages**. While unencrypted weak authentication page is **one of the top three risks** we observe overall, it represents over half of the observed risks for this industry–driven primarily by a electric utility.

With increasing concern over **potential cyber attacks targeting Utilities**, this particular risk could offer threat actors a relatively **easy way into Utility networks unless remediated.**



THE ATTACK SURFACE OF THE INTERNET

UTILITIES [EXCLUDING INTERNET] (JUNE 2022)

Figure 14a: Percentages of Censys-visible risks across hosts in the Utilities (excluding Internet) industry per ASdb, June 2022.

3 Insights Into the Colonial Pipeline Attack and Energy Infrastructure

232%

Increase in publicly accessible hosts and an 66% increase of insecure services/protocols running on the total number of hosts.

130%

Increase in expired certificates. Expired certificates drops encryption, allowing attackers to intercept user credentials to website logins.

1 in 10

Of the 10 US energy organizations Censys observed, only one has a full-time CISO.

The **Colonial Pipeline breach** was made possible via a **reused password** on a Virtual Private Network (VPN) login lacking multi-factor authentication. This **disruption prompted Censys** to utilize its Universal Internet Dataset and Attack Surface Management (ASM) platform to determine risk to and exposure of Critical Infrastructure and Key Resources (CIKR) within **the energy industry from an external, attacker perspective.**

“

For **Security Pros that protect the organization,** Censys is the **best at finding what attackers will exploit.**

www.censys.io

Who We Work With

ABInBev

aircall

AUTODESK

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

cisco

f.

Google

Icertis

Microsoft

nu

okta

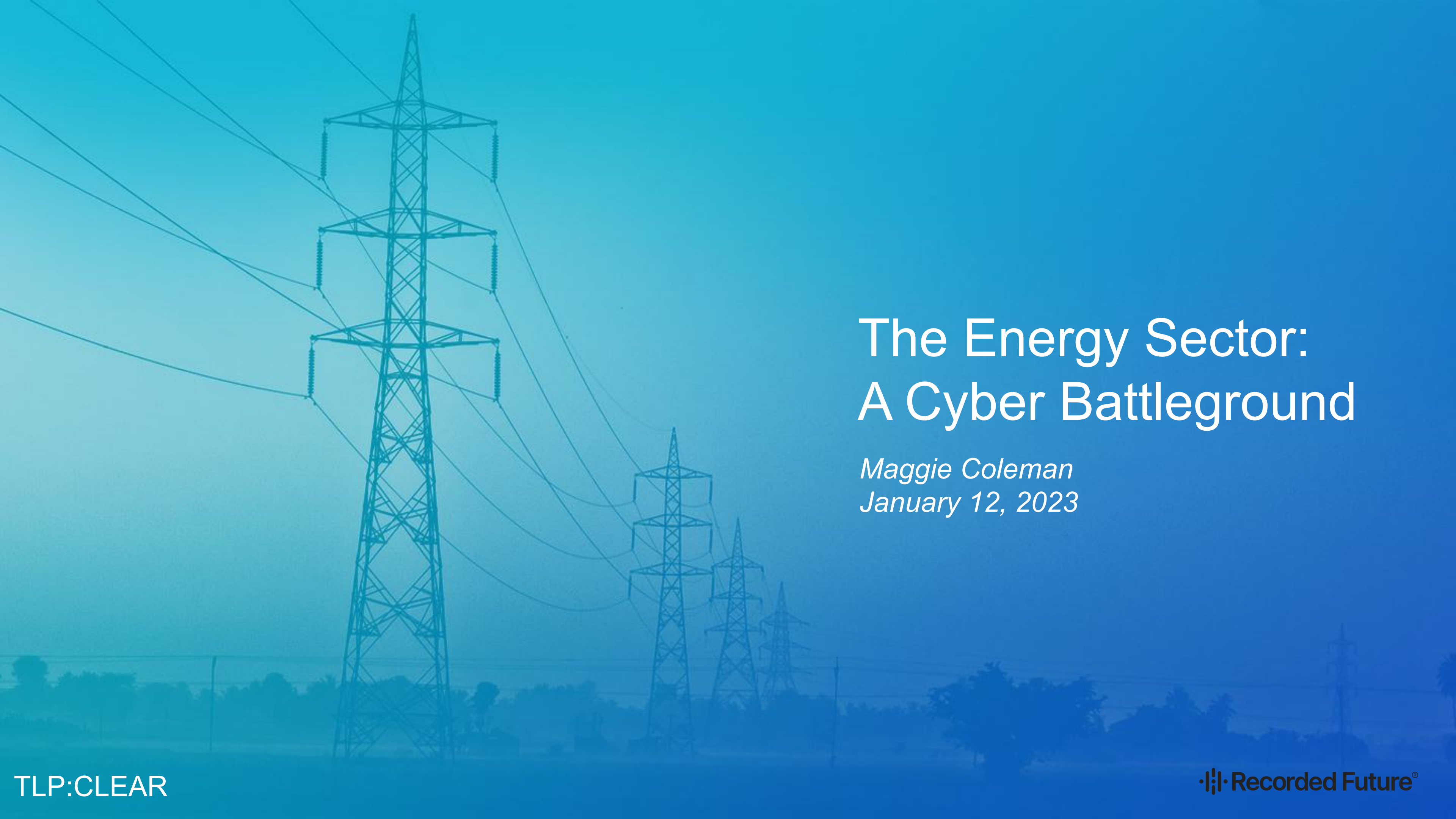
UNIVERSITY OF LOVISVILLE · 1798

Q&A

With Nick Miles, Director Partner Channel

& Dominik Bieszczad, Senior Solutions Engineer

censys



The Energy Sector: A Cyber Battleground

Maggie Coleman
January 12, 2023

TLP:CLEAR

Recorded Future®

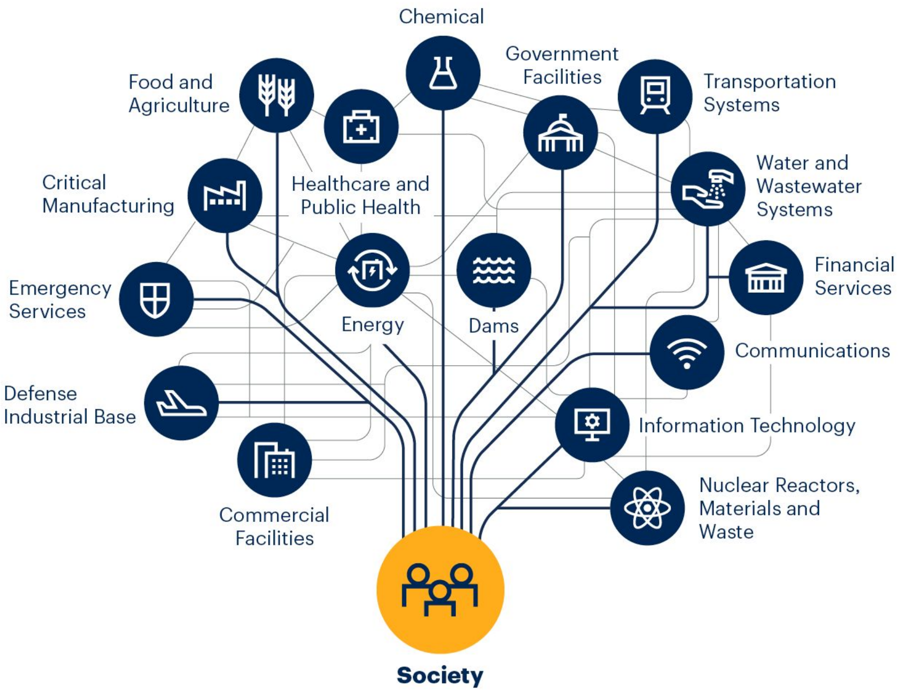
Agenda

1. Understanding the current lay of the land
2. Cyber attacks against the energy sector
3. Deep dive into destructive cyber attacks
4. How to protect against cyber attacks effectively
5. Wrap-up

1

Understanding the current lay of the land

Critical infrastructure is the backbone of our society and economies with the energy sector being at its core



Source: Gartner 2022

Energy sector plays a **pivotal role** among **critical infrastructure sectors,** with its **assets** being **geographically dispersed** and **connected by systems** owned by both **private** and **public sector**

Energy sector presents certain particularities that require attention from IT security and risk perspective

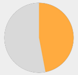
Complexity due to combination of legacy and new technologies

31%

Less than a third of energy professionals **assert confidently** that they **know what to do when confronted** with a **cyber threat** to their organization.*

Convergence of IT and OT

47%



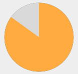
Fewer than **half of energy professionals** believe that their **OT security** is **as robust** as their **IT security**.**

+2,204%

Reconnaissance of OT devices accessible via the internet **massively increased** between **Jan - Sept 2021**.**

