Pointers for complying with the European Resilience Mandates

IIA Norway Risk Roundtable May 15, 2024

Your IIA Norway Risk Roundtable Hosts:

The Institute of
Internal Auditors
Norge

Ellen Brataas, CEO IIA Norway

Ellen has extensive industry and consulting experience across domains like risk management, internal audit and IT resilience.
As CEO of IIA Norway she is continuously advancing GRC best practice and readiness in Scandinavia through peer exchanges, expert blogs and training.
GRC practitioners in the region and beyond draw on Ellen's thought leadership informed by her industry and consulting lens as well as insight from the IIA Norway network.

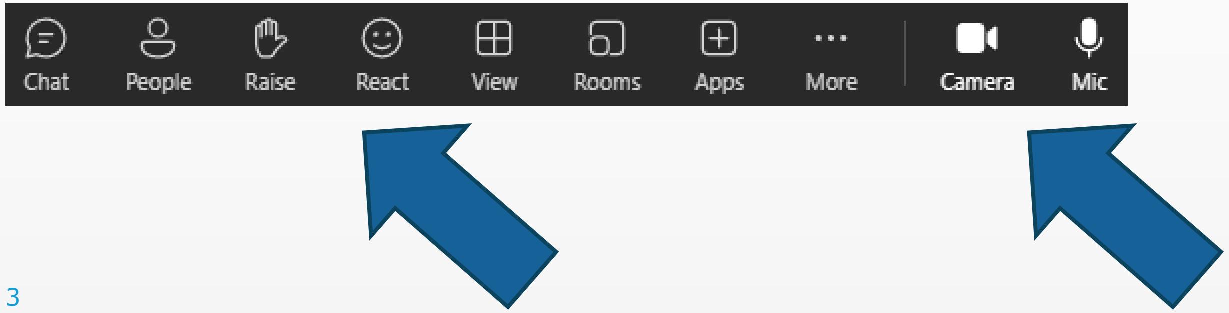
Chika Okoli, GRC Technology Manager

Chika Okoli is a GRC Technology Manager who helps organisations address GRC initiatives and mandates with technology.
The throughline in his career has been digital transformation across domains like KYC, procurement, supply chain finance and GRC.
Lately his focus has been the wave of resilience mandates, that he writes and speaks about at practitioner forums across Europe.

Some Housekeeping:

- A recording of the session will be made available to registrants and participants.
- The lines are not muted because this session will be interactive throughout.
- However, please mute yourself if you are not speaking to avoid audio issues.

Participation Options



A potpourri of European Resilience Mandates

DORA
Digital
Operational
Resilience
Act

NASJONAL SIKKERHETSMYNDIGHET

National Security Act

TISAX®

Trusted Information Security
Assessments Exchange

BaFin

Supervisory Requirements for IT in
Financial Institutions (BAIT)

