
TRUESEC
Hotlandskapet 2023

TRUESEC

Marcus.murray@truesec.com

I provide cyber security advisory, insights and capability. Focus on government bodies, boards and C-level executives

Marcus Murray

Founder of Truesec Group | Protecting the society, governments & organizations against cyber threats | Threat Intelligence | Defense | Offense | Winner of Grand Security Award 2023 | No 1 most influential in Tech 2023

Stockholm, Stockholm, Sverige

15,432 followers · 500+ connections


Hotlandskapet 2023

October 7

Cyber is now an integrated component in every national conflict

TRUESEC

06:12

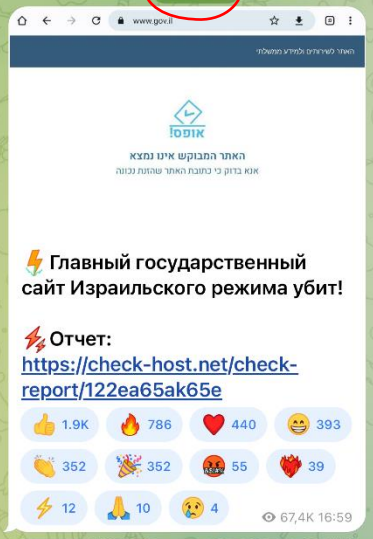
Clear Cache | 1 Selected | Cancel

Pinned Message
ממשלת ישראל, אתה אשם בשפיכות הדמים הזו. עוד ב-

Translate to English

October 8

WE ARE I … d a photo



⚡Главный государственный сайт Израильского режима убит!

⚡Отчет:
https://check-host.net/check-report/122ea65ak65e

👍 1.9K | 🔥 786 | ❤️ 440 | 😁 393
👏 352 | 🎉 352 | 🤬 55 | 💔 39
⚡ 12 | 🙏 10 | 😢 4

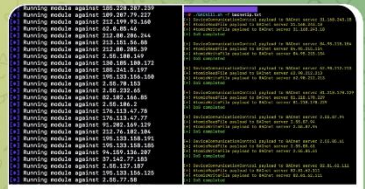
67,4K 16:59

05:53

Sök

41 | AnonymousSudan Chat
2 773 members, 108 online

Pinned Message
Photo



❗Israeli industrial control systems have been attacked by AnonymousSudan ! SiegedSec

- TARGET: Global Navigational Satellite Systems (GNSS)
Various GPS systems around the country will go offline, this could affect industrial systems, critical infrastructure, and other machines

- TARGET: Building Automation and Control Networks (BACNet)
Building control systems could be shut down or modified, possibly resulting in an energy surge, building evacuation, computer shutdown, inconvenience, and critical infrastructure shutdown.

- TARGET: Modbus Industrial Control Systems
Industrial systems around the

The admins of this group have restricted your ability to s… messages.

05:51

Sök

Back | 618 of 623

#AnonymousSudan
#KILLNET

Anonymous Sudan
10-08-23

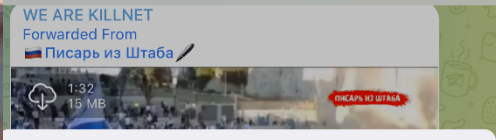
06:02

Safari

41 | WE ARE KILLNET
103 032 subscribers

Pinned Message
ממשלת ישראל, אתה אשם בשפיכות הדמים הזו. עוד ב-

Translate to English



Close | Translate

Russian
Израильтяне или Евреи? more

English
Israelis or Jews?

Jews around the world do not support the ISRAELITES.

They want the genocide of the Arabs, they consider themselves God's chosen ones..

Israel is an invented state, and now, in full coordination with the United States, they will exterminate Arabs and drive them out of their own home.

t.me/killnet_mirror

Copy Translation

Change Language

TRUESEC

The cyber component enables any individual, group or nation the capability to engage in a war!

Cybersecurity experts say these actions by Russian hacktivists appear to be opportunistic moves taking advantage of the ongoing conflict to grab headlines and potentially profit from DDoS attacks.

According to Mattias Wåhlén, a threat intelligence expert at cybersecurity firm Truesec AB, these incidents are an indication that Russia is allying with Hamas against Israel.

Learning from war..
Russian playbook exposed!

CYBERATTACKS BY NUMBERS:

2,194 incidents investigated by CERT-UA
1,148 critical or high-level incidents investigated and mitigated by CERT-UA

RUSSIAN TACTICS:

H1: Focus on disruptive attacks to suppress Ukrainian resilience

H2: Focus shift to
25% on destructive attacks, and
75% cyber espionage and data exfiltration.

Russia's Cyber Tactics: Lessons Learned 2022

State Service of Special Communications and Information Protection of Ukraine

TRUESEC

WAR

Destroy and conquer

ViaSat

14 Jan 2022 **WhisperGate**
Read more | ESET
Read more | Microsoft

23 Feb 2022 **HermeticWiper**
HermeticRansom
Read more | ESET

24 Feb 2022 **AcidRain**
Read more | SentinelOne

24 Feb 2022 **IsaacWiper**
Read more | ESET

1 Mar 2022 **DesertBlade**
Read more | Microsoft

~ 10 Mar 2022 **HermeticWiper**
Read more | Microsoft

14 Mar 2022 **CaddyWiper**
Read more | ESET

~ 17 Mar 2022 **DoubleZero**
Read more | CERT-UA

~ 17 Mar 2022 **DesertBlade**
Read more | Microsoft

~ 17 Mar 2022 **HermeticRansom**
Read more | Microsoft

~ 24 Mar 2022 **HermeticWiper**
HermeticRansom
Read more | Microsoft

1 Apr 2022 **ArguePatch**
CaddyWiper
Read more | ESET

8 Apr 2022 **ArguePatch**
CaddyWiper
ORCSHRED, SOLOSHRED, AWFULSHRED
(Industroyer 2 incident)
Read more | ESET
Read more | CERT-UA

~ 16 May 2022 **ArguePatch**
CaddyWiper
Read more | ESET

20 Jun 2022 **ArguePatch**
CaddyWiper
Read more | ESET

23 Jun 2022 **ArguePatch**
CaddyWiper
Read more | ESET

3 Oct 2022 **CaddyWiper**
Read more | ESET

~ 5 Oct 2022 **HermeticWiper**
Read more | ESET

11 Oct 2022 **Prestige faux ransomware**
Read more | ESET
Read more | Microsoft

11 Oct 2022 **NikoWiper**
Read more | ESET

~ 11 Nov 2022 **Somnia faux ransomware**
Read more | CERT-UA

21 Nov 2022 **RansomBoggs faux ransomware**
Read more | ESET

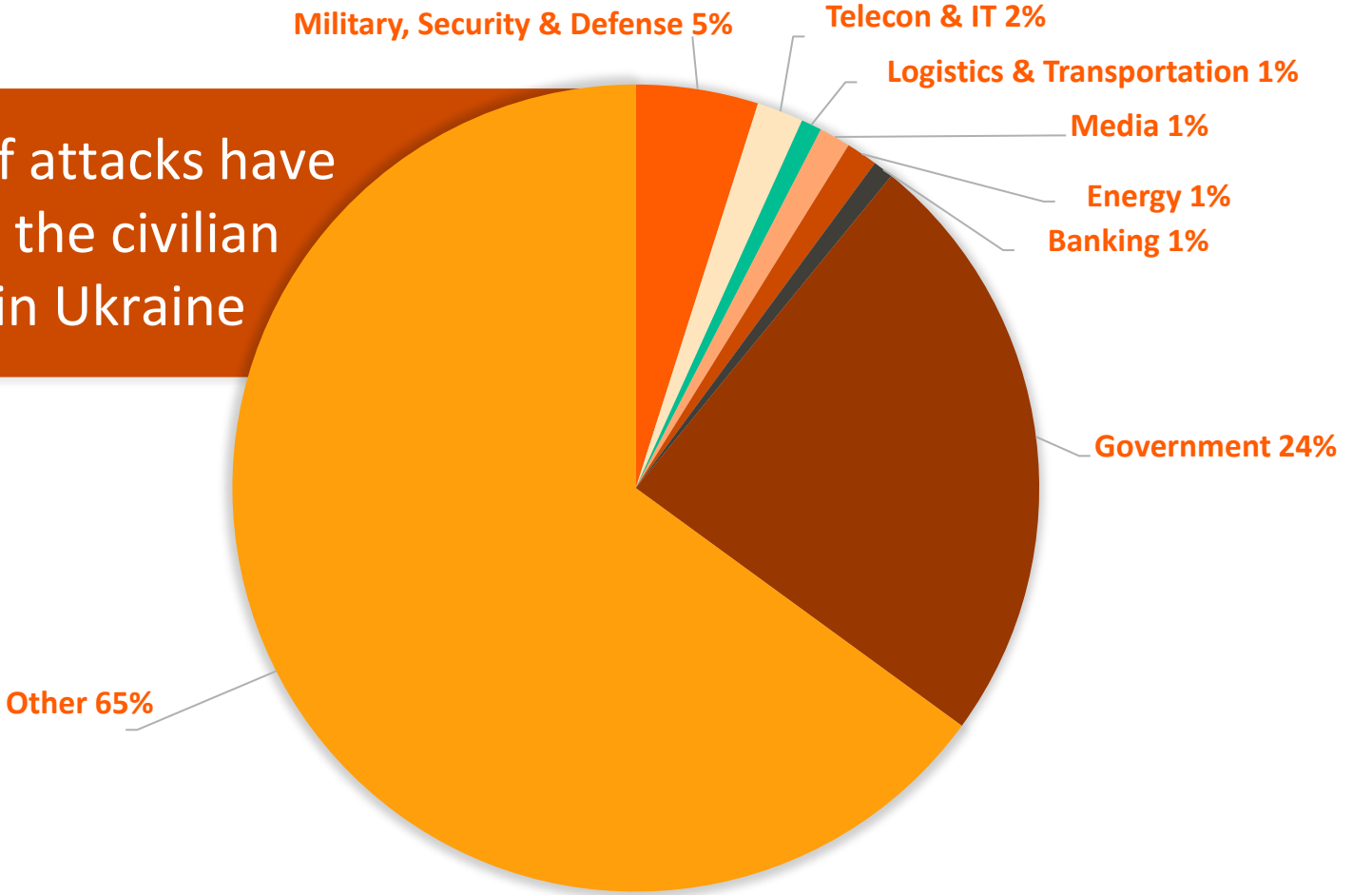
12 Jan 2023 **SDelete**

~ 17 Jan 2023 **CaddyWiper**
ZeroWipe
SDelete
AWFULSHRED
BidSwipe
Read more | CERT-UA