Large attack surface and risk of geographic and cross-industrial cascading effects

85%



Majority of energy professionals believes a cyberattack is **likely to cause operational shutdowns** and **damage to critical infrastructure**.**

*Source: *DNV 2022, ** IBM 2021*

Recorded Future®

Russia’s war against Ukraine

2

Cyber attacks against the energy sector

Cyberattacks can be broadly categorized into three types, but are not always clearly separable from each other

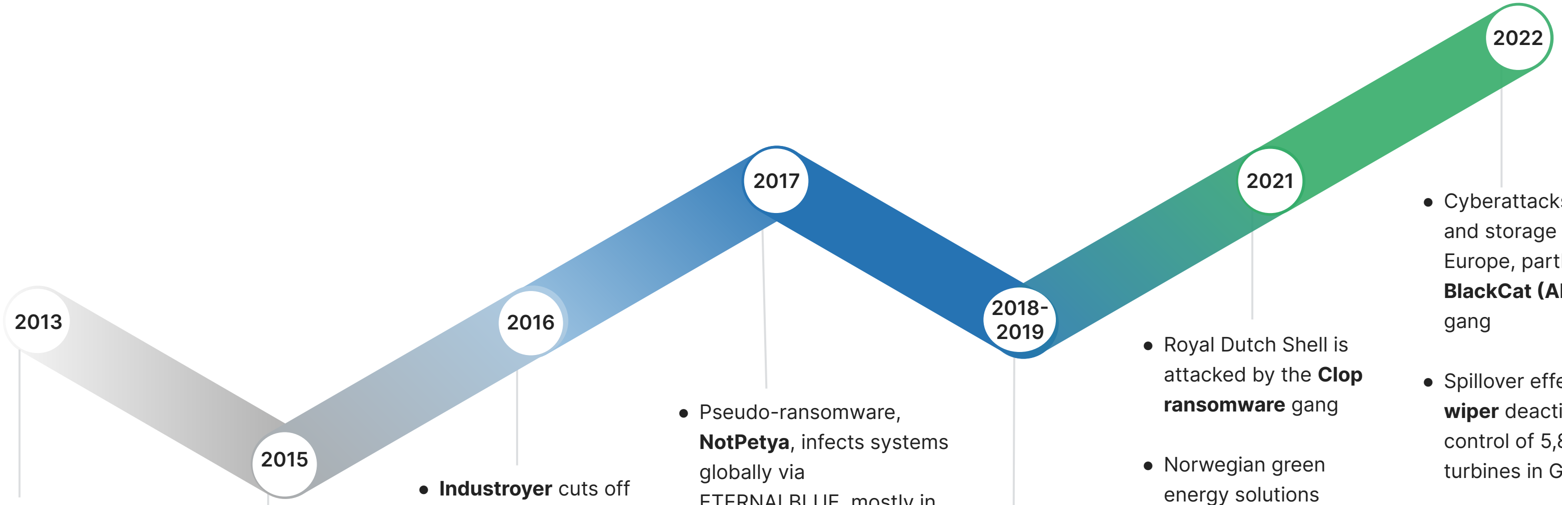
Cybercriminals (financially motivated)

Nation-state groups

Hacktivist groups

Read: ransomware groups

Both financially motivated and nation-state cyberattacks against Europe's energy sector have increased in last years



- **DragonFly** compromises more than 1,000 energy companies in US and Europe in year-long campaign

- **BlackEnergy** causes blackout in Ukraine for several hours, more than 200,000 people affected

- **Industroyer** cuts off power in Kiev, first ever known malware designed to attack electrical grids
- **Conficker** infects nuclear plant of Germany's RWE group

- Pseudo-ransomware, **NotPetya**, infects systems globally via ETERNALBLUE, mostly in Ukraine
- **DragonFly 2.0** re-emerges attacking dozens of energy companies in Europe

- German Intelligence sees Russia behind ongoing hacks of energy firms by **DragonFly 2.0**
- **Iranian APT33** heavily targets European energy sector using **PupyRat**

- Royal Dutch Shell is attacked by the **Clop ransomware** gang
- Norwegian green energy solutions provider Volue targeted by **Ruyk ransomware**

- Cyberattacks affect oil transport and storage companies across Europe, partly attributed to **BlackCat (ALPHV) ransomware** gang
- Spillover effects by **AcidRain wiper** deactivates remote control of 5,800 Enercon wind turbines in Germany
- **Sandworm attackers** attempts to deploy the **Industroyer2** malware against high-voltage electrical substations in Ukraine
- German energy supplier Entega and Luxembourg energy company Encevo Group hacked by **BlackCat (ALPHV) ransomware operators**

Recorded Future®

There are two threat actors that stand out due to their persistence, sophistication, and focus on the energy sector

Sandworm	
Aliases	Voodoo Bear
Emergence	Probably 2014 (FireEye)
Attack types	Destructive attacks
Attribution	Russia, allegedly unit of GRU (military intelligence)
Targets	Mostly Ukraine, special interest in power grids
Notable attacks	● BlackEnergy ● Industroyer ● NotPetya ● Industroyer2 (including CaddyWiper)

DragonFly	
Aliases	Energetic Bear, Berserk Bear
Emergence	Probably 2011 (Symantec)
Attack types	Espionage (surveillance and technical reconnaissance)
Attribution	Russia, more specifically FSB
Targets	Mostly energy organisations in Europe and US
Notable attacks	● Energy organisations in Europe and US

Other honorable mentions

Russia:
- Gamaredon Group
- APT28

North Korea:
- Lazarus Group

China:
- RedEcho
- DEV-0322

Iran:
- LYCEUM

Six key takeaways regarding cyber attacks against Europe’s energy sector

1 Nation-state groups are the **principal threat** against organizations in the energy and utilities sectors.

2 Recorded Future has observed the development and use of **sophisticated malware strains** targeting energy infrastructure in addition to **the exploitation of vulnerabilities**.

3 Recorded Future continues to identify a **large number of exposed credentials** associated with energy organizations, in addition to the sale of **global organizations’ network access**.

4 Ransomware operations have **proven their intent to target the energy and utilities sector** (noting that ransomware groups are mostly opportunistic in their targeting).

5 **Hacktivist groups have experienced a resurgence** in the context of the Russian invasion of Ukraine beginning in February 2022.

6 The Russian invasion of Ukraine has **provoked a rise in activity targeting the energy sector**.

3

Deep dive into destructive cyber attacks

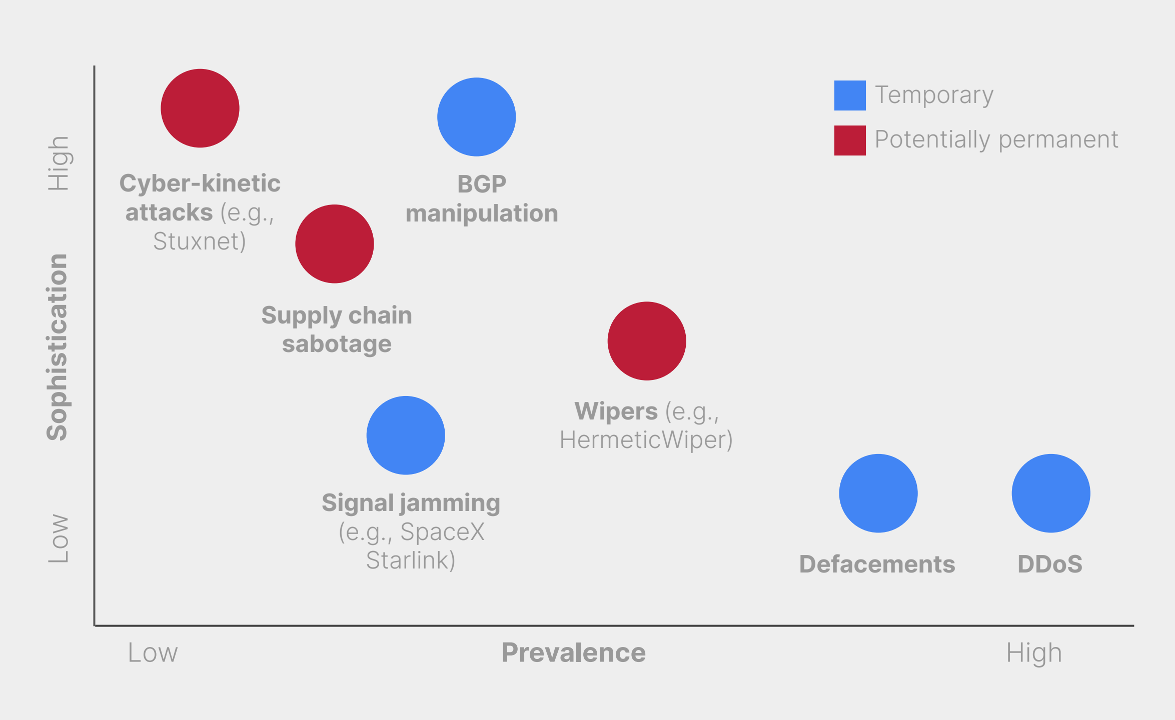
Destructive cyber attacks are diverse in terms of required sophistication, observed prevalence, and impact

Destructive cyber attacks are **cyber attacks potentially resulting** in:

- **death** or **personal injury**,
- **significant physical damage**,

  and/or

- **destruction** or **manipulation** of **information**, **data** or **software**, rendering them **useless unless extensive restoration** is undertaken.