finma

Circular 2023/1
Operational risks and resilience – banks

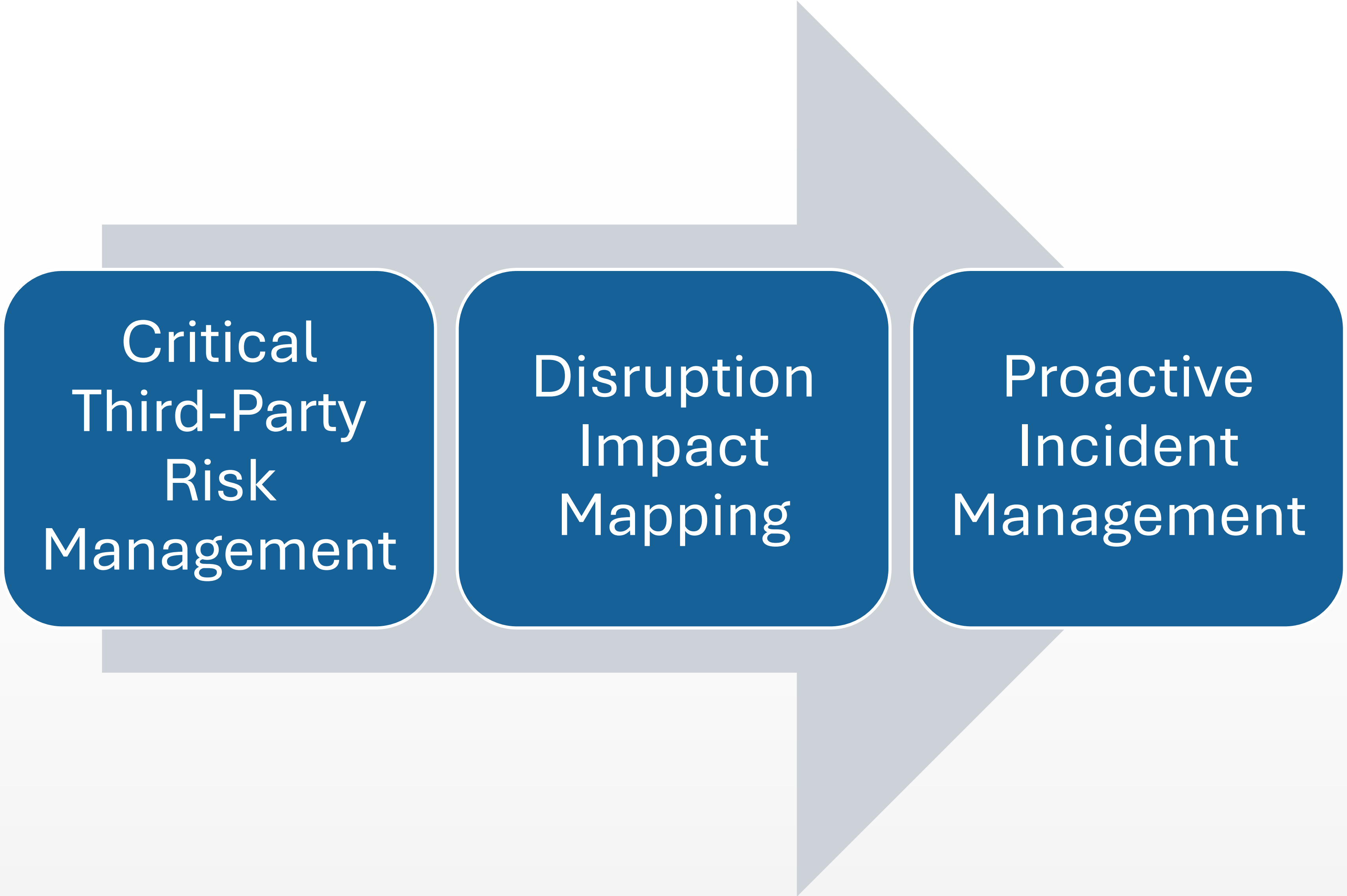
NIS2 Directive

Network and Information
Security (NIS) Directive

BANK OF ENGLAND
PRUDENTIAL REGULATION
AUTHORITY

Supervisory Statement | SS1/21

The common direction of European Resilience Mandates

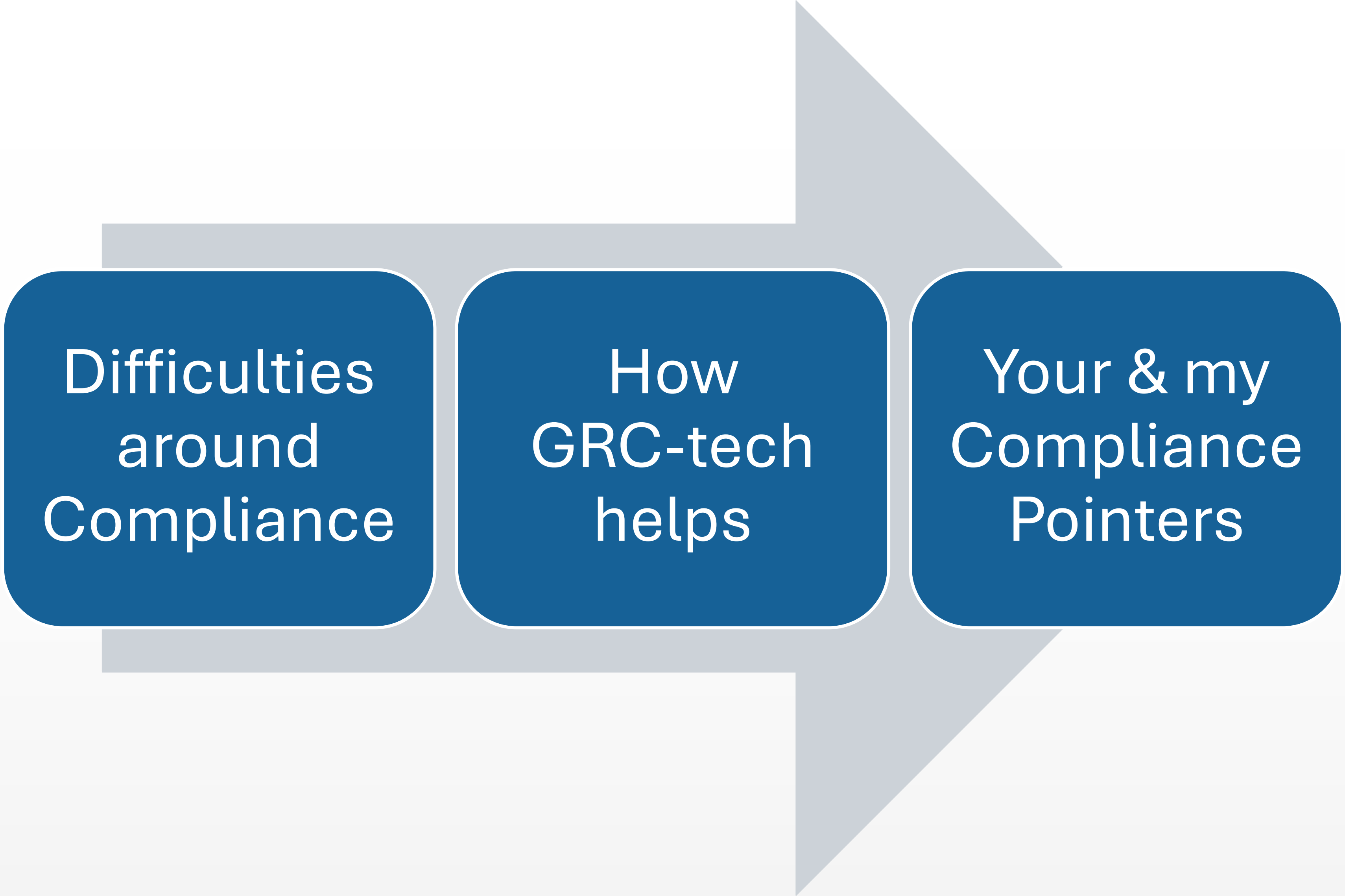


Critical Third-Party Risk Management

Disruption Impact Mapping

Proactive Incident Management

Agenda:



Difficulties around Compliance

How GRC-tech helps

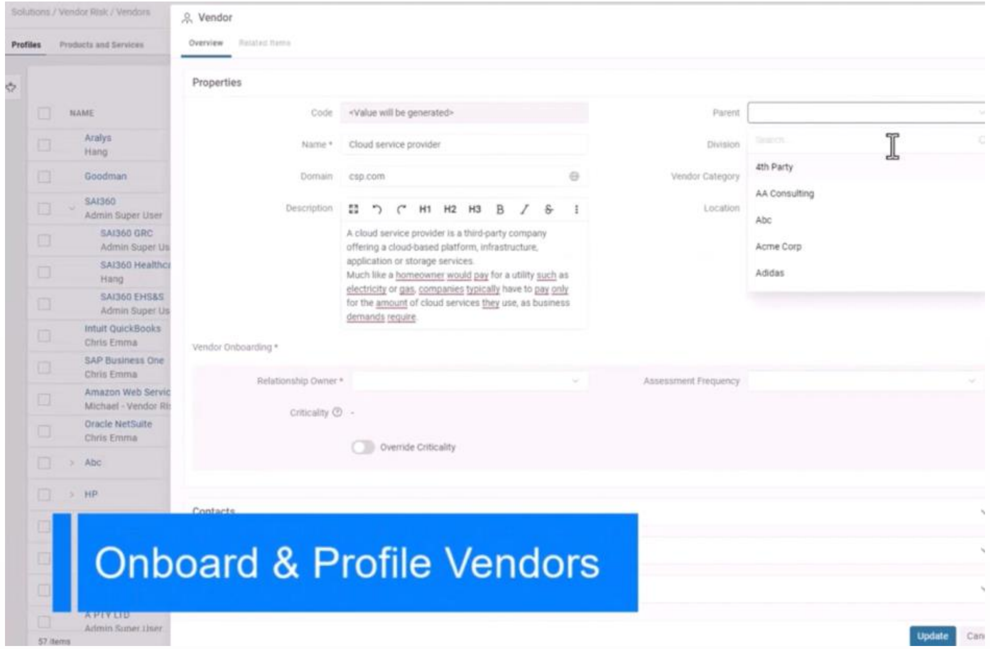
Your & my Compliance Pointers

You collaborate with a sea of suppliers.

Who is a critical supplier here?

Who is a critical supplier here?