25 Jan 2023 **SwiftSlicer**
Read more | ESET

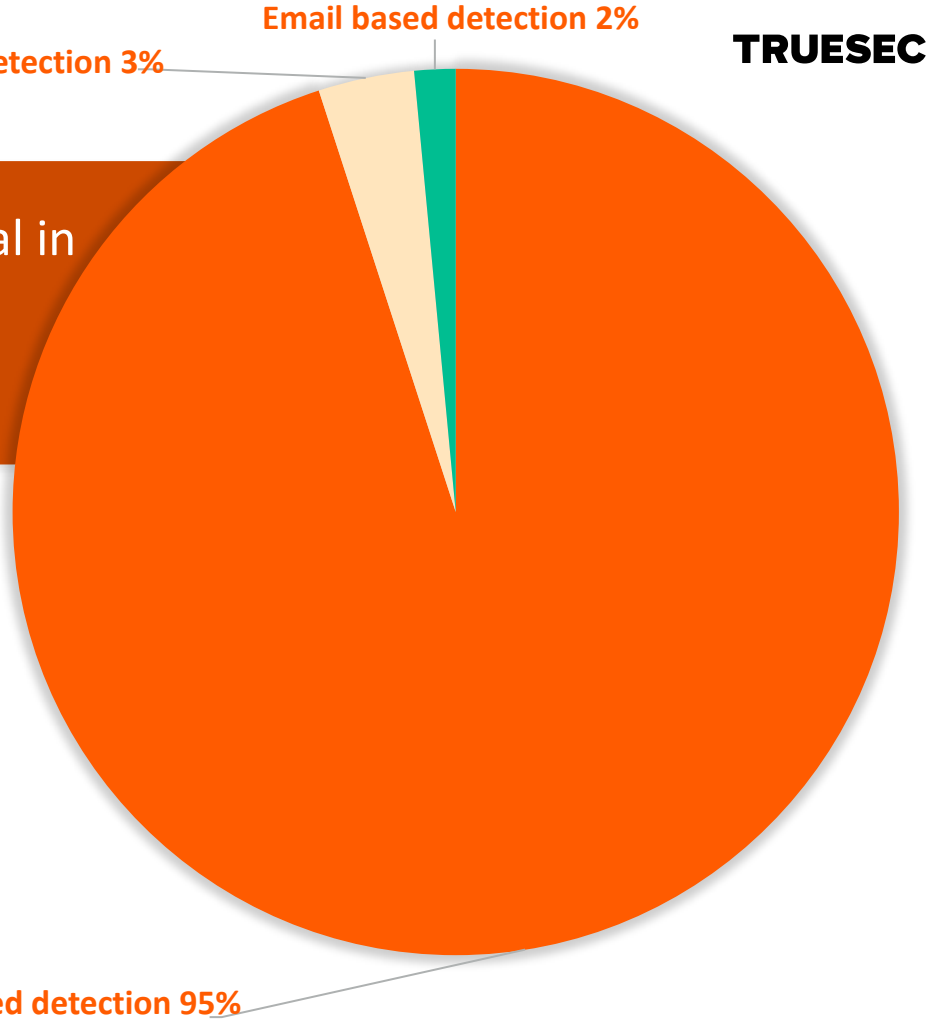
TRUESEC

The majority of attacks have been targeting the civilian infrastructure in Ukraine



TRUESEC

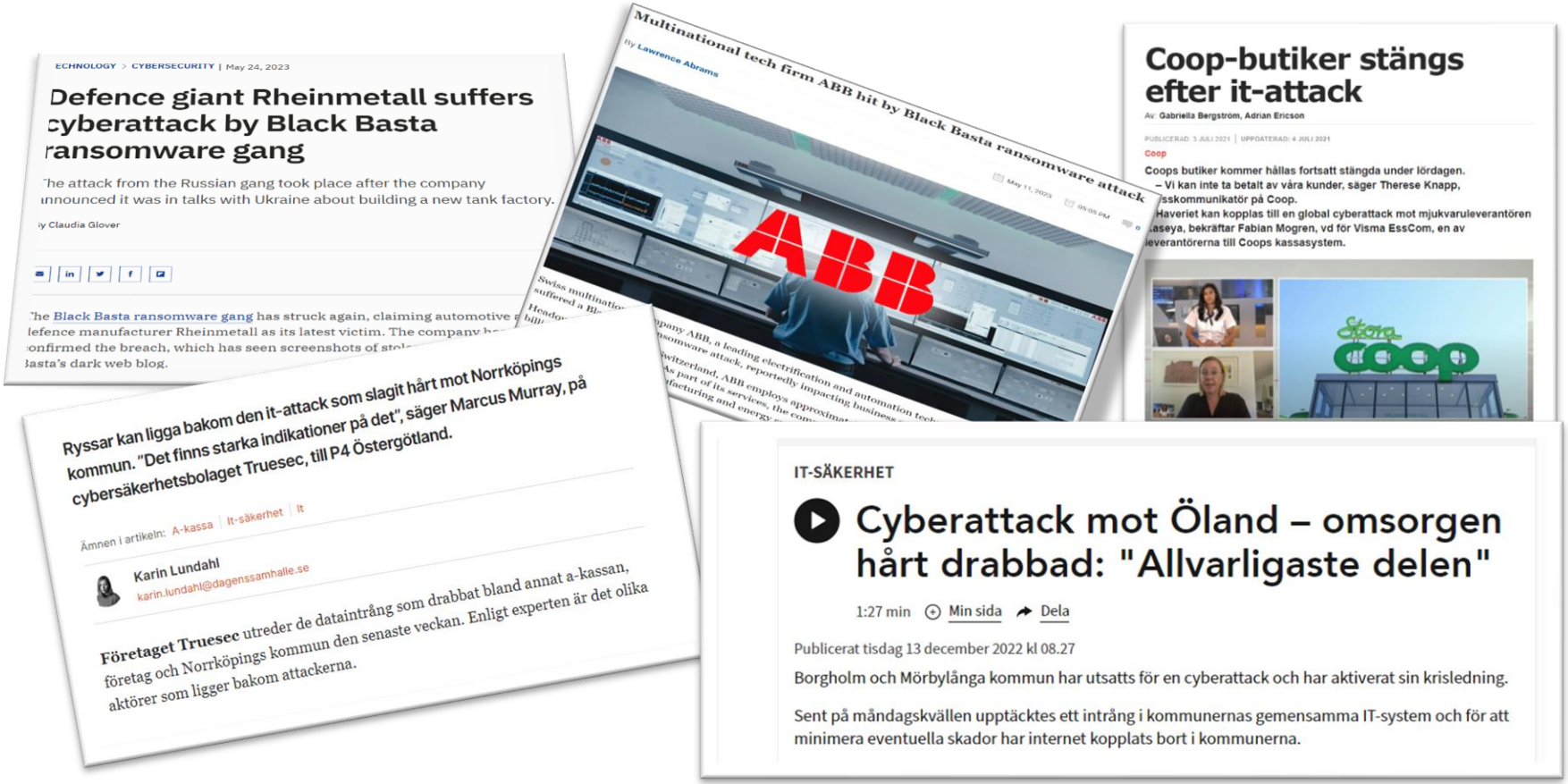
Endpoint detection is absolutely crucial in detection and mitigation of Russian cyberattacks at scale.



Ransomware

TRUESEC

The society is increasingly affected!



ECHNOLOGY > CYBERSECURITY | May 24, 2023

Defence giant Rheinmetall suffers cyberattack by Black Basta ransomware gang

The attack from the Russian gang took place after the company announced it was in talks with Ukraine about building a new tank factory.

By Claudia Glover

The Black Basta ransomware gang has struck again, claiming automotive s defence manufacturer Rheinmetall as its latest victim. The company h confirmed the breach, which has seen screenshots of sto Basta's dark web blog.

Multinational tech firm ABB hit by Black Basta ransomware attack

By Lawrence Abrams

Coop-butiker stängs efter it-attack

Av: Gabriella Bergström, Adrian Ericson

PUBLICERAD: 3 JULI 2021 | UPPDATERAD: 4 JULI 2021

Coop

Coops butiker kommer hållas fortsatt stängda under lördagen.

– Vi kan inte ta betalt av våra kunder, säger Therese Knapp, ...sskommunikatör på Coop.

...Haveriet kan kopplas till en global cyberattack mot mjukvaruleverantören ...aseya, bekräftar Fabian Mogren, vd för Visma EssCom, en av ...leverantörerna till Coops kassasystem.

Ryssar kan ligga bakom den it-attack som slagit hårt mot Norrköpings kommun. "Det finns starka indikationer på det", säger Marcus Murray, på cybersäkerhetsbolaget Truesec, till P4 Östergötland.