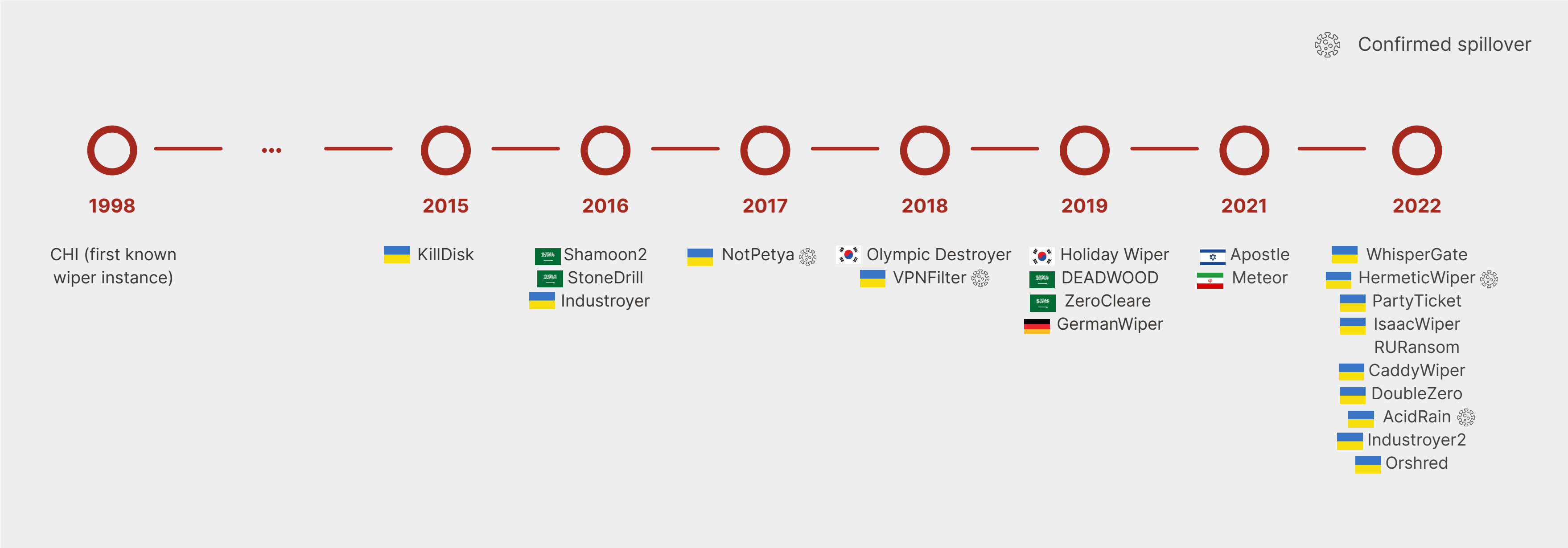


Source: Recorded Future

Recorded Future®

Use of wiper malware is correlated with geopolitical conflicts, is becoming more sophisticated, and has potential to spill over

Timeline of significant wipers and occasional spillover



❋ Confirmed spillover

1998 — CHI (first known wiper instance)

...

2015 — 🇺🇦 KillDisk

2016 — 🇸🇦 Shamoon2
🇸🇦 StoneDrill
🇺🇦 Industroyer

2017 — 🇺🇦 NotPetya ❋

2018 — 🇰🇷 Olympic Destroyer
🇺🇦 VPNFilter ❋

2019 — 🇰🇷 Holiday Wiper
🇸🇦 DEADWOOD
🇸🇦 ZeroCleare
🇩🇪 GermanWiper

2021 — 🇮🇱 Apostle
🇮🇷 Meteor

2022 — 🇺🇦 WhisperGate
🇺🇦 HermeticWiper ❋
🇺🇦 PartyTicket
🇺🇦 IsaacWiper
RURansom
🇺🇦 CaddyWiper
🇺🇦 DoubleZero
🇺🇦 AcidRain ❋
🇺🇦 Industroyer2
🇺🇦 Orshred

Source: Recorded Future

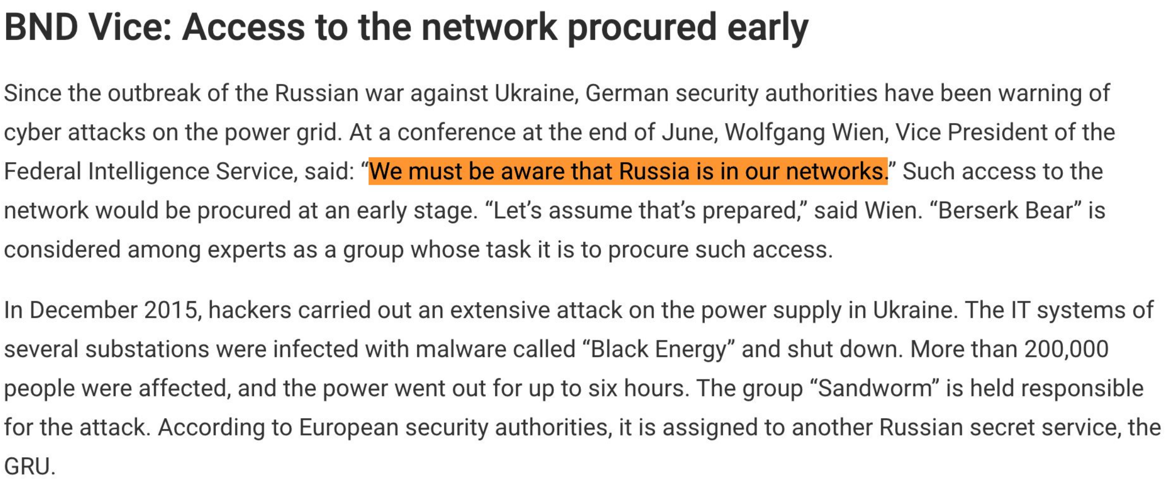
4

How to protect against cyber attacks effectively

There are five major angles on how to protect IT and OT infrastructure from an intelligence perspective

	Brand imitation and mentions	Exploits and malicious innovation	Identities	Supply chains	Attack surface
What	● (Spear-)Phishing ● Typosquats ● Waterholing ● Extortion sites	● New exploits kits ● Vulnerabilities ● New TTPs	● Credentials or whole identities	● Trojanised third party software ● Misconfigured trust relationships	● Exposed systems ● Misconfigurations or vulnerabilities
Example attack	Iranian APT LYCEUM activity (2022); historical BlackEnergy attacks	Industroyer2 in Ukraine (2022)	Mainzer Stadtwerke in Germany (2022) or Colonial Pipeline (2021)	DragonFly targeting updates of ICS (2011-2014)	Exposed RDP access as common attack vector
Example mitigations using intelligence	● Monitor phishing frameworks ● Monitor domain registrations ● Monitor extortion sites	● Monitor trends in tool usage (also regarding OT) ● Monitor tools (e.g., Manjusaka) ● Monitor active vulnerability exploitation	● Monitor credential dumps and malware logs ● Monitor credentials leaks on code repos	● Monitor and assess third party software (e.g., npm libraries)	● Keep track of attack surface ● Reduce attack surface as far as possible

But wait: are we not already infiltrated?



BND Vice: Access to the network procured early

Since the outbreak of the Russian war against Ukraine, German security authorities have been warning of cyber attacks on the power grid. At a conference at the end of June, Wolfgang Wien, Vice President of the Federal Intelligence Service, said: “We must be aware that Russia is in our networks.” Such access to the network would be procured at an early stage. “Let’s assume that’s prepared,” said Wien. “Berserk Bear” is considered among experts as a group whose task it is to procure such access.

In December 2015, hackers carried out an extensive attack on the power supply in Ukraine. The IT systems of several substations were infected with malware called “Black Energy” and shut down. More than 200,000 people were affected, and the power went out for up to six hours. The group “Sandworm” is held responsible for the attack. According to European security authorities, it is assigned to another Russian secret service, the GRU.

Source: globalecho.com (2022)

Threat Hunting

5 Conclusion

So what are the key takeaways?