Determine Third-Party Criticality before incidents through connected (inherent) Risk Assessments



Properties

Code: <Value will be generated>

Name *: Cloud service provider

Domain: csp.com

Description: A cloud service provider is a third-party company offering a cloud-based platform, infrastructure, application or storage services.
Much like a homeowner would pay for a utility such as electricity or gas, companies typically have to pay only for the amount of cloud services they use, as business demands require.

Parent:

Division:

Vendor Category:

Location:

4th Party
AA Consulting
Abc
Acme Corp
Adidas

Vendor Onboarding *

Relationship Owner *:

Assessment Frequency:

Criticality: -

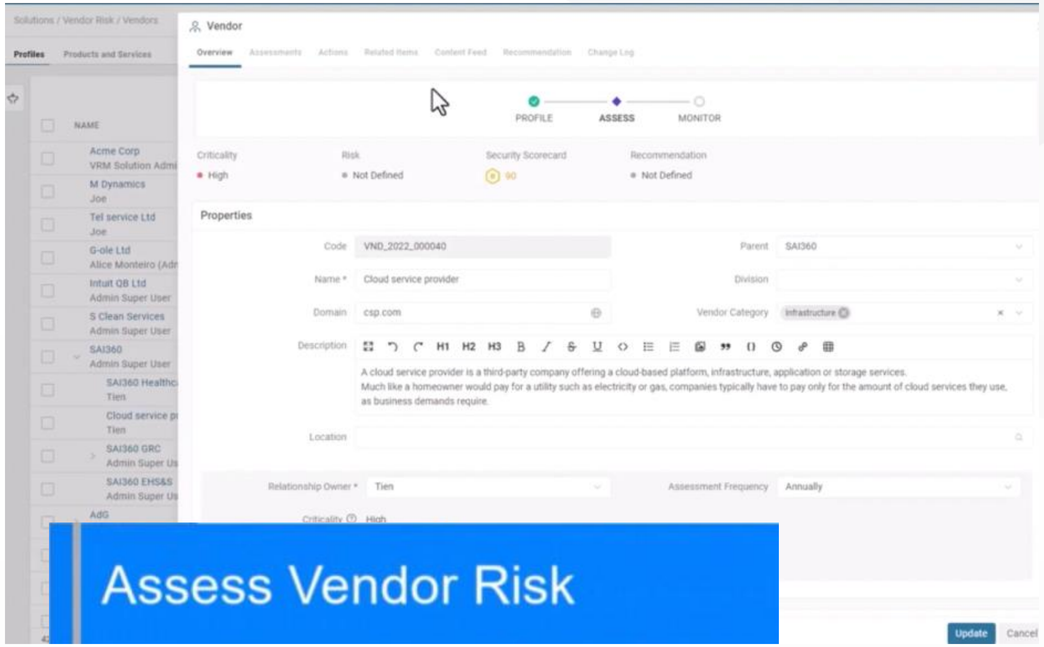
Override Criticality

Contacts

NAME
Aralys Hang
Goodman
SAI360 Admin Super User
SAI360 GRC Admin Super Us
SAI360 Healthc Hang
SAI360 EHS&S Admin Super Us
Intuit QuickBooks Chris Emma
SAP Business One Chris Emma
Amazon Web Servic Michael - Vendor Ri
Oracle NetSuite Chris Emma
Abc
HP
A PTY LTD Admin Super User

57 items

Onboard & Profile Vendors



Criticality: High

Risk: Not Defined

Security Scorecard: 90

Recommendation: Not Defined

Properties

Code: VND_2022_000040

Name *: Cloud service provider

Domain: csp.com

Description: A cloud service provider is a third-party company offering a cloud-based platform, infrastructure, application or storage services.
Much like a homeowner would pay for a utility such as electricity or gas, companies typically have to pay only for the amount of cloud services they use, as business demands require.

Location:

Parent: SAI360

Division:

Vendor Category: Infrastructure

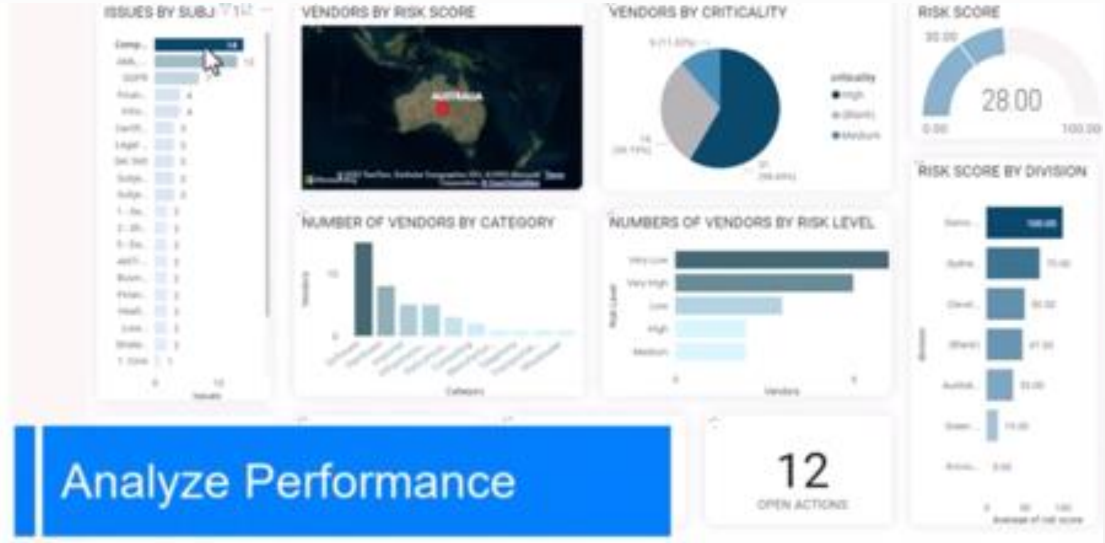
Relationship Owner *: Tien

Assessment Frequency: Annually

Criticality: High

NAME
Acme Corp VRM Solution Admi
M Dynamics Joe
Tel service Ltd Joe
G-ole Ltd Alice Monteiro (Adr
Intuit QB Ltd Admin Super User
S Clean Services Admin Super User
SAI360 Admin Super User
SAI360 Healthc Tien
Cloud service p Tien
SAI360 GRC Admin Super Us
SAI360 EHS&S Admin Super Us
AdG

