Velkommen til InfoSec

Kim P. Pedersen

Disclaimer

- Oplysninger, der gives i denne præsentation, er kun til uddannelsesmæssige formål.
- Jeg er ikke ansvarlig for direkte eller indirekte skader forårsaget af brugen af informationer fra denne præsentation.
- Denne præsentation er relateret til computersikkerhed og ikke handlinger der fremmer hacking/cracking/softwarepirateri.
- Ordet "Hack" eller "Hacking", der bruges i denne præsentation, skal betragtes som henholdsvis "Etisk hack" eller "Etisk hacking".
- With great powers comes great responsibility!

$whoami

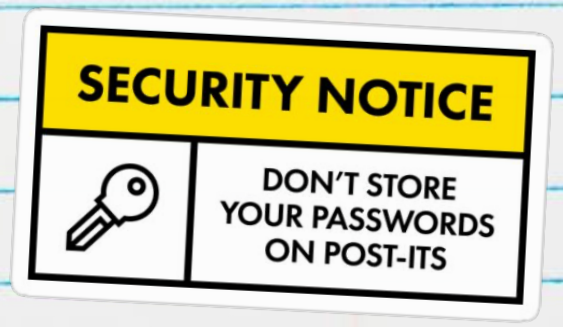
/in/kimppedersen/

@KimHot

KPP@dubex.dk

Kim P. Pedersen

Junior Cyber Security Analyst – Dubex



Kim P. Pedersen

De kedelige facts:

- 36 år
- Greve/Hundige
- Single og ugift
- Elsker sauna

Erhvervserfaring:

- Aviser -> Dørmand
- Over 10 år i sikkerhedsbranchen
- Vagt/Vagtassistent i Securitas
- Junior Cyber Security Analyst i Dubex

Udannelse:

- Datamatiker
- PBA IT Sikkerhed

Certificeringer:

- TryHackMe
- Udemy
- LinkedIn Learning

Også var der en gang jeg lavede musik...

The only place success comes before hard work is in the dictionary.

-Vince Lombardi

Det hele startede her...

SCHOOL HACKS
BY STUDENTS 4 STUDENTS

Security-Tuesday
08-10-2019

cphbusiness
COPENHAGEN BUSINESS ACADEMY


WHO ARE YOU?
NOBODY CARES!
HACKERMAN

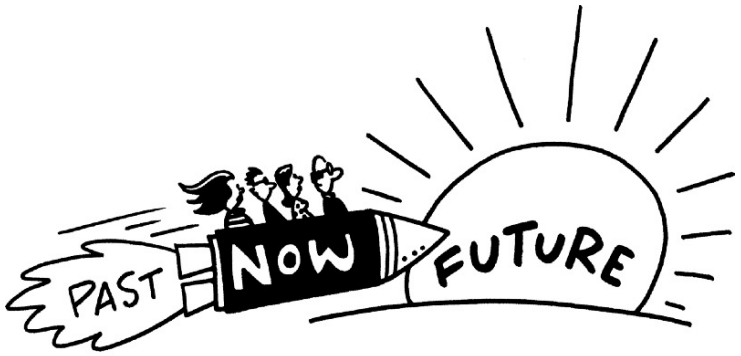

START
HERE!