Ämnen i artikeln: A-kassa | It-säkerhet | It

Karin Lundahl
karin.lundahl@dagenssamhalle.se

Företaget Truesec utreder de dataintrång som drabbat bland annat a-kassan, företag och Norrköpings kommun den senaste veckan. Enligt experten är det olika aktörer som ligger bakom attackerna.

IT-SÄKERHET

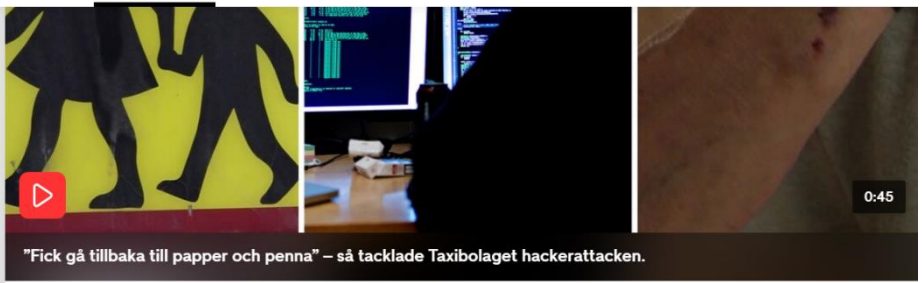
Cyberattack mot Öland – omsorgen hårt drabbad: "Allvarligaste delen"

1:27 min | Min sida | Dela

Publicerat tisdag 13 december 2022 kl 08.27

Borgholm och Mörbylånga kommun har utsatts för en cyberattack och har aktiverat sin krisledning.

Sent på måndagskvällen upptäcktes ett intrång i kommunernas gemensamma IT-system och för att minimera eventuella skador har internet kopplats bort i kommunerna.



”Fick gå tillbaka till papper och penna” – så tacklade Taxibolaget hackerattacken.

Hackarna slog ut barnens skolskjuts – ”Fick ta fram papper och penna”

Nästan hälften av Sveriges kommuner och regioner utsatta för it-attacker

UPPDATERAD: 26 MARS, 2023 PUBLICERAD: 26 MARS, 2023

Nästan hälften av Sveriges kommuner och regioner har utsatts för en eller flera misstänkta it-attacker det senaste året.

Det visar en enkät som TV4 Nyheterna gjort.

I veckan har bland annat skolskjutsar och trygghetslarm på flera håll i landet drabbats av störningar på grund av hackerattacker.

I veckan fick Taxi Trollhättan leta fram papper och penna igen när en hackerattack mot en leverantör släckte bokningssystemet.

– Vi ser varken bokningar eller kan skriva in nya bokningar. Vi kan inte heller se våra fordon, säger Mikael Hermansson, taxiföretagare.

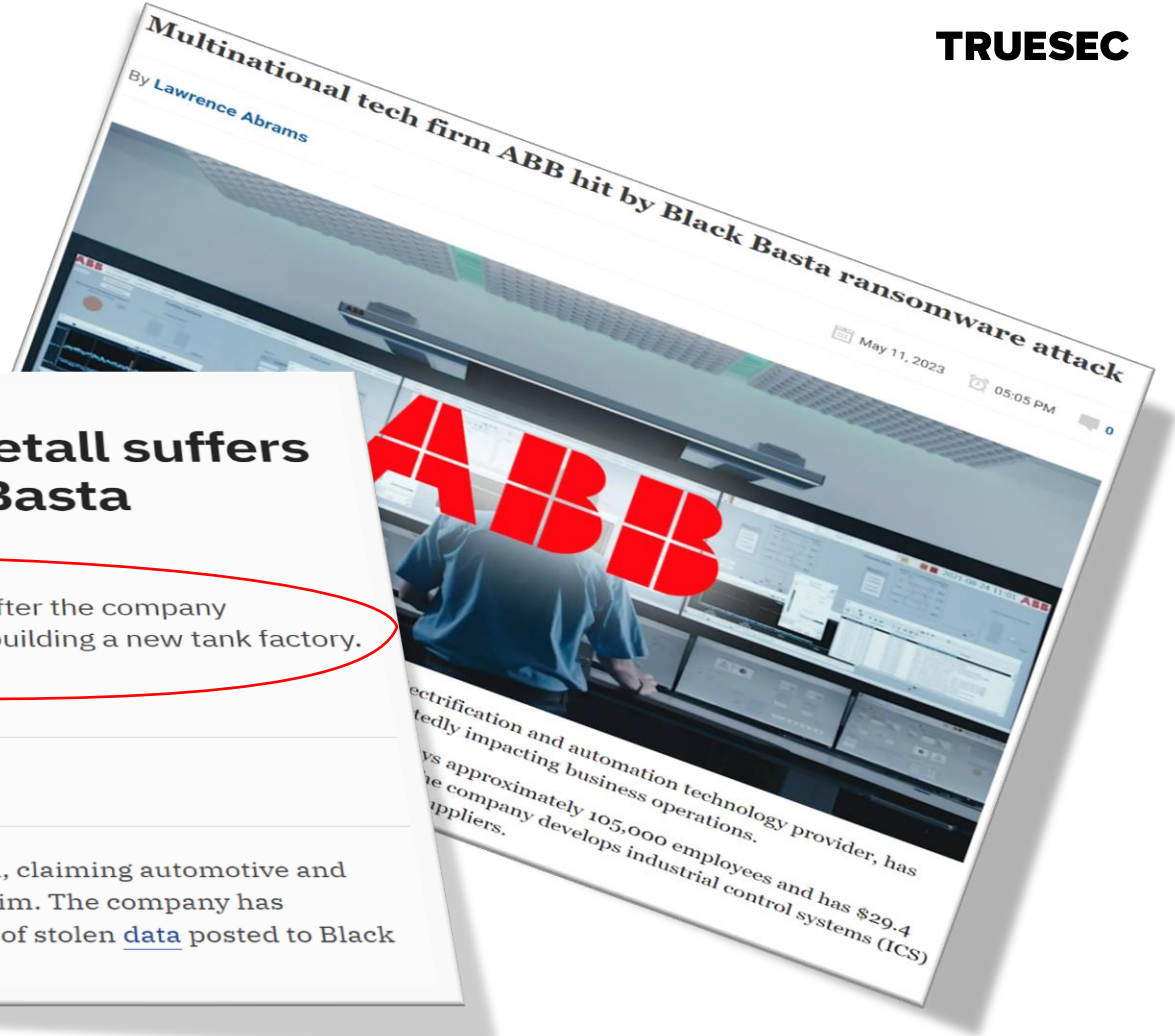
Ett annat angrepp slog i torsdags ut trygghetslarm på flera håll i landet.

Cybersäkerhetschefen: "Allvarligt"

När TV4 Nyheterna frågar Sveriges kommuner och regioner om misstänkta it-attacker det senaste året uppger närmare hälften, 44 procent, av de svarande att de utsatts.

TRUESEC

More often linked to geopolitics



Multinational tech firm ABB hit by Black Basta ransomware attack

By Lawrence Abrams

May 11, 2023 05:05 PM 0

ectrification and automation technology provider, has tedly impacting business operations.

ys approximately 105,000 employees and has $29.4 he company develops industrial control systems (ICS) ppliers.

TECHNOLOGY > CYBERSECURITY | May 24, 2023

Defence giant Rheinmetall suffers cyberattack by Black Basta ransomware gang

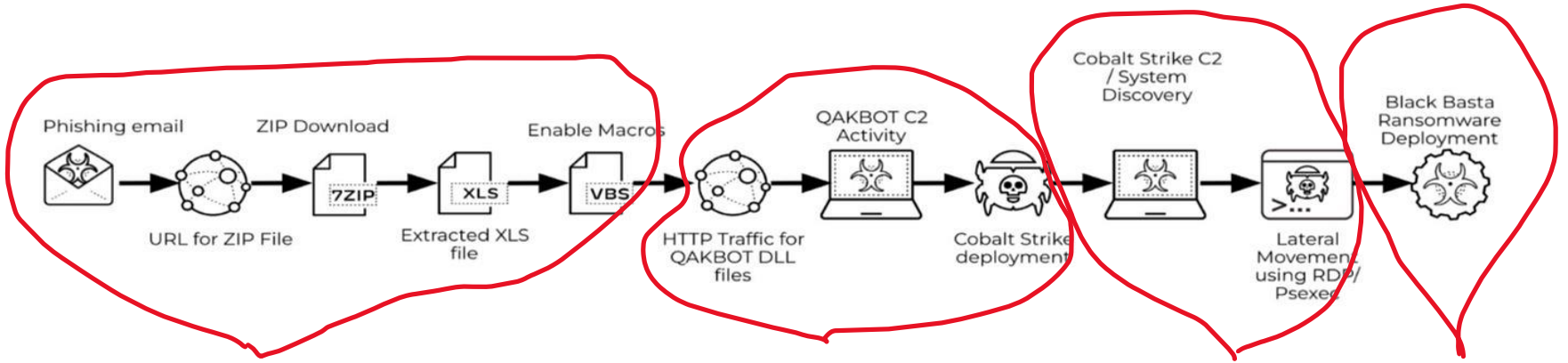
The attack from the Russian gang took place after the company announced it was in talks with Ukraine about building a new tank factory.

By Claudia Glover

The Black Basta ransomware gang has struck again, claiming automotive and defence manufacturer Rheinmetall as its latest victim. The company has confirmed the breach, which has seen screenshots of stolen data posted to Black Basta's dark web blog.