Assess Vendor Risk



Analyze Performance

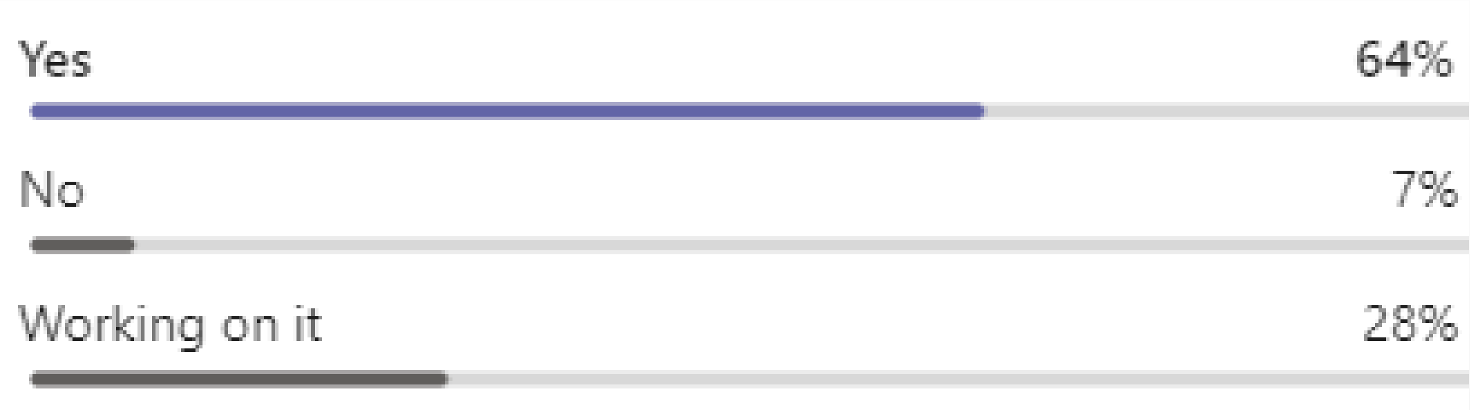
My Pointers for aligning on Criticality

- Settle on a common risk language (i.e. harmonise risk reporting etc.)
- Account for risk dimensions (i.e., processes, risk categories, threat vectors etc.)
- Create a third-party risk inventory (i.e. concentration risk, inherent risk etc.)

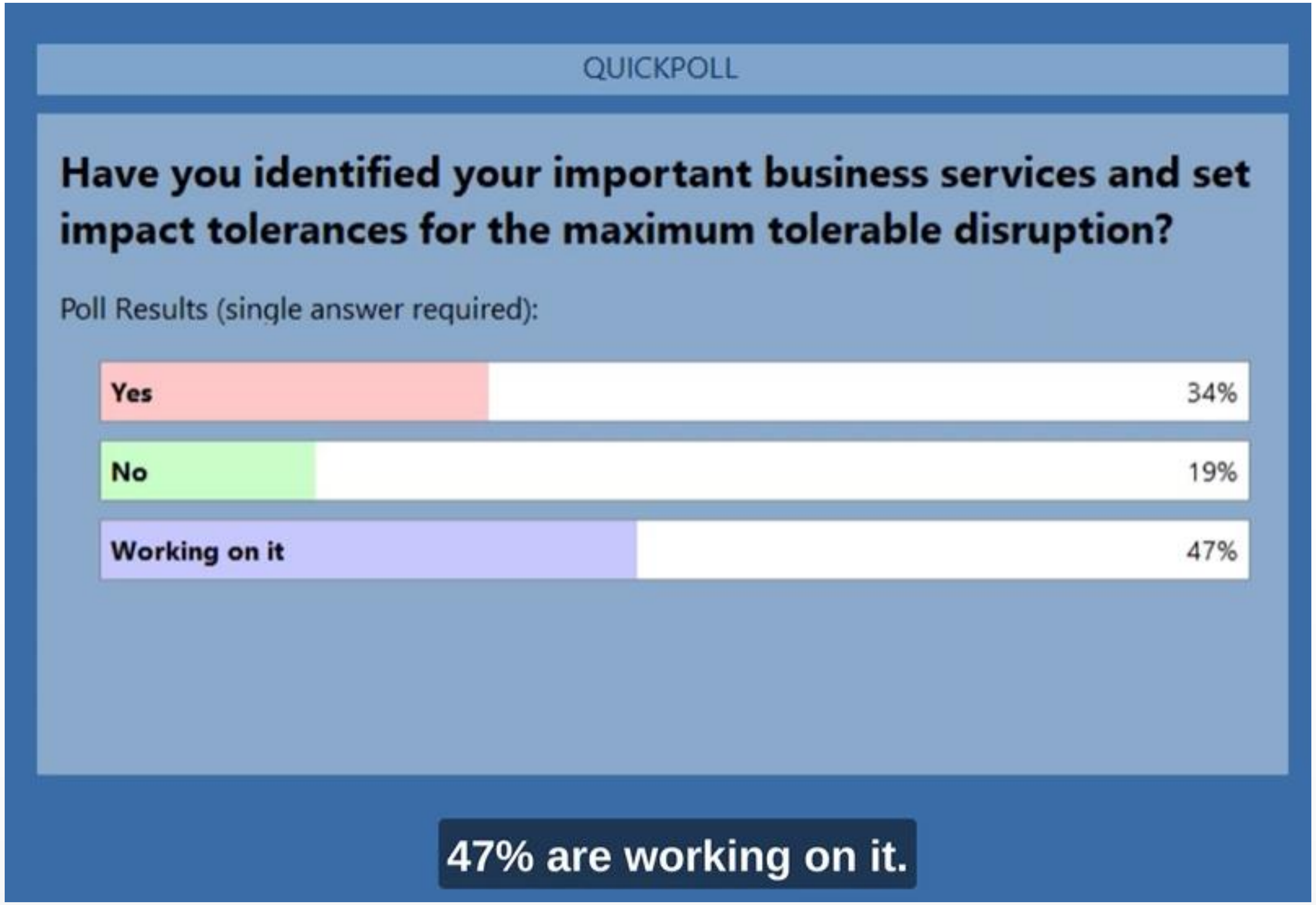
Pointers from the Risk Roundtable participants:

- Categorise suppliers based on critical services and applications they provide
- Account for the sourcing strategy, which could provide clues on criticality (i.e. some inherently risky activities might be outsourced→ hence the partners are likely critical)
- Use the litmus test "any supplier that can disrupt your operation is critical”
- Make criticality assessments a continuous practice with the appropriate tone at the top to drive the continuous evaluation
- Learn from breach notifications by identifying the critical suppliers that led to it.

Have you identified your important business services and set tolerances for the acceptable disruption?



Room for improvement in Disruption Impact Mapping



QUICKPOLL

Have you identified your important business services and set impact tolerances for the maximum tolerable disruption?