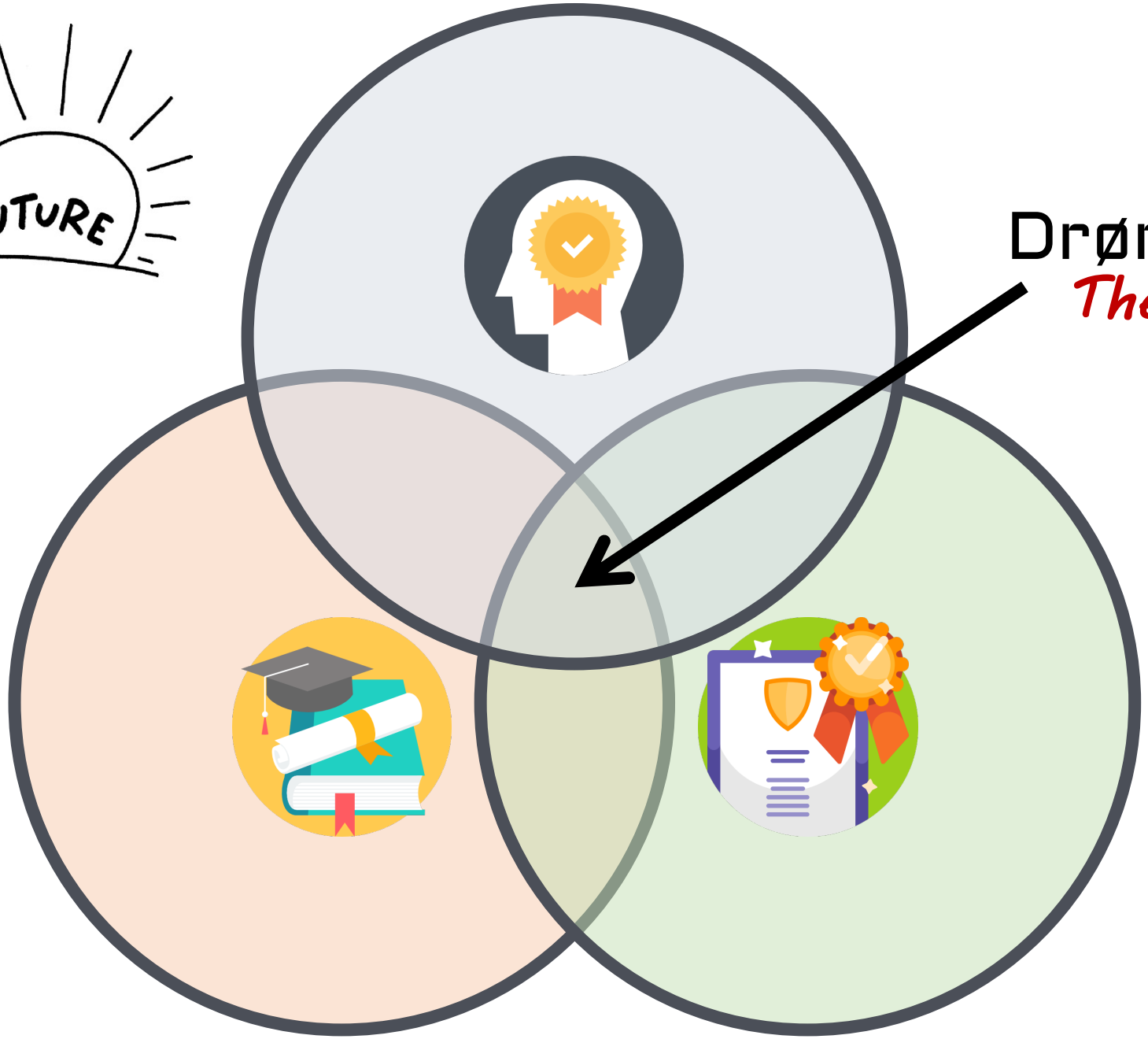
Certifikationer vs. Uddannelse vs. Erfaring