TRUESEC

Typical Black Basta attack

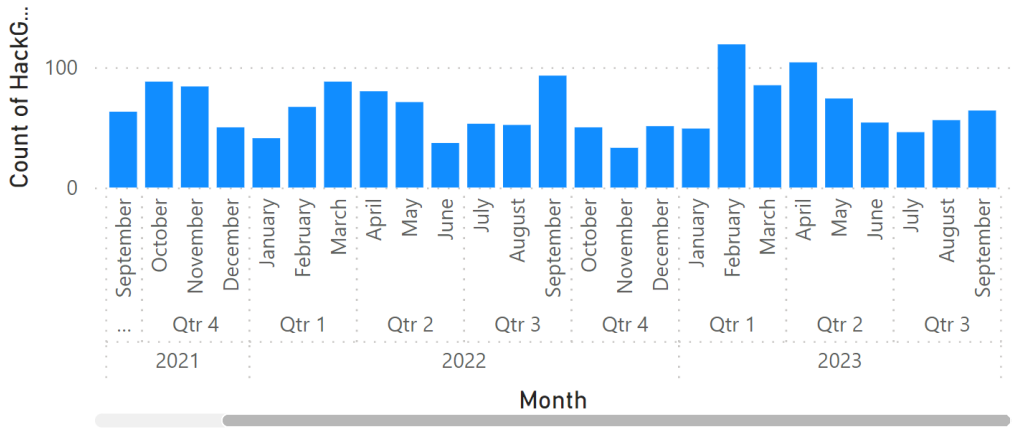



Optislim
OptiVite

HackGroupName

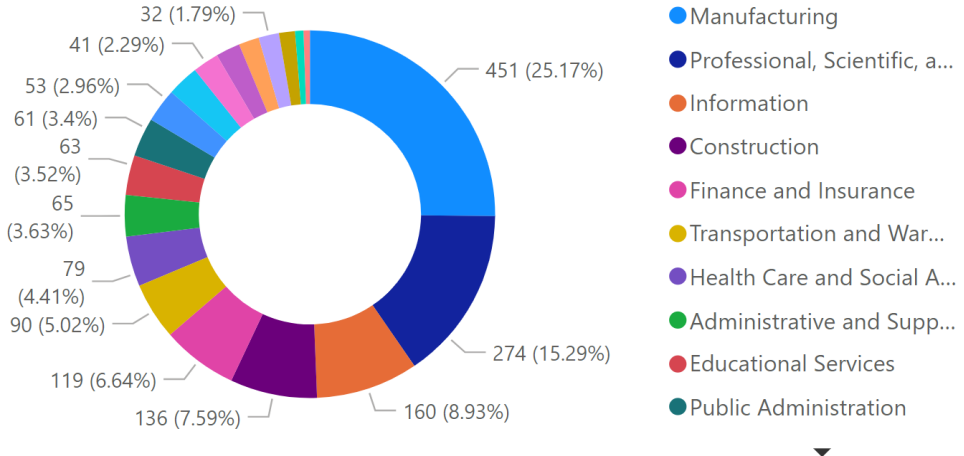
- [ ] kelvinsecurity
- [ ] lapsus
- [ ] Leakcentral12
- [ ] Legionnare
- [x] LOCKBIT
- [x] lockbit2
- [x] lockbit3
- [ ] lockdataauction
- [ ] lorenz
- [ ] LulzSec
- [ ] lv
- [ ] lv2
- [ ] malas
- [ ] malaslocker
- [ ] malaslocker_defaulters
- [ ] mallox
- [ ] marketo
- [ ] maze
- [ ] medusa
- [ ] medusalocker

Count of HackGroupName by Year, Quarter and Month



TRUESEC

Count of HackGroupName by NACISParentIndustryName



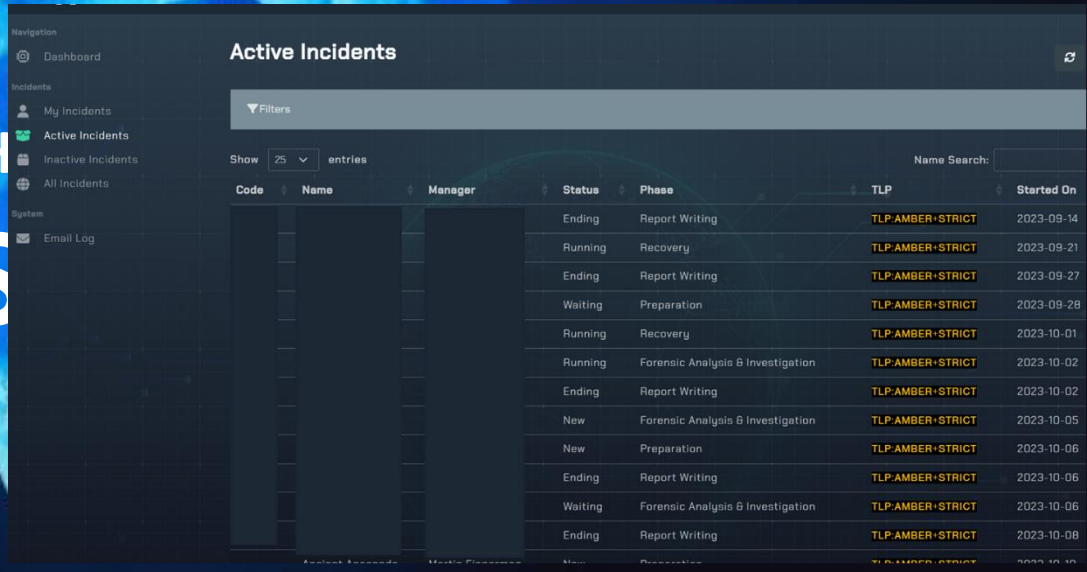
TRUESEC

@Truesec last year:
160 complex IR engagements
30.000 hours of IR

@Truesec this year:
160+ IR engagements to date

H

RANS



mitre-attack | mitre-mobile-attack | mitre-pre-attack

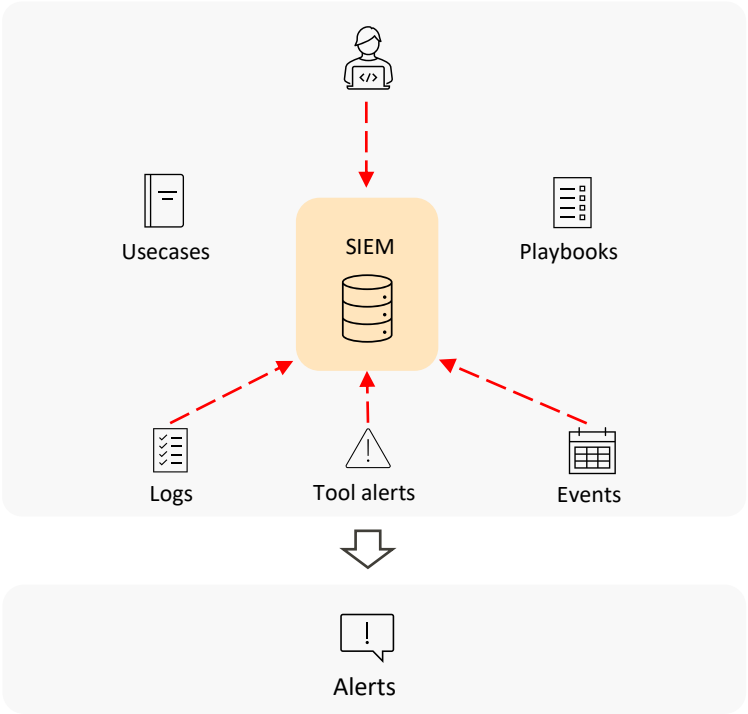
0 26 Show all

Reconnaissance	Resource development	Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Command and control	Exfiltration	Impact
Active Scanning	Acquire Access	Valid Accounts	Scheduled Task	Valid Accounts	Valid Accounts	Valid Accounts	LSASS Memory	Network Service Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Remote Access Software	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Scanning IP Blocks	Acquire Infrastructure	External Remote Services	PowerShell	External Remote Services	Scheduled Task	Disable or Modify Tools	Credentials from Web Browsers	Domain Account	Lateral Tool Transfer	Data from Local System	Commonly Used Port	Exfiltration Over Unencrypted Non-C2 Protocol	Data Destruction
Business Relationships	Botnet	Phishing	Service Execution	Scheduled Task	Domain Accounts	Domain Accounts	NTDS	Remote System Discovery	Remote Desktop Protocol	Local Data Staging	DNS	Exfiltration to Cloud Storage	Inhibit System Recovery
CDNs	Botnet	Exploit Public-Facing Application	System Services	Create Account	Exploitation for Privilege Escalation	Cloud Accounts	OS Credential Dumping	Debugger Evasion	Replication Through Removable Media	ARP Cache Poisoning	Non-Standard Encoding	Exfiltration Over Web Service	Defacement
Client Configurations	Cloud Accounts	Domain Accounts	Python	Domain Accounts	Cloud Accounts	Local Accounts	Brute Force	Local Account	SMB/Windows Admin Shares	Adversary-in-the-Middle	Non-Standard Port	Transfer Data to Cloud Account	Disk Structure Wipe
Code Repositories	Cloud Accounts	Cloud Accounts	Shared Modules	Cloud Accounts	Local Accounts	Indicator Removal	Kerberoasting	Network Service Scanning	Windows Remote Management	Archive Collected Data	Proxy	Automated Exfiltration	Disk Structure Wipe
Credentials	Code Signing Certificates	Local Accounts	Visual Basic	Domain Account	Registry Run Keys / Startup Folder	Match Legitimate Name or Location	/etc/passwd and /etc/shadow	Network Share Discovery	Application Access Token	Archive via Custom Method	Web Protocols	Data Compressed	Internal Defacement
DNS	Code Signing Certificates	Default Accounts	Windows Command Shell	Local Accounts	Bypass User Account Control	Bypass User Account Control	ARP Cache Poisoning	Account Discovery	Application Access Token	Archive via Library	Application Layer Protocol	Data Encrypted	Network Denial of Service
DNS/Passive DNS	Compromise Accounts	Replication Through Removable Media	Windows Management Instrumentation	Web Shell	Default Accounts	Clear Linux or Mac System Logs	AS-REP Roasting	Application Window Discovery	Application Deployment Software	Archive via Utility	Asymmetric Cryptography	Data Transfer Size Limits	Service Stop
Determine Physical Locations	Compromise Infrastructure	Spearphishing Link	AppleScript	Local Account	Dylib Hijacking	Clear Windows Event Logs	Adversary-in-the-Middle	Browser Bookmark Discovery	Cloud Services	Audio Capture	Bidirectional Communication	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	System Shutdown/Reboot
Digital Certificates	DNS Server	Spearphishing Link	AppleScript	Registry Run Keys / Startup Folder	Dynamic Linker Hijacking	Debugger Evasion	Bash History	Browser Information	Component Object Model	Automated Collection	Communication Through	Exfiltration Over Bluetooth	Account Access Removal
Domain Properties	DNS Server	Compromise Hardware Supply Chain	At (Linux)	Default Accounts	Image File Execution Options Injection	Default Accounts						Channel	Flood
Email Addresses	Develop Capabilities	Compromise Software Dependencies and	At (Windows)	Device Registration	RC Scripts	Disable Windows Event Logging	Cached Domain Credentials	Cloud Groups				Exfiltration Over Other Network Medium	Application or System Exploitation