1. **Energy sector** plays a **special role** embedded in the **ecosystem of critical infrastructure,** with very **specific IT security issues** and **risks,**

2. There is an **increased interest** in the **energy sector** by **state-sponsored, financially motivated, and hacktivist threat actors.**

3. **Ransomware leads financially motivated attacks.**

4. **Destructive cyber attacks** on **energy sector** have mostly occurred **along conflict lines** (e.g., Ukraine) with **few spillover effects** (e.g., AcidRain).

5. Despite threat, there are **numerous ways** in which **threat intelligence** can be **deployed** to **mitigate, detect,** and **prevent cyber attacks** against **energy sector.**

6

Questions?

Sigma as common language of cybersecurity

QCTR Q4 2022

CCB Connect & Share event

by Andrii Bezverkhyi

socprime.com | uncoder.io

SOC PRIME

_whoami

Founded SOC Prime Inc. in 2015

Invented uncoder.io

Attributed NotPetya to Sandworm in 5 days using ATT&CK +sigma

(June 28 to July 2 2017)

Officially M.A.D. on CTI since March 2022

Headlining team of 12 M.A.D. people

Pro bono consultant to SSSCIP & CERT UA

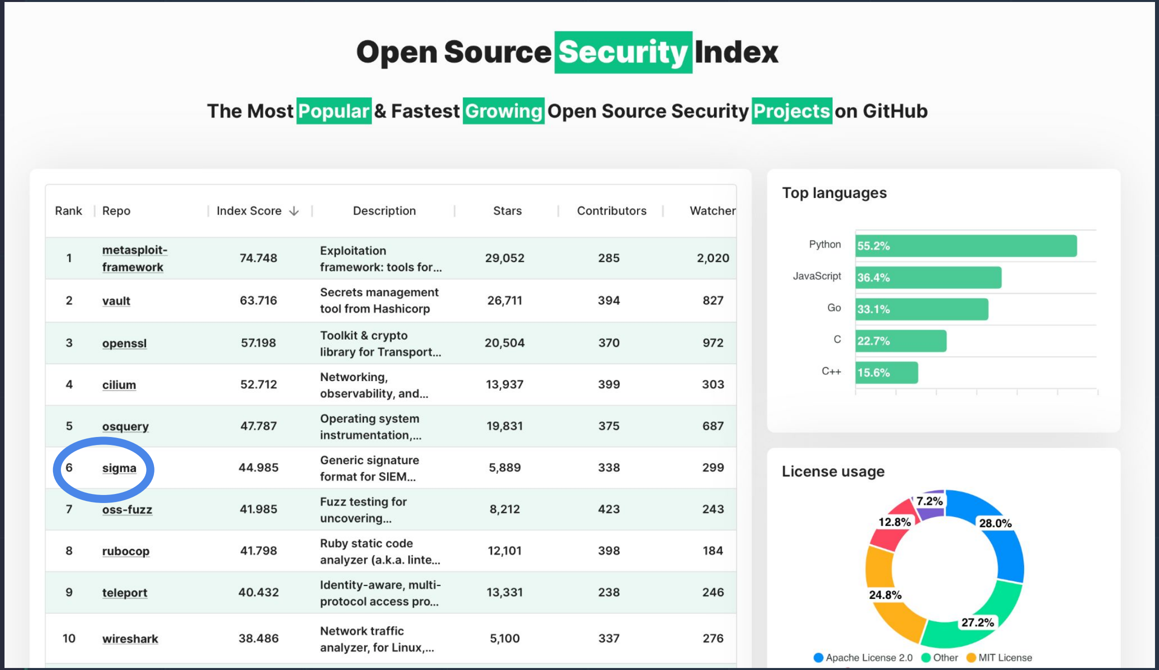
MITRE ATT&CK Defender™
ATT&CK®
CYBER THREAT INTELLIGENCE
CERTIFICATION

MITRE ATT&CK Defender™
ATT&CK®
SECURITY OPERATIONS CENTER ASSESSMENT
CERTIFICATION

MITRE ATT&CK Defender™
ATT&CK®
ADVERSARY EMULATION METHODOLOGY
CERTIFICATION

#6 oss project, download trends

Evolution of Sigma language adoption



Open Source Security Index

The Most Popular & Fastest Growing Open Source Security Projects on GitHub

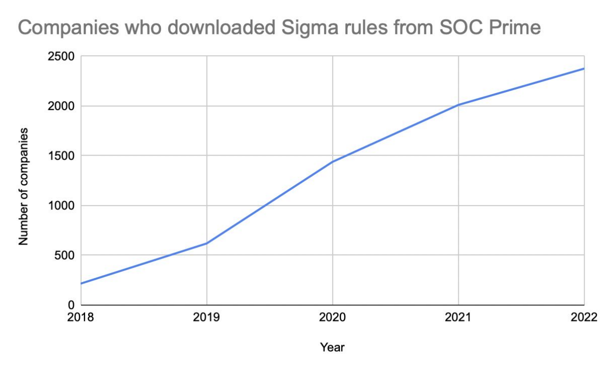
Rank	Repo	Index Score ↓	Description	Stars	Contributors	Watcher
1	metasploit-framework	74.748	Exploitation framework: tools for...	29,052	285	2,020
2	vault	63.716	Secrets management tool from Hashicorp	26,711	394	827
3	openssl	57.198	Toolkit & crypto library for Transport...	20,504	370	972
4	cilium	52.712	Networking, observability, and...	13,937	399	303
5	osquery	47.787	Operating system instrumentation,...	19,831	375	687
6	sigma	44.985	Generic signature format for SIEM...	5,889	338	299
7	oss-fuzz	41.985	Fuzz testing for uncovering...	8,212	423	243
8	rubocop	41.798	Ruby static code analyzer (a.k.a. linte...	12,101	398	184
9	teleport	40.432	Identity-aware, multi-protocol access pro...	13,331	238	246
10	wireshark	38.486	Network traffic analyzer, for Linux,...	5,100	337	276

Top languages

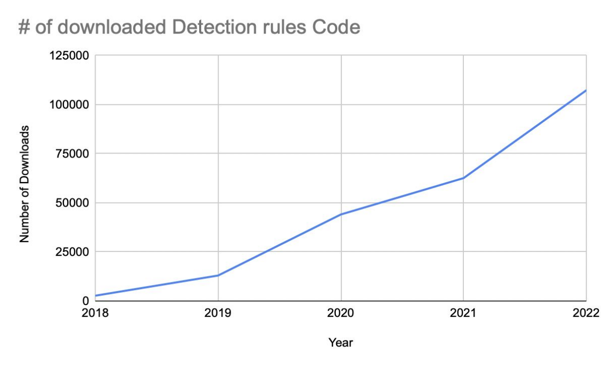
Python	55.2%
JavaScript	36.4%
Go	33.1%
C	22.7%
C++	15.6%

License usage

● Apache License 2.0	28.0%
● Other	27.2%
● MIT License	24.8%
	12.8%
	7.2%



Companies who downloaded Sigma rules from SOC Prime



# of downloaded Detection rules Code

So who is using Sigma rules?

And how does it connect with ATT&CK?