- Erfaring er gratis,
  men der er ingen hjælp

- Certifikationer koster penge

- Uddannelse koster tid





Drømmejobbet

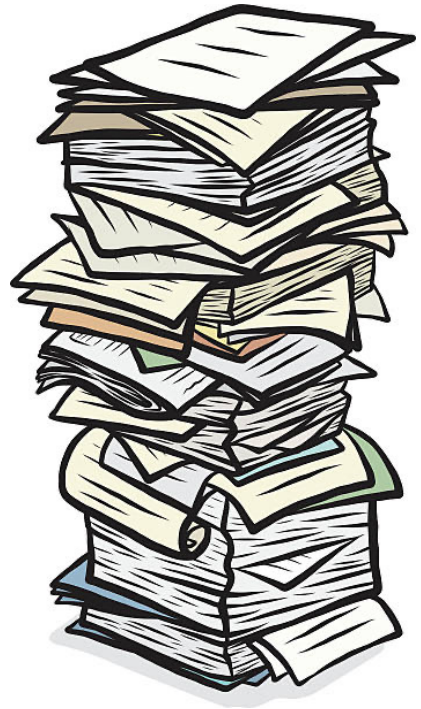
The sweet spot

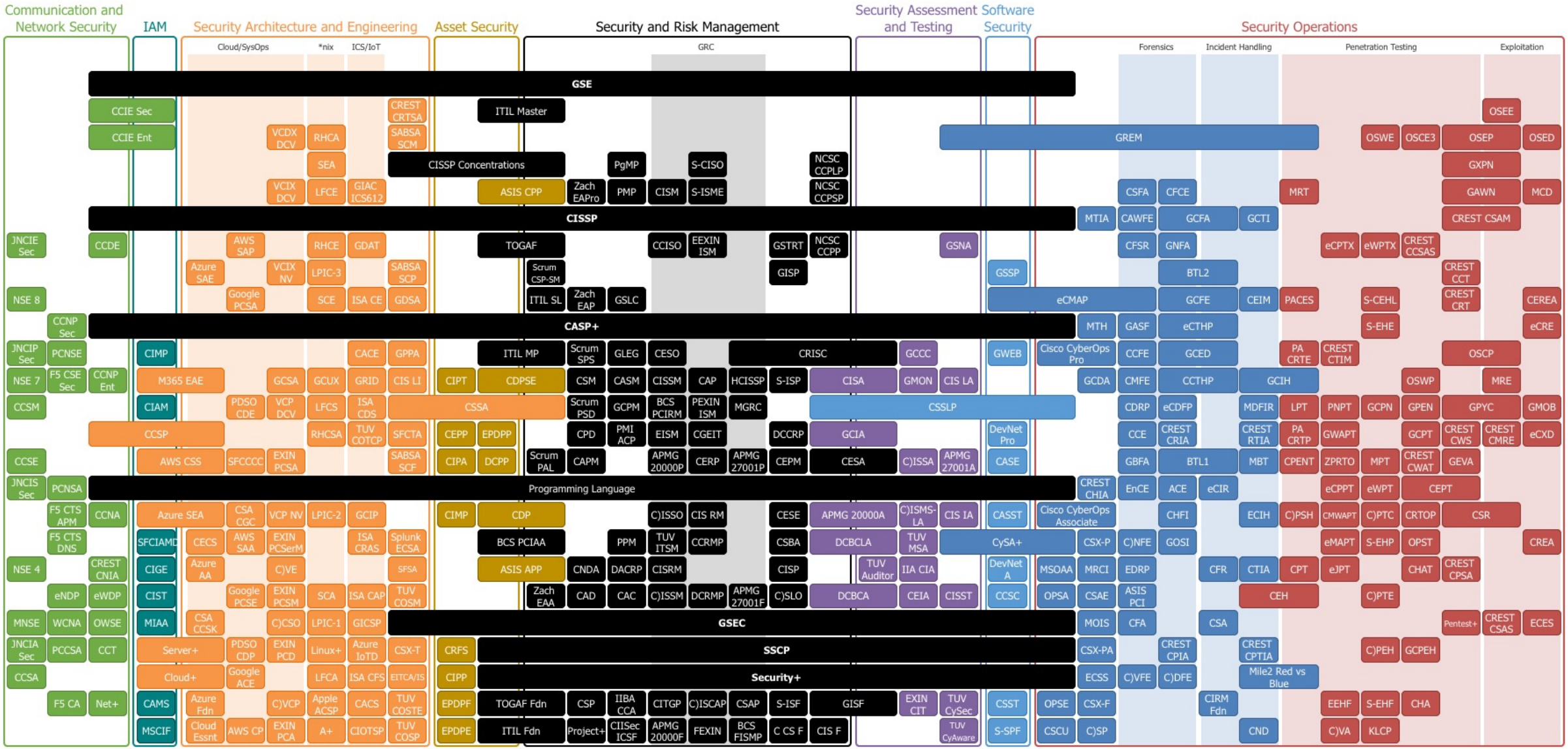
Jeg valgte (også) uddanelsen…

- Jeg er uddannet datamatiker – men koder stortset aldrig mere
  - Det er dog brugbart i forhold til fejlsøgning eller hvis et open-source værktøj er i stykker
  - Bruger det dog mest til at automatisere ting fordi jeg er doven!