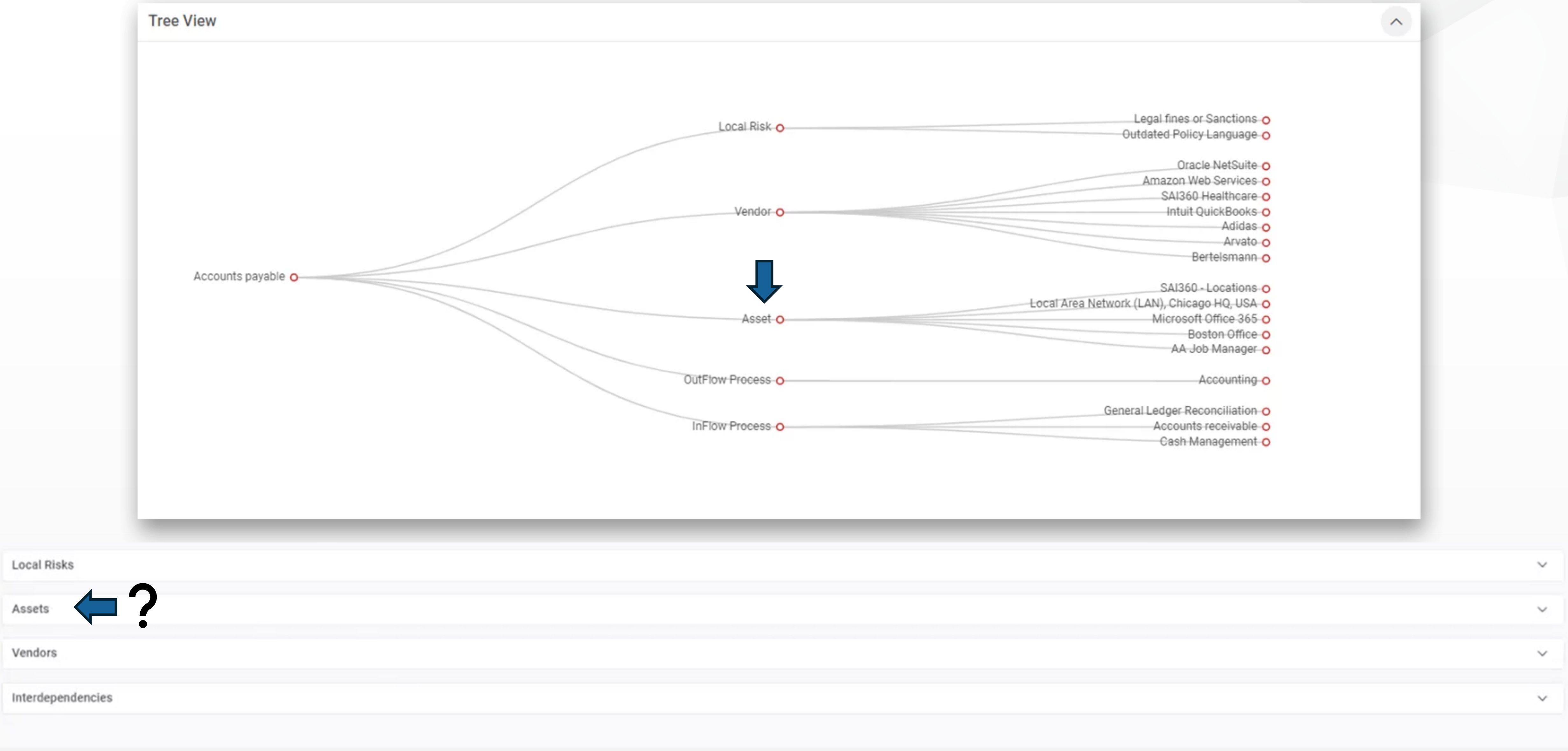
Poll Results (single answer required):

Yes	34%
No	19%
Working on it	47%

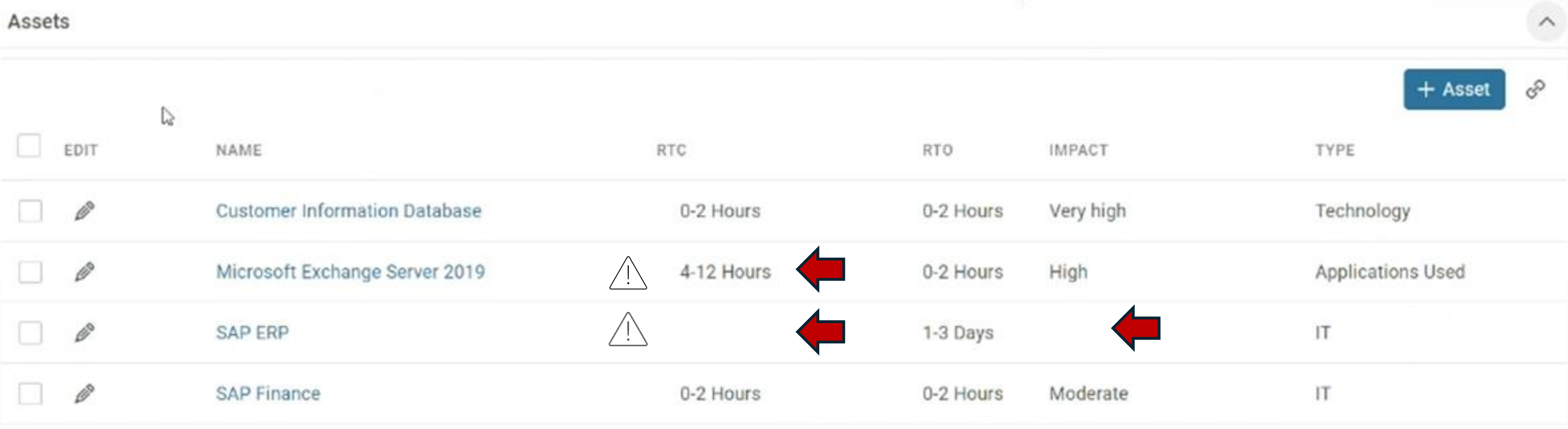
47% are working on it.