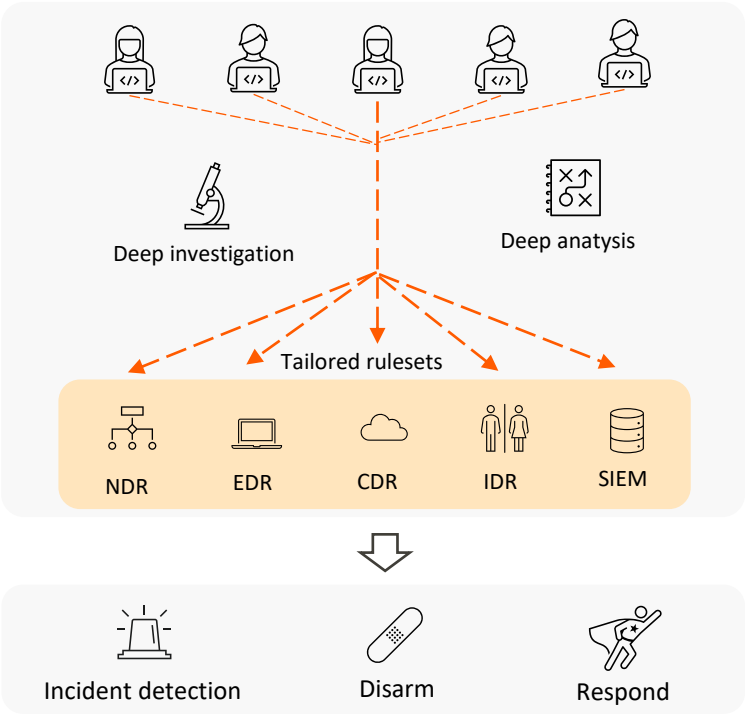
Our 26 latest ransomware incidents - Mitre Att&ck

TRUESEC

GENERIC **SIEM CENTRIC** DETECTION

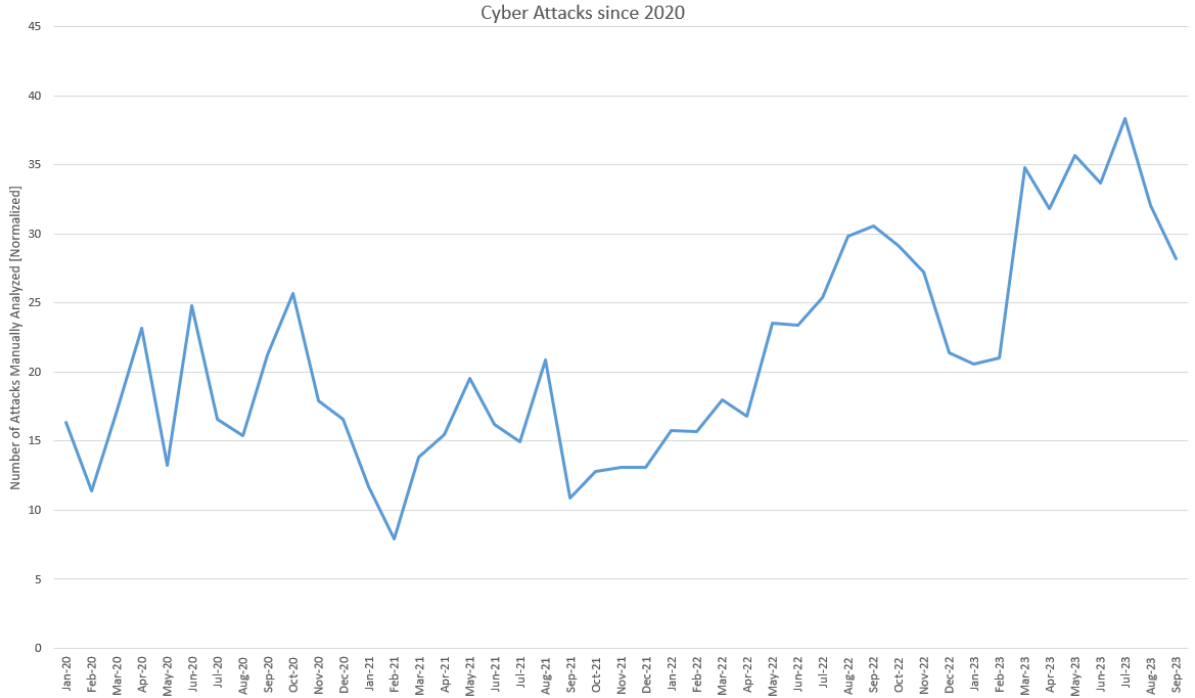


TRUESEC **XDR CENTRIC** DETECTION



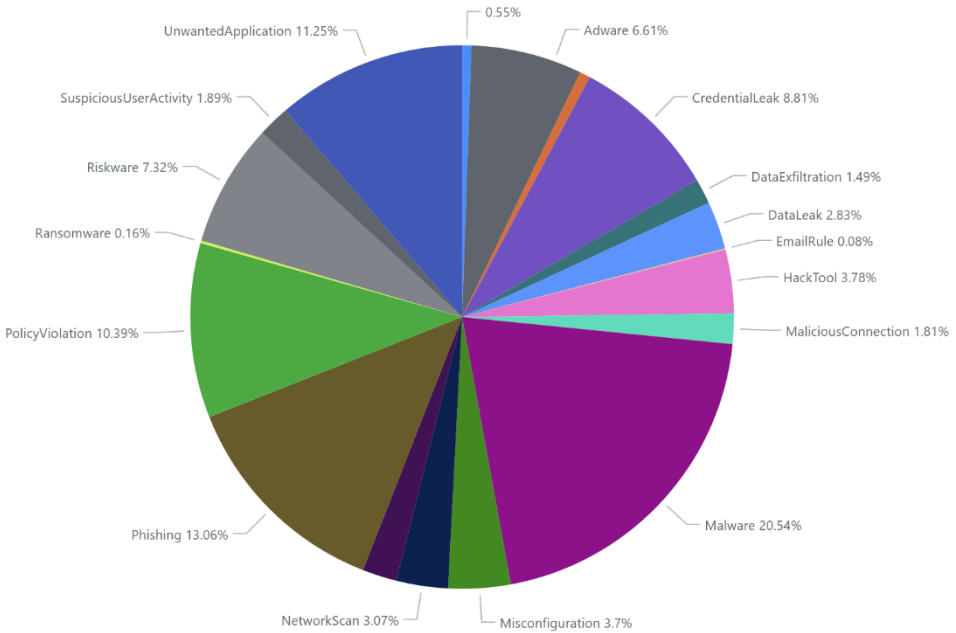
TRUESEC

Calming from high levels



TRUESEC

1100 cyber attacks disarmed in September



TRUESEC

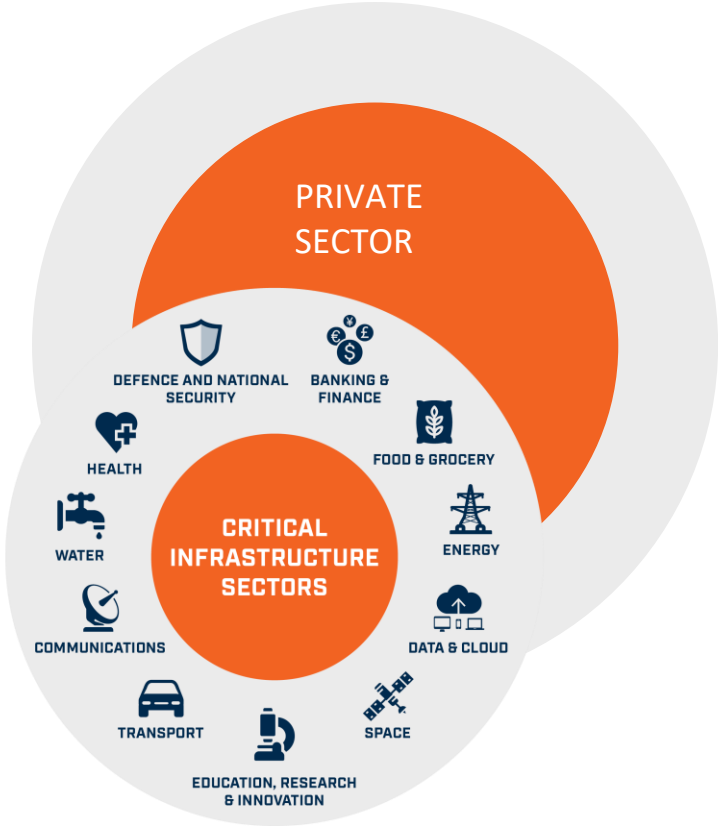
Threat actors in the Nordics..