Det jeg har lært på min PBA er:

- At skrive rapporter og dokumentation – Hvilket er det vigtigste.
  - Kunden betaler ikke ikke for opgaven (f.eks. Pentesten), men for rapporten.
  - Ingen kunder nøjes med en løst opgave (f.eks. Incedent Response), de betaler for rapporten eller dokumentaionen.



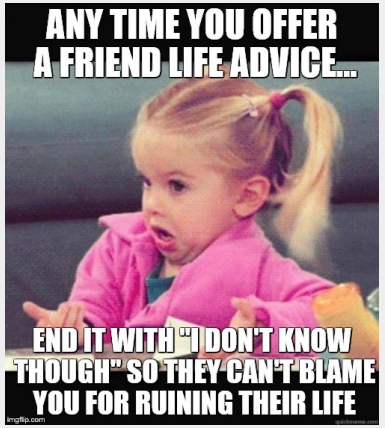


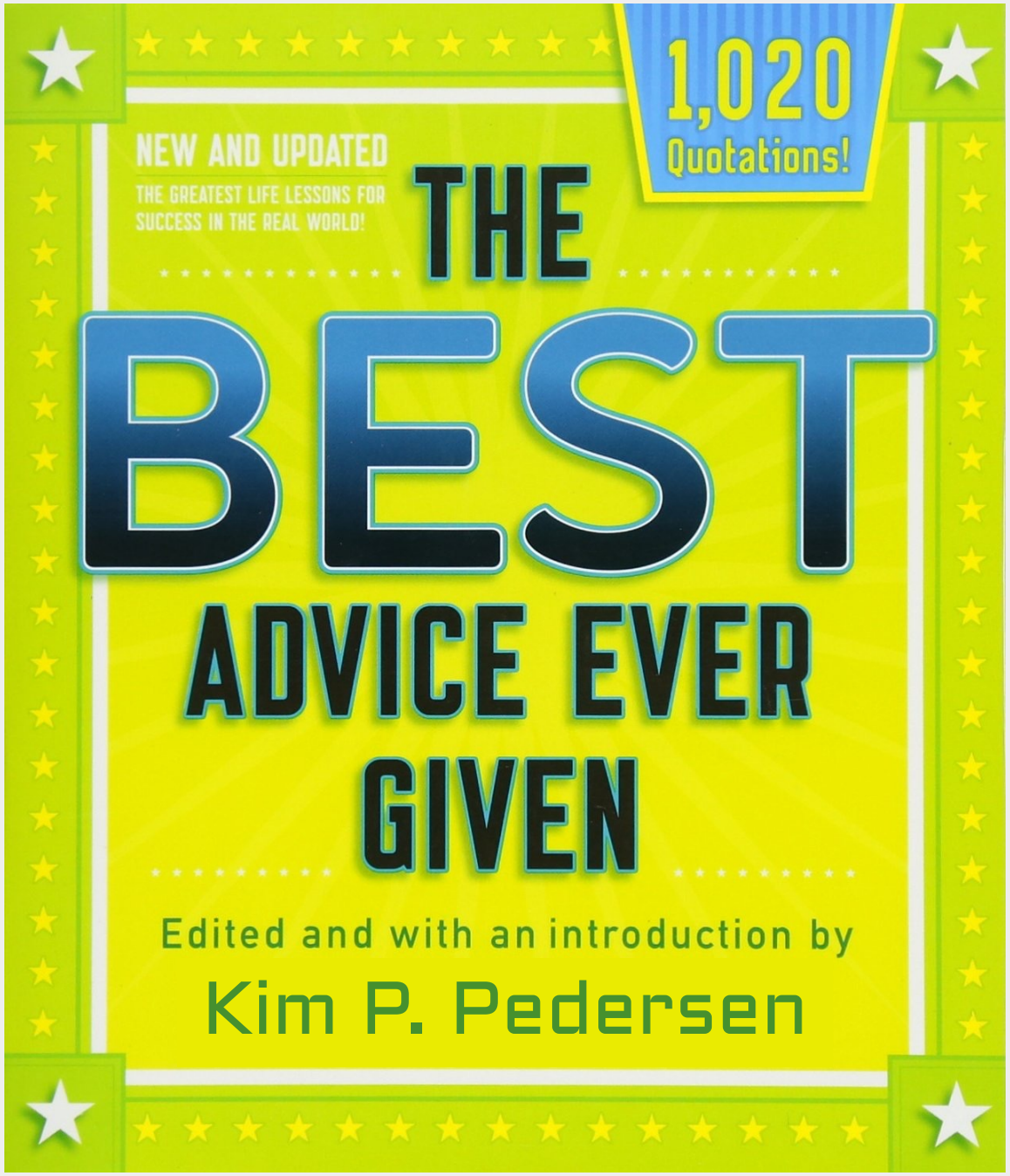
399 certifications listed | July 2021

https://pauljerimy.com/security-certification-roadmap/

Vi skaber værdi når deler
– Pay it forward!

De bedste råd fra en begynder

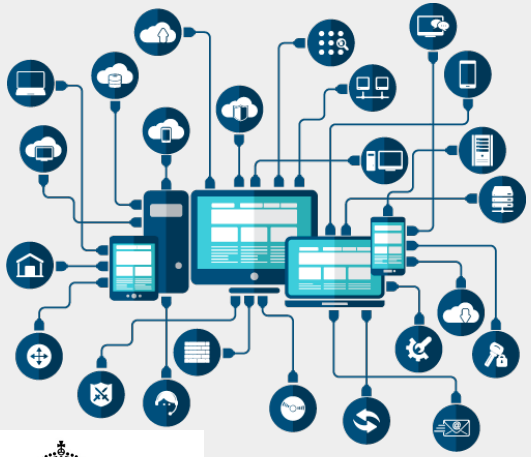




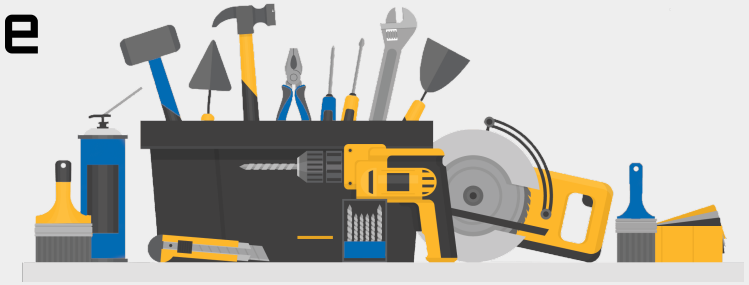
Hvad skal man lære som ny?