Source: EU DORA Webinar Feb. 2023

GRC Technology eases Disruption Impact Mapping



Monitor the Resilience Chain & receive timely Business Continuity Alerts



Assets

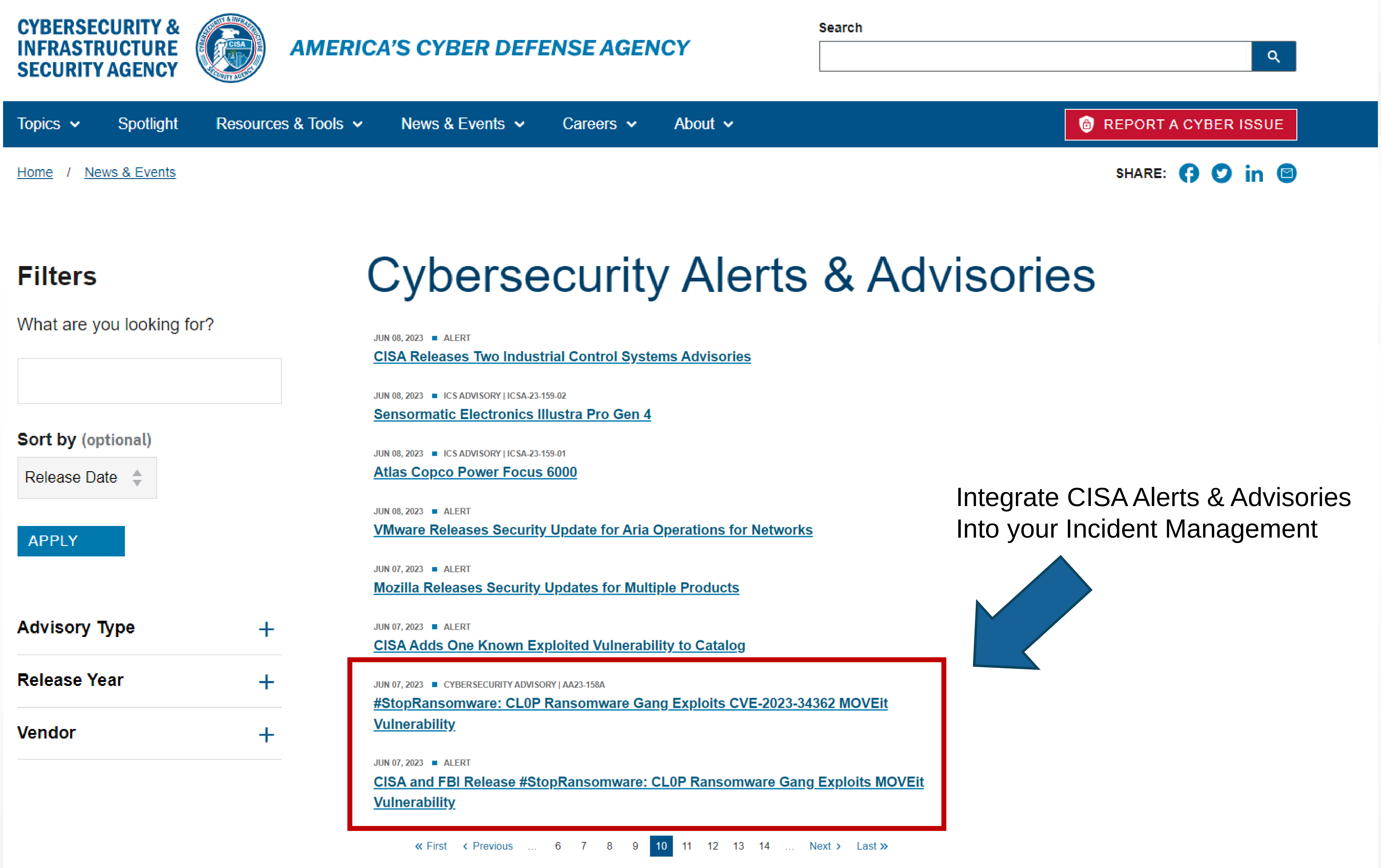
□	EDIT	NAME	RTC	RTO	IMPACT	TYPE
□	✎	Customer Information Database	0-2 Hours	0-2 Hours	Very high	Technology
□	✎	Microsoft Exchange Server 2019	⚠ 4-12 Hours	0-2 Hours	High	Applications Used
□	✎	SAP ERP	⚠	1-3 Days		IT
□	✎	SAP Finance	0-2 Hours	0-2 Hours	Moderate	IT

My Pointers for Disruption Impact Mapping

- Identify critical assets
- Map linkages to processes, affected stakeholders, regulatory dimensions etc.
- Set and monitor disruption tolerance (i.e. EU DORA, NIS2 and the UK's PRA requirements)

Pointers from the Risk Roundtable participants:

- Map the recovery sequence to ease the recovery prioritisation (i.e. Ascertain which assets need to be recovered first to be operational)
- Ensure that critical assets have Recovery Time Capabilities (RTCs) that are below the Recovery Time Objectives (RTOs) and monitor for unacceptable RTCs.
- Aggregate RTC/O data to arrive at the recovery metrics of your important business services (IBS) as a whole (i.e. the IBS recovery might be the sum of RTCs/Os of several assets that you identified beforehand-see my pointer above)



Cybersecurity Alerts & Advisories

JUN 08, 2023 ■ ALERT
CISA Releases Two Industrial Control Systems Advisories

JUN 08, 2023 ■ ICS ADVISORY | ICSA-23-159-02
Sensormatic Electronics Illustra Pro Gen 4

JUN 08, 2023 ■ ICS ADVISORY | ICSA-23-159-01
Atlas Copco Power Focus 6000

JUN 08, 2023 ■ ALERT
VMware Releases Security Update for Aria Operations for Networks

JUN 07, 2023 ■ ALERT
Mozilla Releases Security Updates for Multiple Products

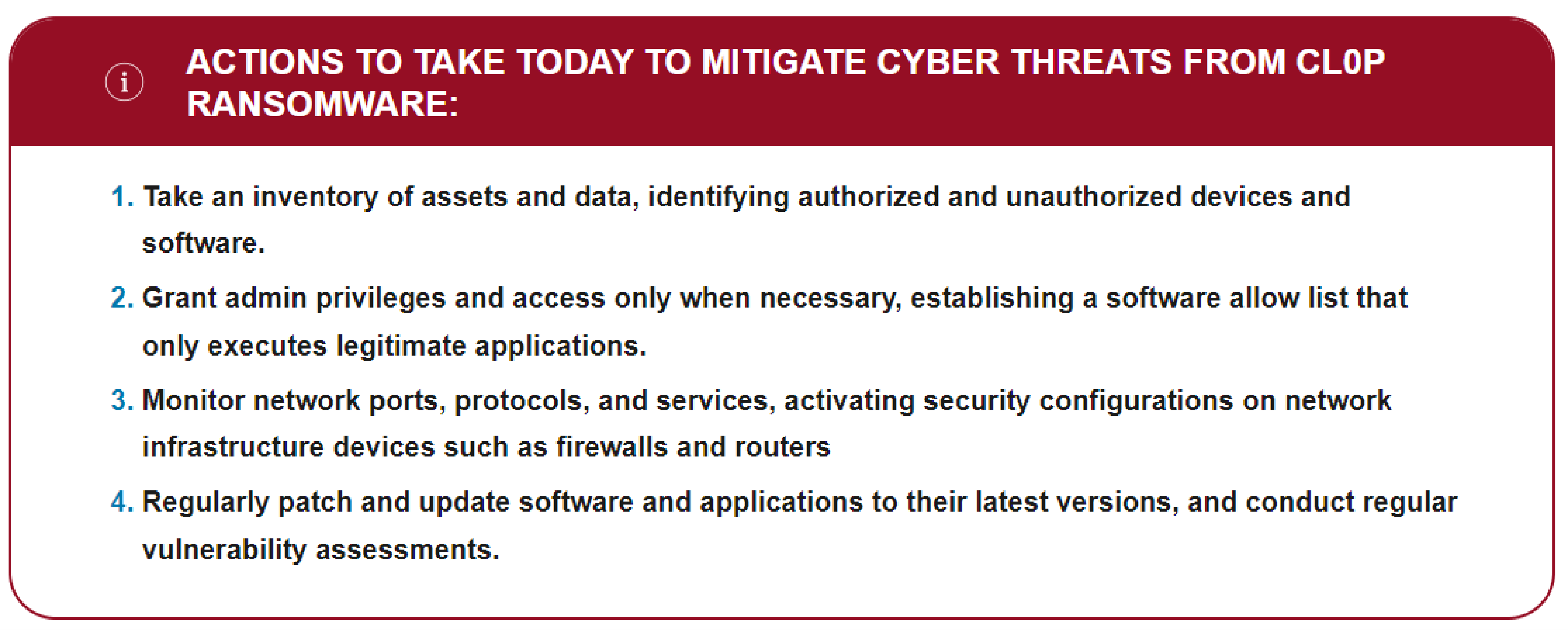
JUN 07, 2023 ■ ALERT
CISA Adds One Known Exploited Vulnerability to Catalog