Russian state-actors

Pro-Russian cyber activists

Chinese state-actors

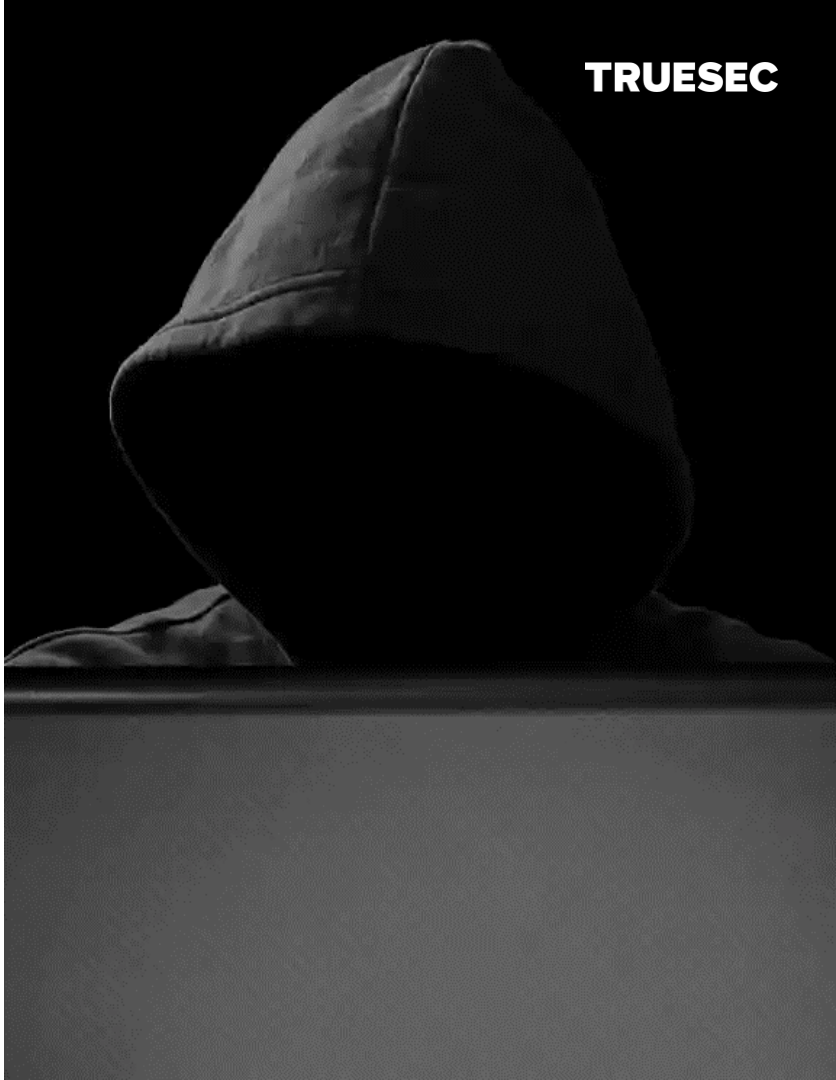
Cyber criminals (Russia etc.)
State-actors (North korea, Iran etc.)



Will it get worse?

Sanctions drive cybercrime

- Western companies are leaving Russia
- Russian economy is taking a big hit
- Unemployed IT-pros need to support their families
- Cybercrime is flourishing
- Russia is a global leader in RaaS



February 10, 13:35, updated February 10, 13:46

Khinshtein said that hackers acting in the interests of the Russian Federation should be released from responsibility

Currently, the creation, use and distribution of malicious computer programs faces imprisonment for up to seven years.

MOSCOW, February 10. /TASS/. The so-called white hackers acting in the interests of the Russian Federation on its territory and abroad should be exempt from liability, this issue is planned to be worked out. This was stated to journalists by the head of the State Duma Committee on Information Policy Alexander Khinshtein on Friday.

"We are talking about generally working out an exemption from liability for those persons who act in the interests of the Russian Federation in the field of computer information both in the territory of our country and abroad. We will talk in more detail when it receives some clear wording," he said, answering a question from TASS following a meeting of the committee at which issues of cybersecurity of the Russian Federation were discussed.

According to the parliamentarian, it is necessary to think about legislative consolidation of the rights of hackers acting in the interests of the state. "I, for one, am firmly convinced that it is necessary to use any resources to effectively fight the enemy. If today we are attacked by such centers, then Russia should have the opportunity for an adequate response," he said.

Currently, the creation, use and distribution of malicious computer programs faces imprisonment for up to seven years (Article 273 of the Criminal Code of the Russian Federation).

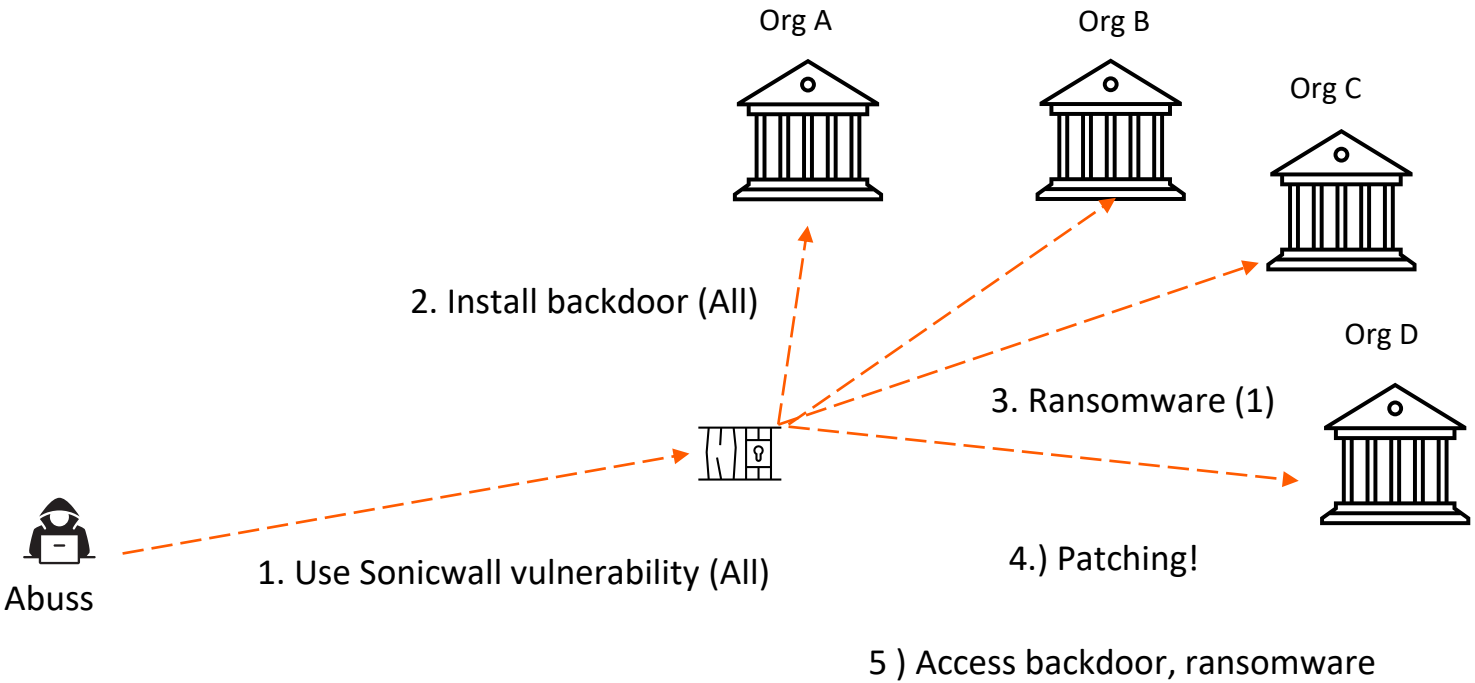
Tags: Russia Khinshtein, Alexander Evseevich

Piracy

- From the medieval time to 1850 authorization letters to commit piracy for personal gain was hander out by governments and kings.

- Piracy was internationally agreed to be prohibited as part of the Paris declaration 1856. As part of the peace treaty after the Crimean war

Trend: Stealth - access all before impacting one.



(Also Cl0p-MOVEit)

TRUESEC

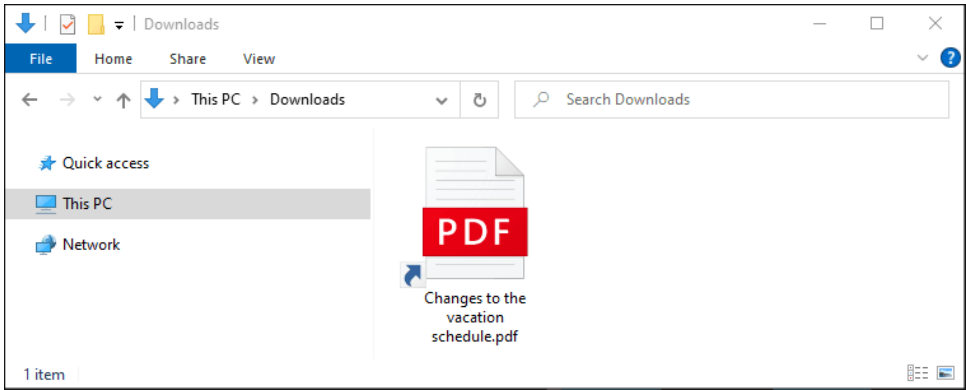
Blog 2023-09-06

DarkGate Loader Malware Delivered via Microsoft Teams

Malspam campaigns involving DarkGate Loader have been on the rise since its author started advertising it as a Malware-as-a-Service offering on popular cybercrime forums in June 2023. Until now DarkGate Loader was seen delivered via traditional email malspam campaigns similar to those of Emotet. In August an operator started using Microsoft Teams to deliver the malware via HR-themed social engineering chat messages.