42% of Fortune 100

30% of Global 500

21% of Global 2000

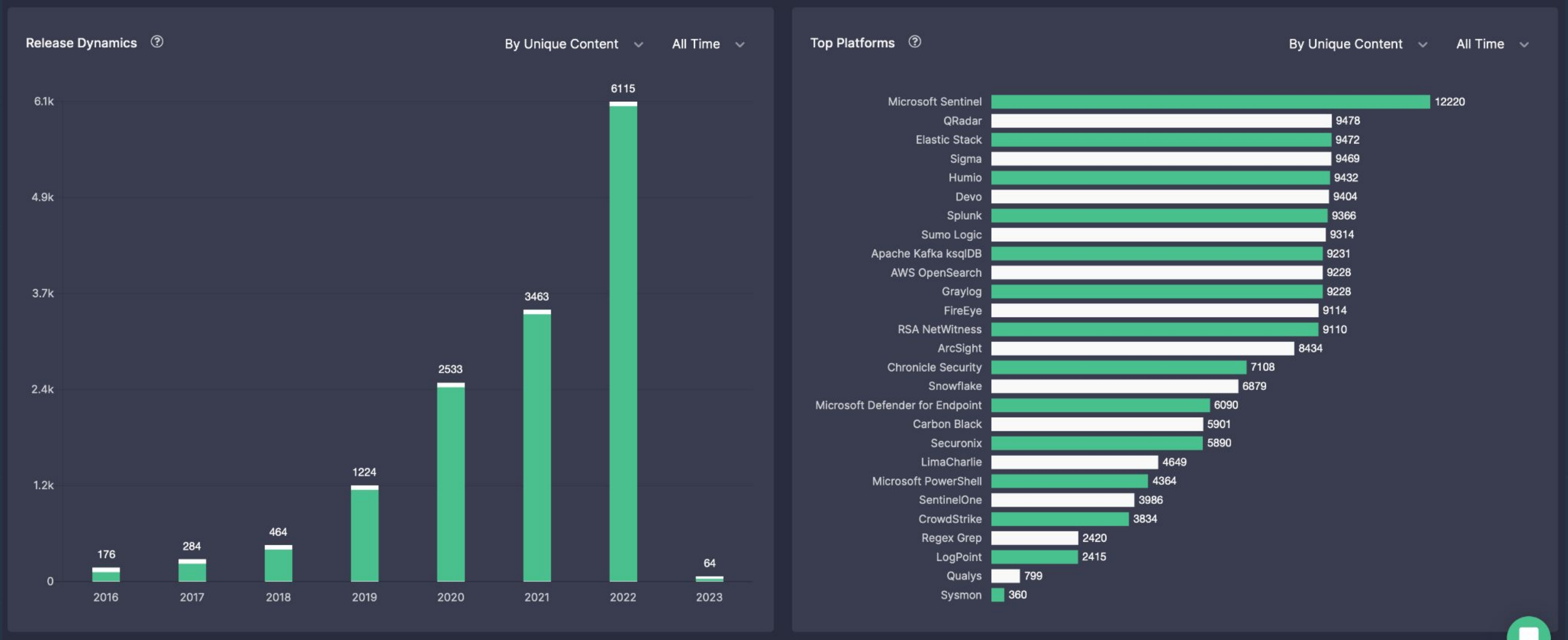
320+ ISV, MSSP & MDR providers***

***42% download Microsoft Sentinel translations (KQL)

94% of all Sigma rules are tagged with ATT&CK,
yet not all SIEM/EDR support ATT&CK tags,
so link to ATT&CK lives in Sigma rule name or UUID

Is Sigma over 9000?

Yes



Release Dynamics

By Unique Content

All Time

Top Platforms

By Unique Content

All Time

Sigma use cases

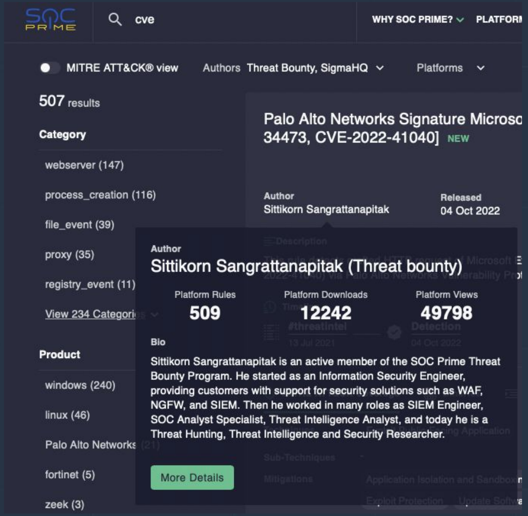
SOC alerts and Threat Hunting

Based on field feedback, SOC Prime lab testing and ATT&CK tags
2020: 20% of Sigma rules are for alerting, 80% for threat hunting
2022: 5% are for alerting, 95% for threat hunting

What happened to 15%? They need additional tuning before prod (excludes, allow lists, false-positive filters)

We lack people, time and collaboration to get above 5% today

Using MITRE ATT&CK & Sigma rules as hard skills proof, new CV for our future teammates



MITRE ATT&CK® view Authors Threat Bounty, SigmaHQ Platforms

507 results

Category

- webserver (147)
- process_creation (116)
- file_event (39)
- proxy (35)
- registry_event (11)

View 234 Categories

Product

- windows (240)
- linux (46)
- Palo Alto Networks (21)
- fortinet (5)
- zeek (3)

Palo Alto Networks Signature Microso
34473, CVE-2022-41040] NEW

Author
Sittikorn Sangrattanapitak

Released
04 Oct 2022

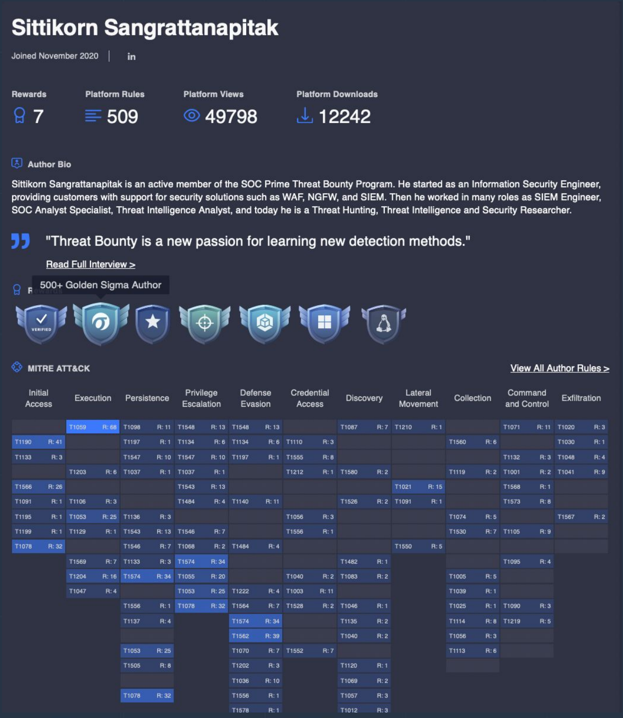
Author
Sittikorn Sangrattanapitak (Threat bounty)

Platform Rules	Platform Downloads	Platform Views
509	12242	49798

Bio

Sittikorn Sangrattanapitak is an active member of the SOC Prime Threat Bounty Program. He started as an Information Security Engineer, providing customers with support for security solutions such as WAF, NGFW, and SIEM. Then he worked in many roles as SIEM Engineer, SOC Analyst Specialist, Threat Intelligence Analyst, and today he is a Threat Hunting, Threat Intelligence and Security Researcher.

More Details



Sittikorn Sangrattanapitak

Joined November 2020 | in

Rewards	Platform Rules	Platform Views	Platform Downloads
7	509	49798	12242

Author Bio

Sittikorn Sangrattanapitak is an active member of the SOC Prime Threat Bounty Program. He started as an Information Security Engineer, providing customers with support for security solutions such as WAF, NGFW, and SIEM. Then he worked in many roles as SIEM Engineer, SOC Analyst Specialist, Threat Intelligence Analyst, and today he is a Threat Hunting, Threat Intelligence and Security Researcher.

> "Threat Bounty is a new passion for learning new detection methods."