JUN 07, 2023 ■ CYBERSECURITY ADVISORY | AA23-158A
#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability

JUN 07, 2023 ■ ALERT
CISA and FBI Release #StopRansomware: CL0P Ransomware Gang Exploits MOVEit Vulnerability

Integrate CISA Alerts & Advisories Into your Incident Management

Immediate actions from the CISA Alert can be executed with the help of GRC Technology

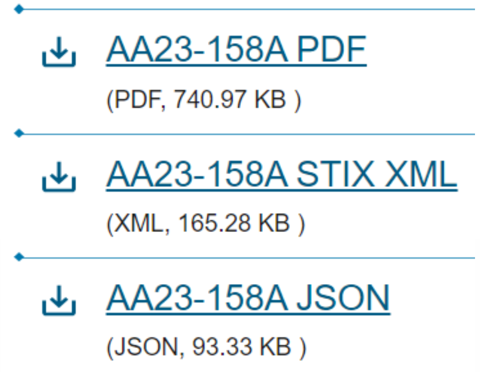


ⓘ **ACTIONS TO TAKE TODAY TO MITIGATE CYBER THREATS FROM CL0P RANSOMWARE:**

1. Take an inventory of assets and data, identifying authorized and unauthorized devices and software.
2. Grant admin privileges and access only when necessary, establishing a software allow list that only executes legitimate applications.
3. Monitor network ports, protocols, and services, activating security configurations on network infrastructure devices such as firewalls and routers
4. Regularly patch and update software and applications to their latest versions, and conduct regular vulnerability assessments.

Further actions:

1. Download the PDF/STIX/JSON version of the CISA report

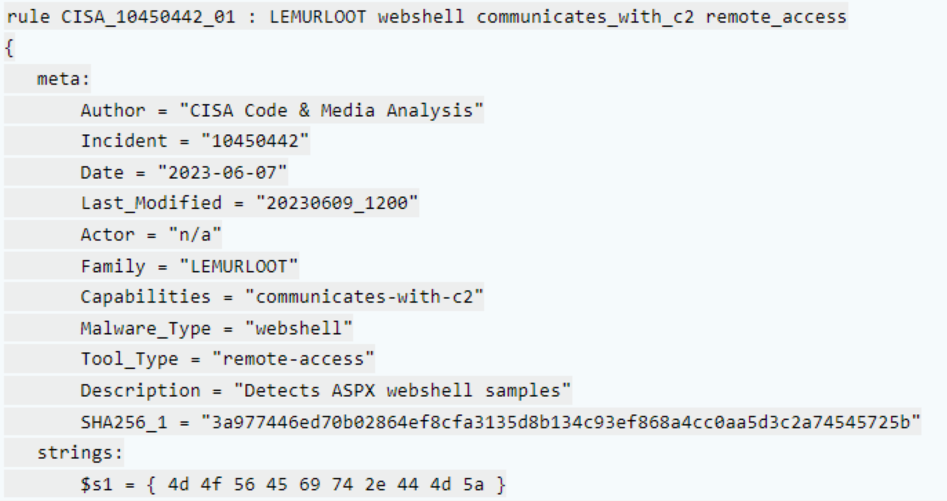


AA23-158A PDF
(PDF, 740.97 KB)

AA23-158A STIX XML
(XML, 165.28 KB)

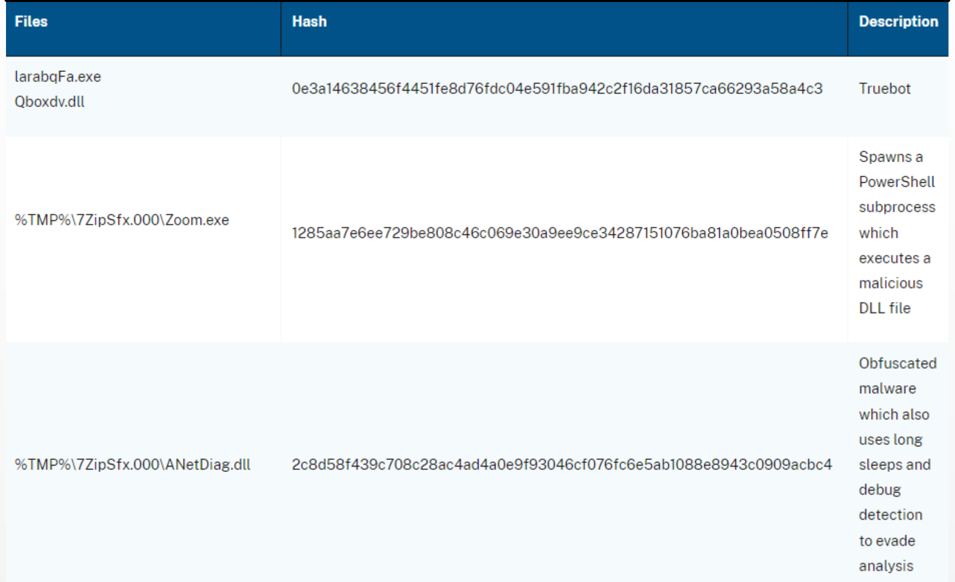
AA23-158A JSON
(JSON, 93.33 KB)