Title: DarkGate Loader delivered via Teams - Truesec

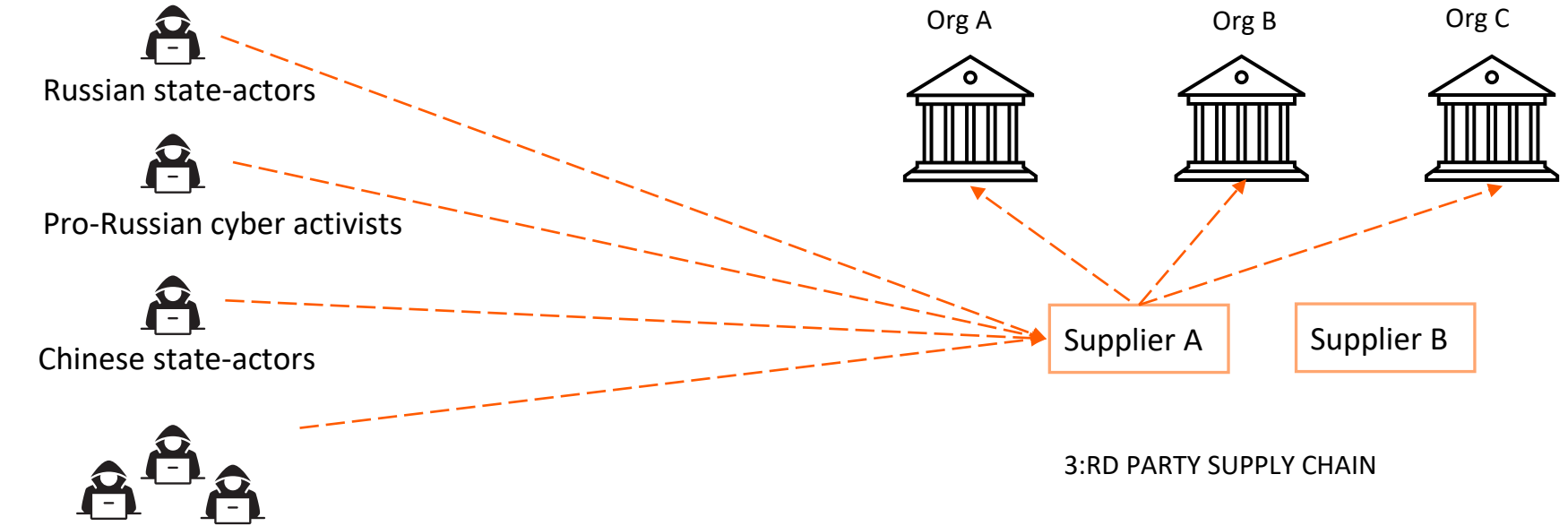
5 min read
Jakob Nordenlund



Supply-chain threats

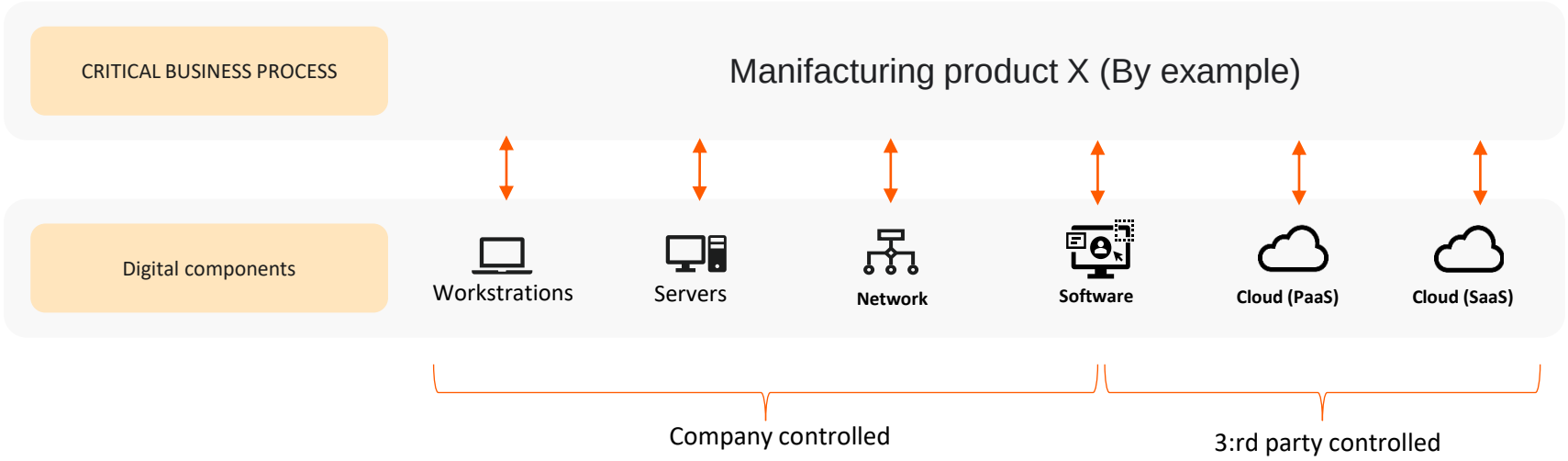
Trend: Low investments – high impact!

Target suppliers with sometimes lower security, but with big impact



TRUESEC

Each critical business process is depending on various digital components



Information om Visma Recruits driftstörning

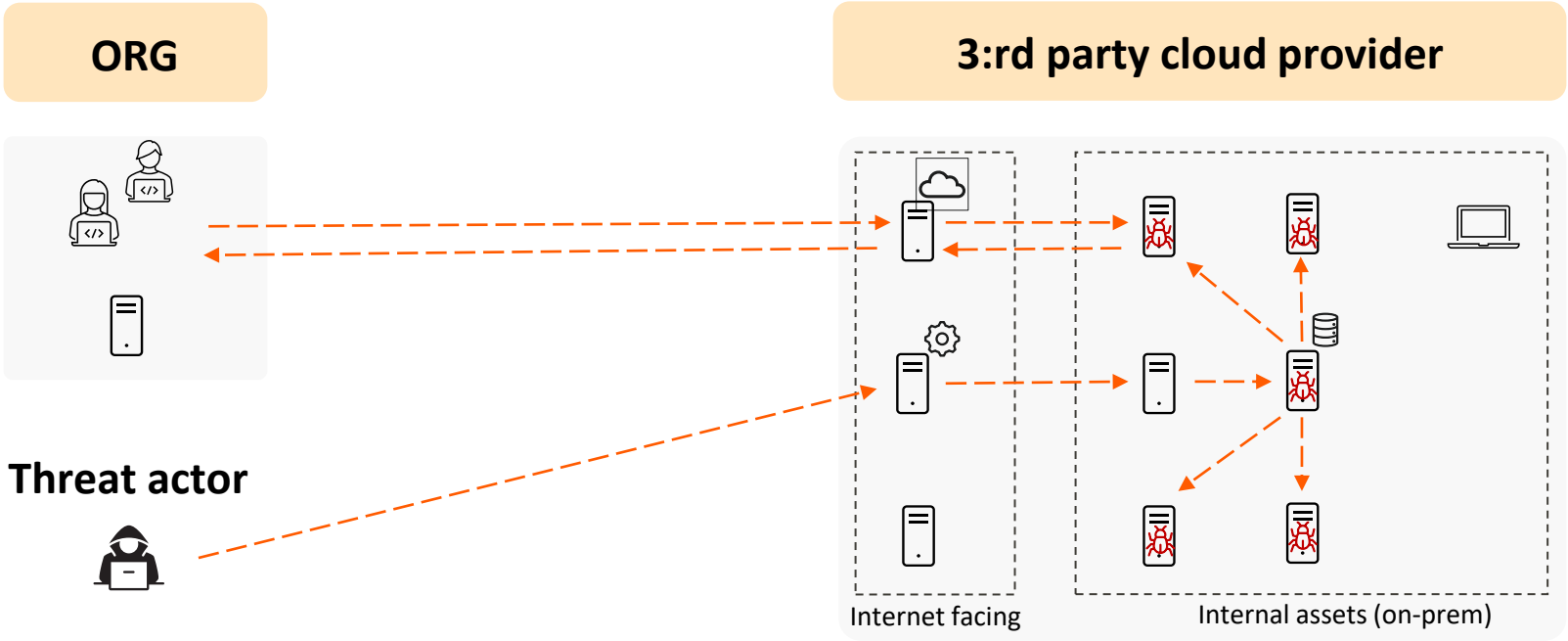
TRUESEC

Under perioden 24/4-1/5 gick det inte att söka jobb hos Uppvidinge kommun, då rekryteringssystemet vi använder utsatts för en cyberattack.

Visma Recurit och Offentliga jobb är ett verksamhetssystem för bland annat rekrytering som Uppvidinge kommun och andra kommuner använder. Driftleverantören till Visma Recruit utsattes för en cyberattack och stängde ner systemet den 24 april 2023.

TRUESEC

3:rd party Risk dependencies [Example 1]



Should we only worry about ransomware?

Espionage

Putin orders FSB to go after western digital assets

As before, one of the priorities of the Foreign Intelligence Service is to assist in the industrial and technological development of our country, in strengthening its defense potential.

..the Chinese is however leaders in espionage

TRUESEC

Article 7
All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of.

Article 10
As necessary for their work, national intelligence work institutions are to use the necessary means, tactics, and channels to carry out intelligence efforts, domestically and abroad.

Truesec skyddar svenska kommuner, välkommen att kontakta mig direkt!