Read Full Interview >

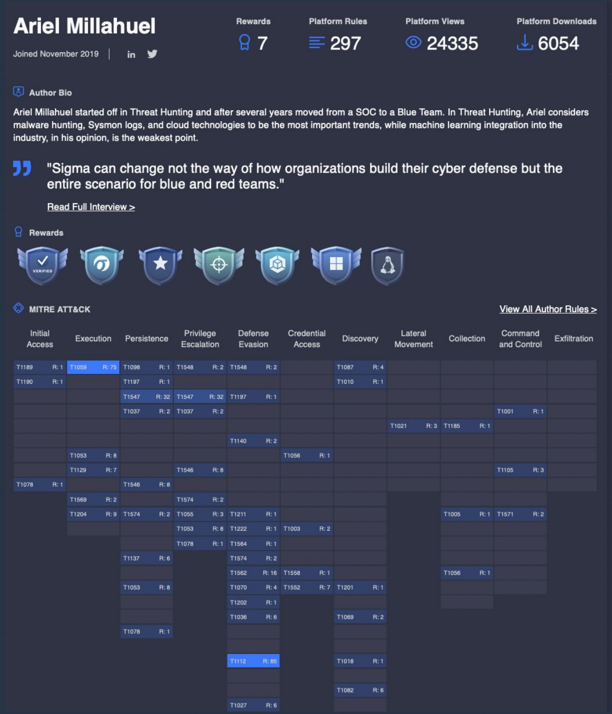
Rewards

500+ Golden Sigma Author

MITRE ATT&CK

View All Author Rules >

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
	T1059 R: 68	T1098 R: 11	T1548 R: 13	T1548 R: 13		T1087 R: 7	T1210 R: 1		T1071 R: 11	T1020 R: 3
T1190 R: 41		T1197 R: 1	T1134 R: 6	T1134 R: 6	T1110 R: 3			T1560 R: 6		T1030 R: 1
T1133 R: 3		T1547 R: 10	T1547 R: 10	T1197 R: 1	T1555 R: 8				T1132 R: 3	T1048 R: 4
	T1203 R: 6	T1037 R: 1	T1037 R: 1		T1212 R: 1	T1580 R: 2		T1119 R: 2	T1001 R: 2	T1041 R: 9
T1566 R: 26			T1543 R: 13				T1021 R: 15		T1568 R: 1	
T1091 R: 1	T1106 R: 3		T1484 R: 4	T1140 R: 11		T1526 R: 2	T1091 R: 1		T1573 R: 8	
T1195 R: 1	T1053 R: 25	T1136 R: 3			T1056 R: 3			T1074 R: 5		T1567 R: 2
T1199 R: 1	T1129 R: 1	T1543 R: 13	T1546 R: 7		T1556 R: 1			T1530 R: 7	T1105 R: 9	
T1078 R: 32		T1546 R: 7	T1068 R: 2	T1484 R: 4			T1550 R: 5			
	T1569 R: 7	T1133 R: 3	T1574 R: 34			T1482 R: 1			T1095 R: 4	
	T1204 R: 16	T1574 R: 34	T1055 R: 20		T1040 R: 2	T1083 R: 2		T1005 R: 5		
	T1047 R: 4		T1053 R: 25	T1222 R: 4	T1003 R: 11			T1039 R: 1		
		T1556 R: 1	T1078 R: 32	T1564 R: 7	T1528 R: 2	T1046 R: 1		T1025 R: 1	T1090 R: 3	
		T1137 R: 4		T1574 R: 34		T1135 R: 2		T1114 R: 8	T1219 R: 5	
				T1562 R: 39		T1040 R: 2		T1056 R: 3		
		T1053 R: 25		T1070 R: 7	T1552 R: 7			T1113 R: 6		
		T1505 R: 8		T1202 R: 3		T1120 R: 1				
				T1036 R: 10		T1069 R: 2				
		T1078 R: 32		T1556 R: 1		T1057 R: 3				
				T1578 R: 1		T1012 R: 3				



Ariel Millahuel

Joined November 2019 | in

Rewards	Platform Rules	Platform Views	Platform Downloads
7	297	24335	6054

Author Bio

Ariel Millahuel started off in Threat Hunting and after several years moved from a SOC to a Blue Team. In Threat Hunting, Ariel considers malware hunting, Sysmon logs, and cloud technologies to be the most important trends, while machine learning integration into the industry, in his opinion, is the weakest point.

> "Sigma can change not the way of how organizations build their cyber defense but the entire scenario for blue and red teams."

Read Full Interview >

Rewards

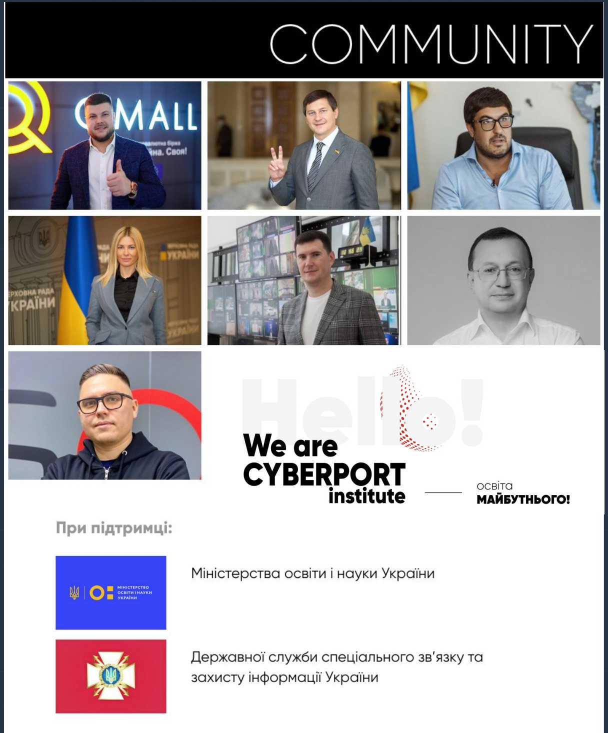
MITRE ATT&CK

View All Author Rules >

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
T1189 R: 1	T1059 R: 75	T1098 R: 1	T1548 R: 2	T1548 R: 2		T1087 R: 4				
T1190 R: 1		T1197 R: 1				T1010 R: 1				
		T1547 R: 32	T1547 R: 32	T1197 R: 1						
		T1037 R: 2	T1037 R: 2						T1001 R: 1	
							T1021 R: 3	T1185 R: 1		
				T1140 R: 2						
	T1053 R: 8				T1056 R: 1					
	T1129 R: 7		T1546 R: 8						T1105 R: 3	
T1078 R: 1		T1546 R: 8								
	T1569 R: 2		T1574 R: 2							
	T1204 R: 9	T1574 R: 2	T1055 R: 3	T1211 R: 1				T1005 R: 1	T1571 R: 2	
			T1053 R: 8	T1222 R: 1	T1003 R: 2					
			T1078 R: 1	T1564 R: 1						
		T1137 R: 6		T1574 R: 2						
				T1562 R: 16	T1558 R: 1			T1056 R: 1		
		T1053 R: 8		T1070 R: 4	T1552 R: 7	T1201 R: 1				
				T1202 R: 1						
				T1036 R: 6		T1069 R: 2				
		T1078 R: 1								
				T1112 R: 85		T1018 R: 1				
						T1082 R: 6				
				T1027 R: 6						

Sigma & ATT&CK education

Training 100+ students already in 2022



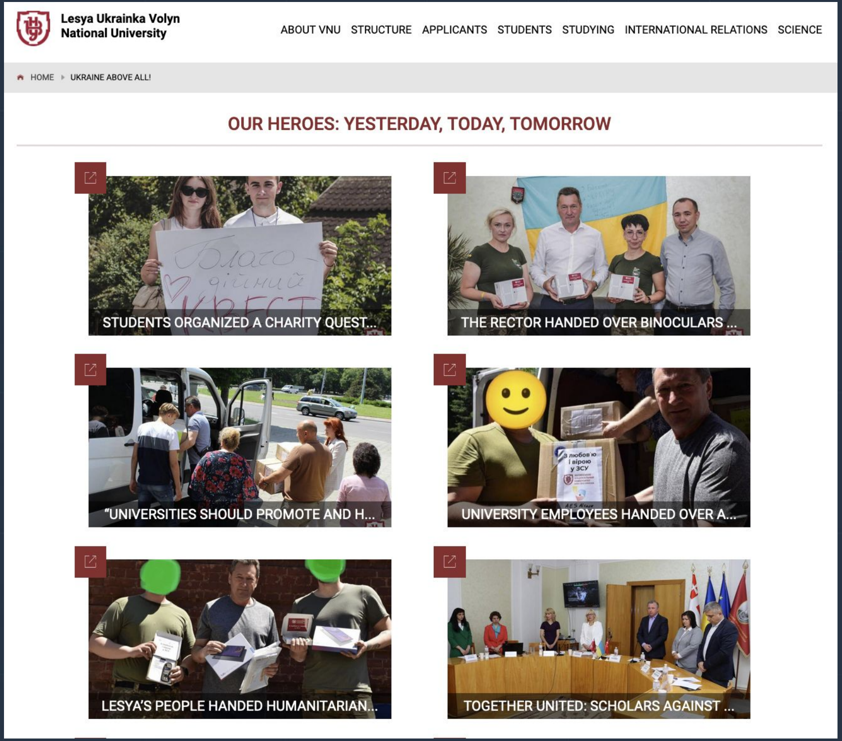
COMMUNITY

We are CYBERPORT institute — освіта МАЙБУТНЬОГО!

При підтримці:

Міністерства освіти і науки України

Державної служби спеціального зв’язку та захисту інформації України



Lesya Ukrainka Volyn National University

OUR HEROES: YESTERDAY, TODAY, TOMORROW

STUDENTS ORGANIZED A CHARITY QUEST...

THE RECTOR HANDED OVER BINOCULARS ...

“UNIVERSITIES SHOULD PROMOTE AND H...

UNIVERSITY EMPLOYEES HANDED OVER A...

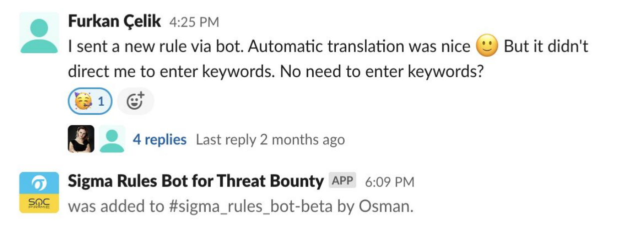
LESYA’S PEOPLE HANDED HUMANITARIAN...

TOGETHER UNITED: SCHOLARS AGAINST ...

Sigma & ATT&CK education via Slack

Sigma Rules bot for Threat Bounty

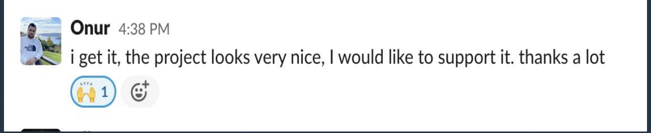
Code, test, tag with att&ck & share Sigma rules in slack



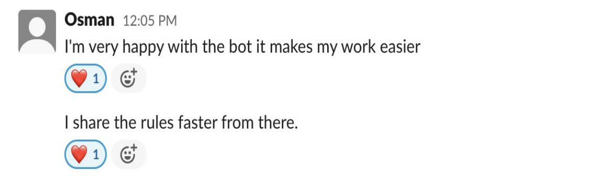
Furkan Çelik 4:25 PM
I sent a new rule via bot. Automatic translation was nice 🙂 But it didn't direct me to enter keywords. No need to enter keywords?