2. Apply Yara Rules to detect malicious activity



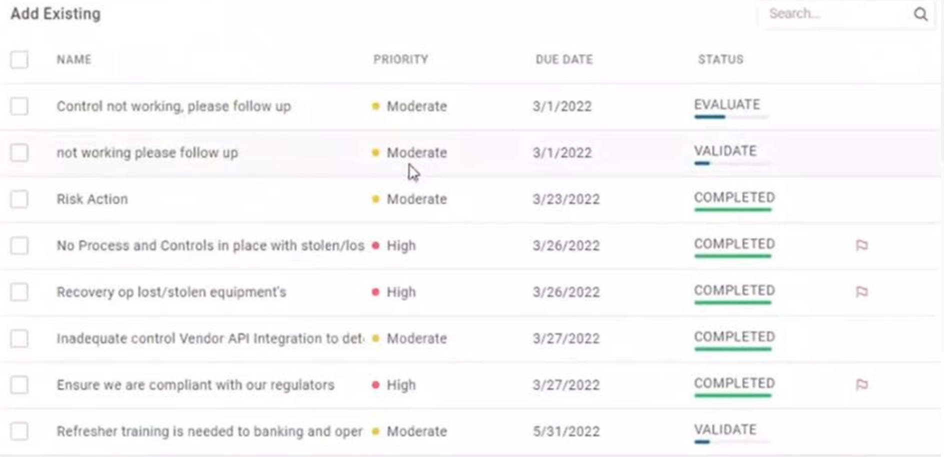
```
rule CISA_10450442_01 : LEMURLOOT webshell communicates_with_c2 remote_access
{
   meta:
       Author = "CISA Code & Media Analysis"
       Incident = "10450442"
       Date = "2023-06-07"
       Last_Modified = "20230609_1200"
       Actor = "n/a"
       Family = "LEMURLOOT"
       Capabilities = "communicates-with-c2"
       Malware_Type = "webshell"
       Tool_Type = "remote-access"
       Description = "Detects ASPX webshell samples"
       SHA256_1 = "3a977446ed70b02864ef8cfa3135d8b134c93ef868a4cc0aa5d3c2a74545725b"
   strings:
       $s1 = { 4d 4f 56 45 69 74 2e 44 4d 5a }
```

3. Scan for indicators of compromise



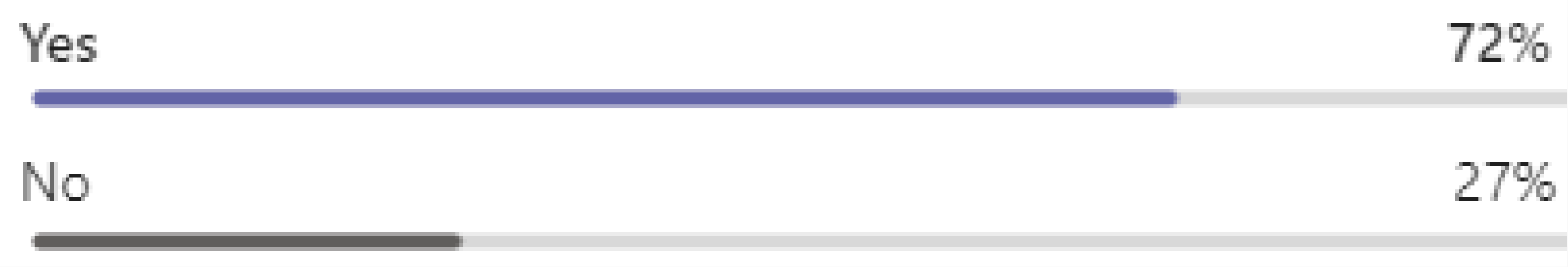
Files	Hash	Description
larabqFa.exe Qboxdv.dll	0e3a14638456f4451fe8d76fdc04e591fba942c2f16da31857ca66293a58a4c3	Truebot
%TMP%\7ZipSfx.000\Zoom.exe	1285aa7e6ee729be808c46c069e30a9ee9ce34287151076ba81a0bea0508ff7e	Spawns a PowerShell subprocess which executes a malicious DLL file
%TMP%\7ZipSfx.000\ANetDiag.dll	2c8d58f439c708c28ac4ad4a0e9f93046cf076fc6e5ab1088e8943c0909acbc4	Obfuscated malware which also uses long sleeps and debug detection to evade analysis

4. Track & Manage Task Completion



□	NAME	PRIORITY	DUE DATE	STATUS	
□	Control not working, please follow up	● Moderate	3/1/2022	EVALUATE	
□	not working please follow up	● Moderate	3/1/2022	VALIDATE	
□	Risk Action	● Moderate	3/23/2022	COMPLETED	
□	No Process and Controls in place with stolen/los	● High	3/26/2022	COMPLETED	⚐
□	Recovery op lost/stolen equipment's	● High	3/26/2022	COMPLETED	⚐
□	Inadequate control Vendor API Integration to det	● Moderate	3/27/2022	COMPLETED	
□	Ensure we are compliant with our regulators	● High	3/27/2022	COMPLETED	⚐
□	Refresher training is needed to banking and oper	● Moderate	5/31/2022	VALIDATE	

Do you use free data sources and tools for threat monitoring and emerging risk management?



My Pointers for proactive Incident Management

- Incorporate threat, risk and incident advisories (i.e. CISA, MITRE ATT&CK etc.)
- Scan assets to pre-empt incidents
- Report latent threats, potential risk exposures and near-misses internally

Pointers from the Risk Roundtable participants:

- In addition to the free sources there are premium data sources and services that curate data for pre-empting incidents and utilise AI to reduce false negatives (i.e. www.EPAM.com)
- Reduce the attack surface by limiting devices to authorised and vetted ones (i.e. including internal threats through Active Directory management linked to authorised employee/user devices, access rights hardened with MFA ideally)
- Consider how network security changes over time due to management decisions with their knock-on effects on incident management

Resilience is…

Let’s keep the conversation going:

The Institute of
Internal Auditors

Norge

Chika Okoli

GRC Technology Manager

www.iia.no

www.linkedin.com/in/chika-o-n

Source of the Incident Management pointer and further sources for threat intelligence

www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a	Implement cyber threat management suggestions (the example from slide 17- 19).
www.cisa.gov/news-events/cybersecurity-advisories	Integrate **CISA** data and combine with automated GRC technology workflows.
https://malpedia.caad.fkie.fraunhofer.de	Request membership of the **Malpedia** Malware Defence Group then integrate data for threat and risk management with GRC technology workflows.
https://malpedia.caad.fkie.fraunhofer.de/details/win.clop	Implement cyber threat management & detection suggestions from the *Malware Defence Group*.
https://github.com/xaitax/SploitScan	**SploitScan** is a free powerful and user-friendly tool designed by Alexander Hagenah, Head of Cyber Controls at SIX. It streamlines the process of identifying exploits for known vulnerabilities as well as the risk scoring of their respective exploitation probabilities.