TRUESEC

Marcus.murray@truesec.com

marcusmurrayse

0709-18 30 01

Marcus Murray

Founder of Truesec Group | Protecting the society, governments & organizations against cyber threats | Threat Intelligence | Defense | Offense | Winner of Grand Security Award 2023 | No 1 most influential in Tech 2023

Stockholm, Stockholm, Sverige

15,432 followers · 500+ connections

Advice

Insight 1
Build capabilities in the right order!

TRUESEC

What should be a priority?

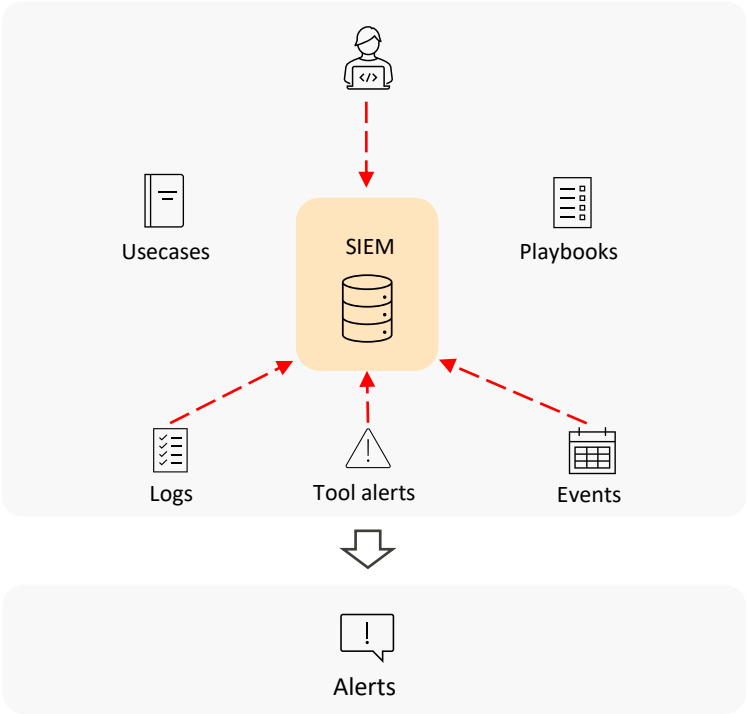
	Capability	Description
4	Identify	What processes and assets need protection?
3	Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
1	Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
2	Respond	Develop techniques to contain the impacts of cybersecurity events
3	Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

Insight 2
Optimize your breach detection

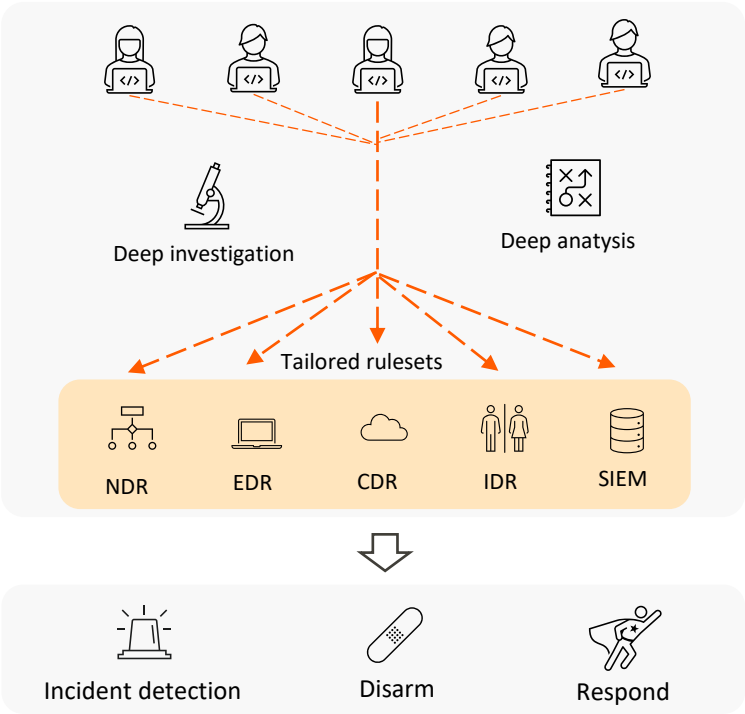
(Many organizations only have an “alert flooding service”)

TRUESEC

SIEM CENTRIC DETECTION



XDR CENTRIC DETECTION



TRUESEC

SIEM CENTRIC DETECTION

Multi-source collect all approach

Multi-source log/event/alert collection and analysis based on enterprise-wide collection from assets and security tooling

Threat Identification

Brings visibility by analysing logs/event/alert based on policy-based usecased and playbooks.

People & process

Normalized rules in one-stop shop solution, well-defined responsibilities, highly scalable – minimize human analysis

Output-Centric

Security alerting based on agreed poliys **and compliacy.**
Focusing on logging everything. Limited capabilities to respond.

XDR CENTRIC DETECTION

Tailored Incident detection approach

Asset-specific XDR tooling to detect suspicious threat actor activities (TAA) in mission-critical asset types

Threat Detection & Response

Designed detect sophisticated threats and to enable rapid detection and response with containment to minimize impact

People & process

Operate directly in XDR tooling to optimize capability.
Wide rules to catch suspicions to optimize detection.
Deep analysis & investigations to deliver higher value

Outcome-Centric

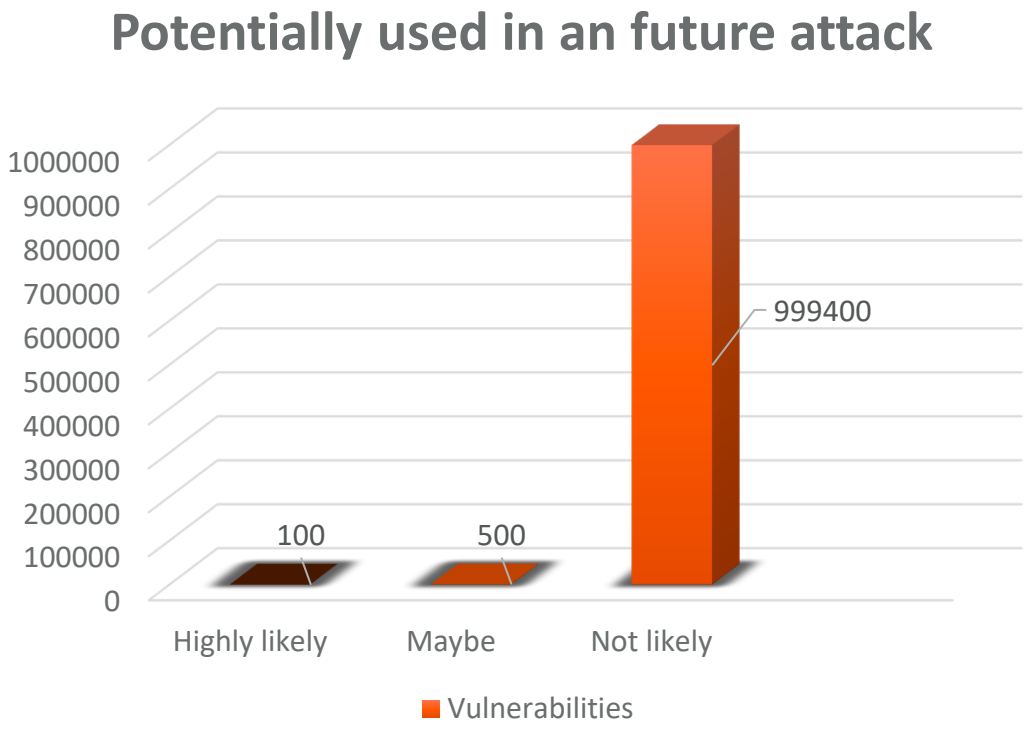
Prevent cyber incidents by actionable detection and response to confirmed threats – **Protect business from negative impact**

Insight 3
Focus on the right vulnerabilities!

(Many organizations only have huge backlog)

TRUESEC

Focus on the right vulnerabilities!



TRUESEC

Know thy enemy

Incident detection

External TI

IR engagements

Vulnerability Intelligence

Identify vulnerabilities

Vulnerability Scanning

Hunting/Bug bounty
Pentest/Redteam
Code analysis

Posture management

Risk of being exploited in future attacks?

Contextualize, Analyze and prioritize

Practical impact?

Exposure?

Prioritized  Vulnerabilities

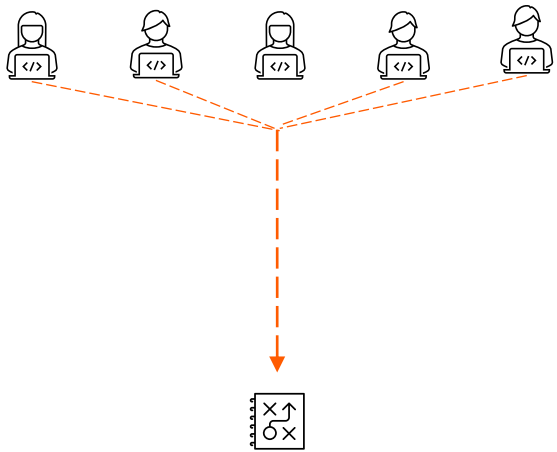
Mitigation and IImprovements

Insight 4

Use specialists for IR from the start

TRUESEC

Use specialists for IR from the start



Thank you!

TRUESEC

Marcus.murray@truesec.com

I provide cyber security advisory, insights and capability. Focus on government bodies, boards and C-level executives

Marcus Murray

Founder of Truesec Group | Protecting the society, governments & organizations against cyber threats | Threat Intelligence | Defense | Offense | Winner of Grand Security Award 2023 | No 1 most influential in Tech 2023

Stockholm, Stockholm, Sverige

15,432 followers · 500+ connections