4 replies Last reply 2 months ago

Sigma Rules Bot for Threat Bounty APP 6:09 PM
was added to #sigma_rules_bot-beta by Osman.

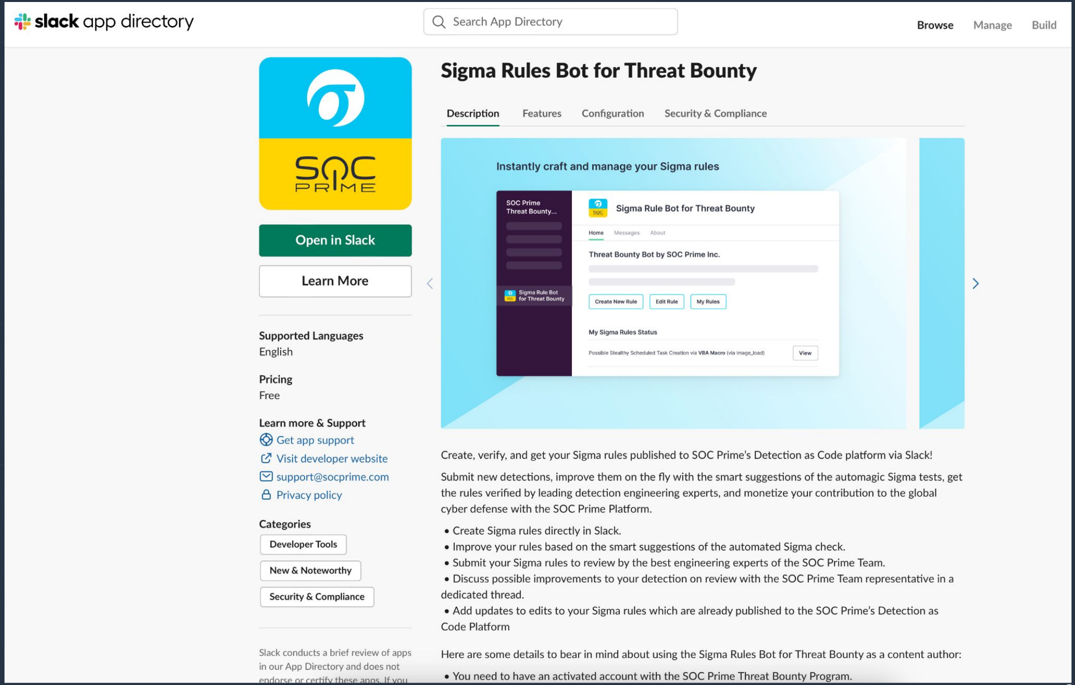


Onur 4:38 PM
i get it, the project looks very nice, I would like to support it. thanks a lot



Osman 12:05 PM
I'm very happy with the bot it makes my work easier

I share the rules faster from there.



Sigma Rules Bot for Threat Bounty

Threat Bounty Bot by SOC Prime Inc.

My Sigma Rules Status

Possible Stealthy Scheduled Task Creation via **VBA Macro** (via image_load)

Supported Languages
English

Pricing
Free

Learn more & Support
Get app support
Visit developer website
support@socprime.com
Privacy policy

Categories
Developer Tools
New & Noteworthy
Security & Compliance

Slack conducts a brief review of apps in our App Directory and does not endorse or certify these apps. If you

Create, verify, and get your Sigma rules published to SOC Prime's Detection as Code platform via Slack!

Submit new detections, improve them on the fly with the smart suggestions of the automagic Sigma tests, get the rules verified by leading detection engineering experts, and monetize your contribution to the global cyber defense with the SOC Prime Platform.

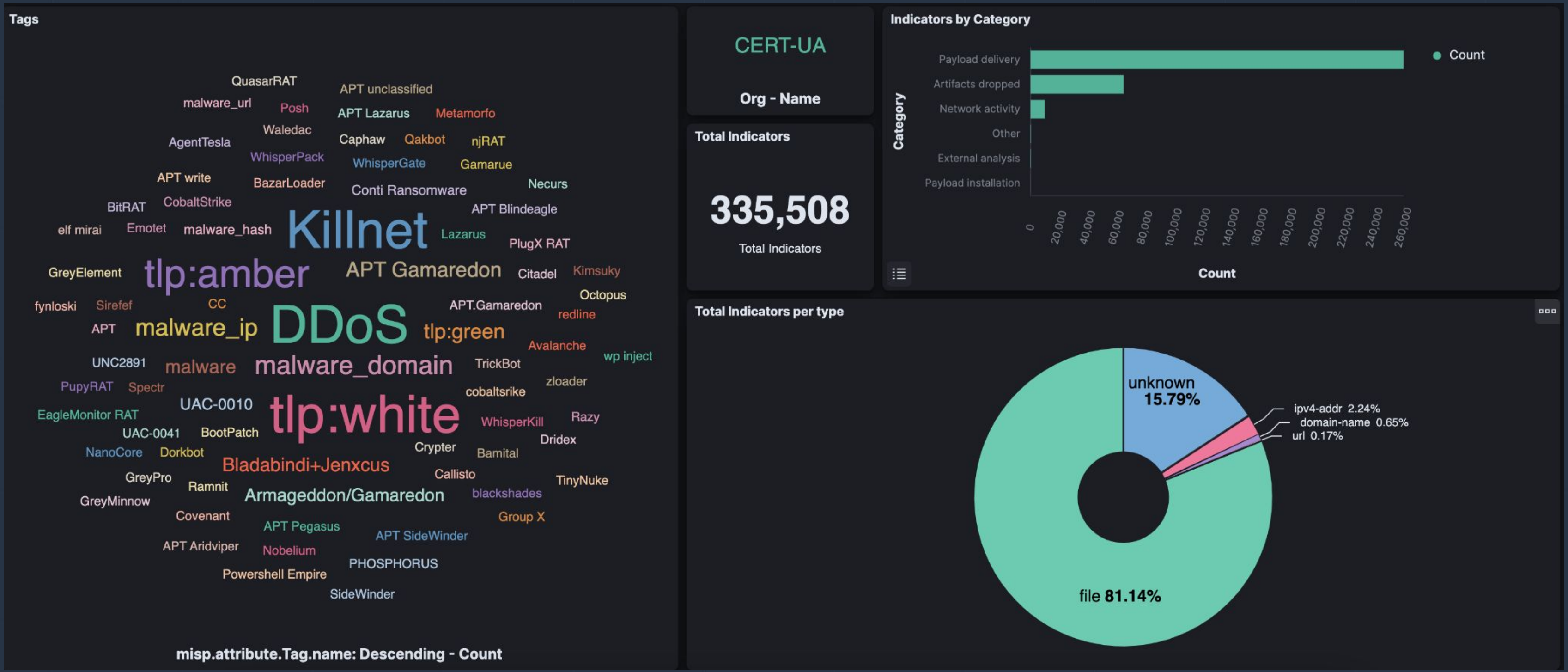
- Create Sigma rules directly in Slack.
- Improve your rules based on the smart suggestions of the automated Sigma check.
- Submit your Sigma rules to review by the best engineering experts of the SOC Prime Team.
- Discuss possible improvements to your detection on review with the SOC Prime Team representative in a dedicated thread.
- Add updates to edits to your Sigma rules which are already published to the SOC Prime's Detection as Code Platform

Here are some details to bear in mind about using the Sigma Rules Bot for Threat Bounty as a content author:

- You need to have an activated account with the SOC Prime Threat Bounty Program.

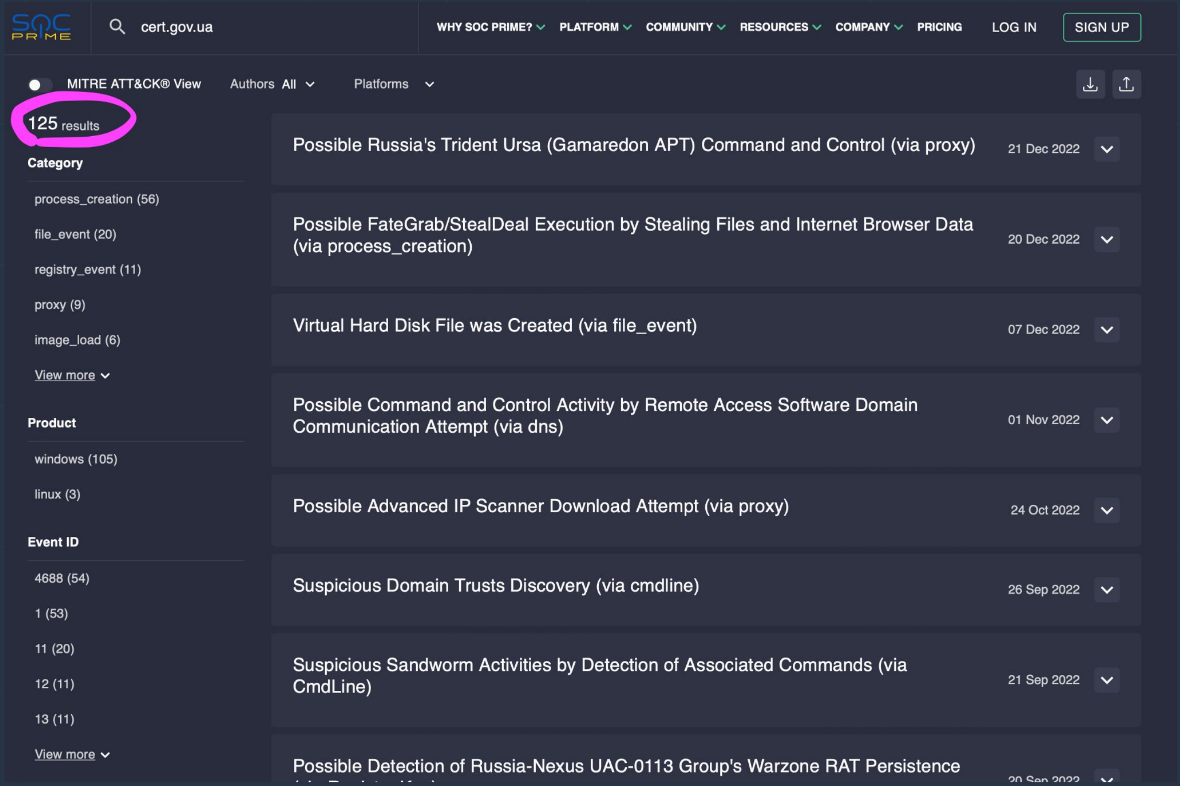
335,508 Indicators of Compromise

Shared by CERT-UA team, from 2100 / 1500 cyber attacks | 2022



125 behavior Sigma rules

Developed and linked to incidents publicly disclosed by CERT-UA



cert.gov.ua

Authors All

125 results

Category

- process_creation (56)
- file_event (20)
- registry_event (11)
- proxy (9)
- image_load (6)
- View more

Product

- windows (105)
- linux (3)

Event ID

- 4688 (54)
- 1 (53)
- 11 (20)
- 12 (11)
- 13 (11)
- View more

Possible Russia's Trident Ursa (Gamaredon APT) Command and Control (via proxy)	21 Dec 2022
Possible FateGrab/StealDeal Execution by Stealing Files and Internet Browser Data (via process_creation)	20 Dec 2022
Virtual Hard Disk File was Created (via file_event)	07 Dec 2022
Possible Command and Control Activity by Remote Access Software Domain Communication Attempt (via dns)	01 Nov 2022
Possible Advanced IP Scanner Download Attempt (via proxy)	24 Oct 2022
Suspicious Domain Trusts Discovery (via cmdline)	26 Sep 2022
Suspicious Sandworm Activities by Detection of Associated Commands (via CmdLine)	21 Sep 2022
Possible Detection of Russia-Nexus UAC-0113 Group's Warzone RAT Persistence	20 Sep 2022

Sigma rules to stay ahead of the threats

Practical proof

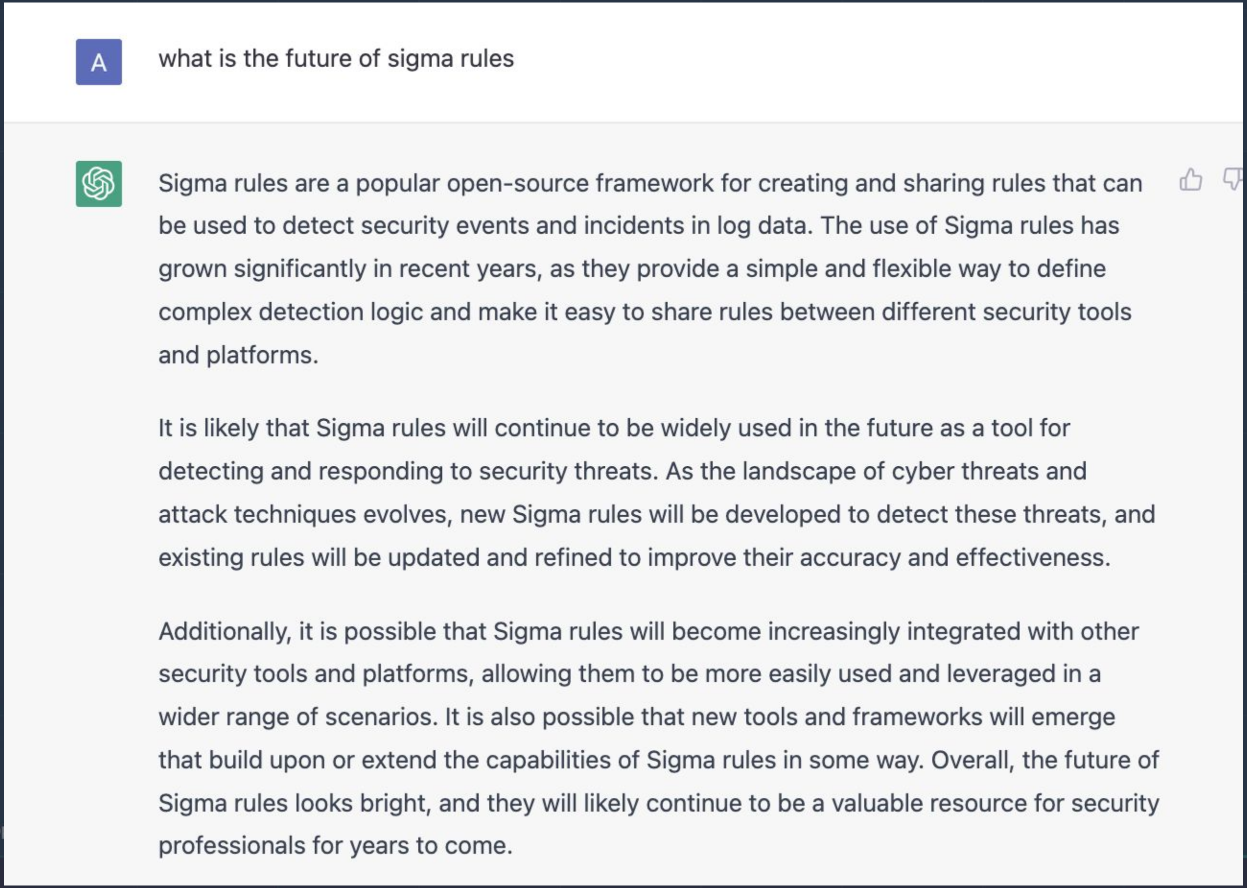
2100 cyber attacks just against Ukraine in 2022

335,508 Indicators of Compromise (compute challenge)

125 behavior Sigma rules to detect all TLP:WHITE incidents

>51% of rules created in 2020-2021

We asked ChatGPT:



A

what is the future of sigma rules

Sigma rules are a popular open-source framework for creating and sharing rules that can be used to detect security events and incidents in log data. The use of Sigma rules has grown significantly in recent years, as they provide a simple and flexible way to define complex detection logic and make it easy to share rules between different security tools and platforms.

It is likely that Sigma rules will continue to be widely used in the future as a tool for detecting and responding to security threats. As the landscape of cyber threats and attack techniques evolves, new Sigma rules will be developed to detect these threats, and existing rules will be updated and refined to improve their accuracy and effectiveness.

Additionally, it is possible that Sigma rules will become increasingly integrated with other security tools and platforms, allowing them to be more easily used and leveraged in a wider range of scenarios. It is also possible that new tools and frameworks will emerge that build upon or extend the capabilities of Sigma rules in some way. Overall, the future of Sigma rules looks bright, and they will likely continue to be a valuable resource for security professionals for years to come.

Sigma rules

What's next

Update of Uncoder.IO to help write rules faster and better
Free online education for thousands of students on Sigma rules

Sigma for OT, IoT, Space and Connected Vehicles
Collective Cyberdefense System using Sigma rules + feedback

chatGPT can generate basic rules. sometimes.

THANK YOU!

search anything on sigma rules @ socprime.com

Translate Sigma to SIEM, EDR & Big Data queries @ uncoder.io

twitter: @andriinb

one UI & feedback, get involved @

https://github.com/socprime/the-prime-hunt

SigmaHQ https://github.com/SigmaHQ/sigma