- Virtuelle Maskiner [VM's]
- Lær Command Line

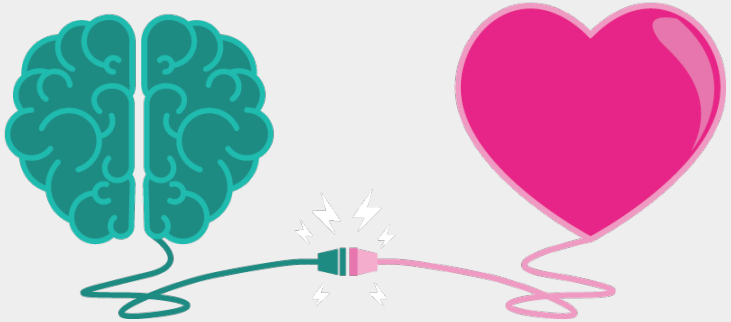


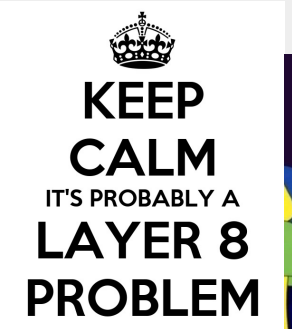



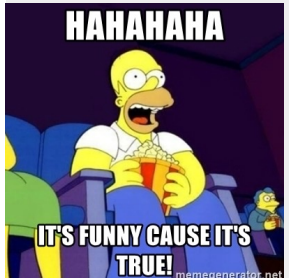
- Lær dine værktøjer at kende



- Netværk
- Finde noget at være passioneret omkring!







Sørg for at tage noter

- Obsidian
- Joplin
- Cherrytree

Youtube

- Network Chuck
- Lawrence Systems
- Hackernoon
- Hackersploit

Podcast

- Darknet Diaries
- Unsupervised Learning
- The Social-Engineer Podcast
- Smashing Security

Webinars

- Black Hills Information Security
- Wild West Hackin’ Fest


CERTIFICATE OF COMPLETION

THIS CERTIFICATE IS PRESENTED TO

Kim P. Pedersen

FOR HAVING SUCESSFULLY COMPLETED

Regular Expressions, Your New Lifestyle | Joff Thyer

VELDA LEMPKA
COO

JOHN STRAND
CEO

May 25, 2021

4-Hours


CERTIFICATE
PROUDLY PRESENTED TO

Kim P. Pedersen

Hack for Show, Report for Dough: Part 2 w/ BB King (1-Hour)

Oct 28, 2021
Date of Completion

John Strand
Organizer


CERTIFICATE
PROUDLY PRESENTED TO


CERTIFICATE
PROUDLY PRESENTED TO


CERTIFICATE
PROUDLY PRESENTED TO

for Post-Exploitation | Kyle

WildWestHackinFest
WWHF
Organizer


CERTIFICATE
PROUDLY PRESENTED TO

Kim P. Pedersen

ELK - Tips, Tricks, and Lessons Learned | Mark McLauchlin & Nicolas Taina | 1-Hour

Aug 18, 2021
Date of Completion

WildWestHackinFest
WWHF
Organizer


CERTIFICATE
PROUDLY PRESENTED TO

Kim P. Pedersen

The Roundup by Wild West Hackin' Fest: Red Team | Corey Overstreet | 4 Hours

Aug 12, 2021
Date of Completion

WildWestHackinFest
WWHF
Organizer


CERTIFICATE
PROUDLY PRESENTED TO

Kim P. Pedersen

IR Playbooks - A New Open Source Resource | Mathieu Saulnier | 1-Hour

Oct 20, 2021
Date of Completion

WildWestHackinFest
WWHF
Organizer


CERTIFICATE
PROUDLY PRESENTED TO

Kim P. Pedersen

Interviewee Field Manual: Hack the Interview | Doug Brush | 1 Hour

Mar 31, 2021
Date of Completion

WildWestHackinFest
WWHF
Organizer

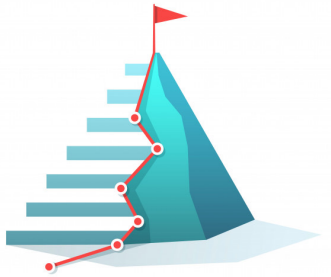
CTF's, Hack the Box, TryHackMe

Try Hack Me

HACKTHEBOX

CTF
CAPTURE THE FLAG

- Formålet er at løse en række tekniske opgaver indenfor Cybersikkerhed
- Dette en god læringsvej



Forensics

Cryptography

Web Exploitation

Reverse Engineering

Binary Exploitation

Den danske Foreninger og events

- BSides København
- OWASP Copenhagen Chapter
- OWASP Aarhus Chapter
- Infosecurity Denmark

Når du skal ud og have et job

- Udnyt din praktik
- Brug dit netværk
- Tal med et rekruteringsfirma
- Tag ud til events
- Hold dig aktiv!

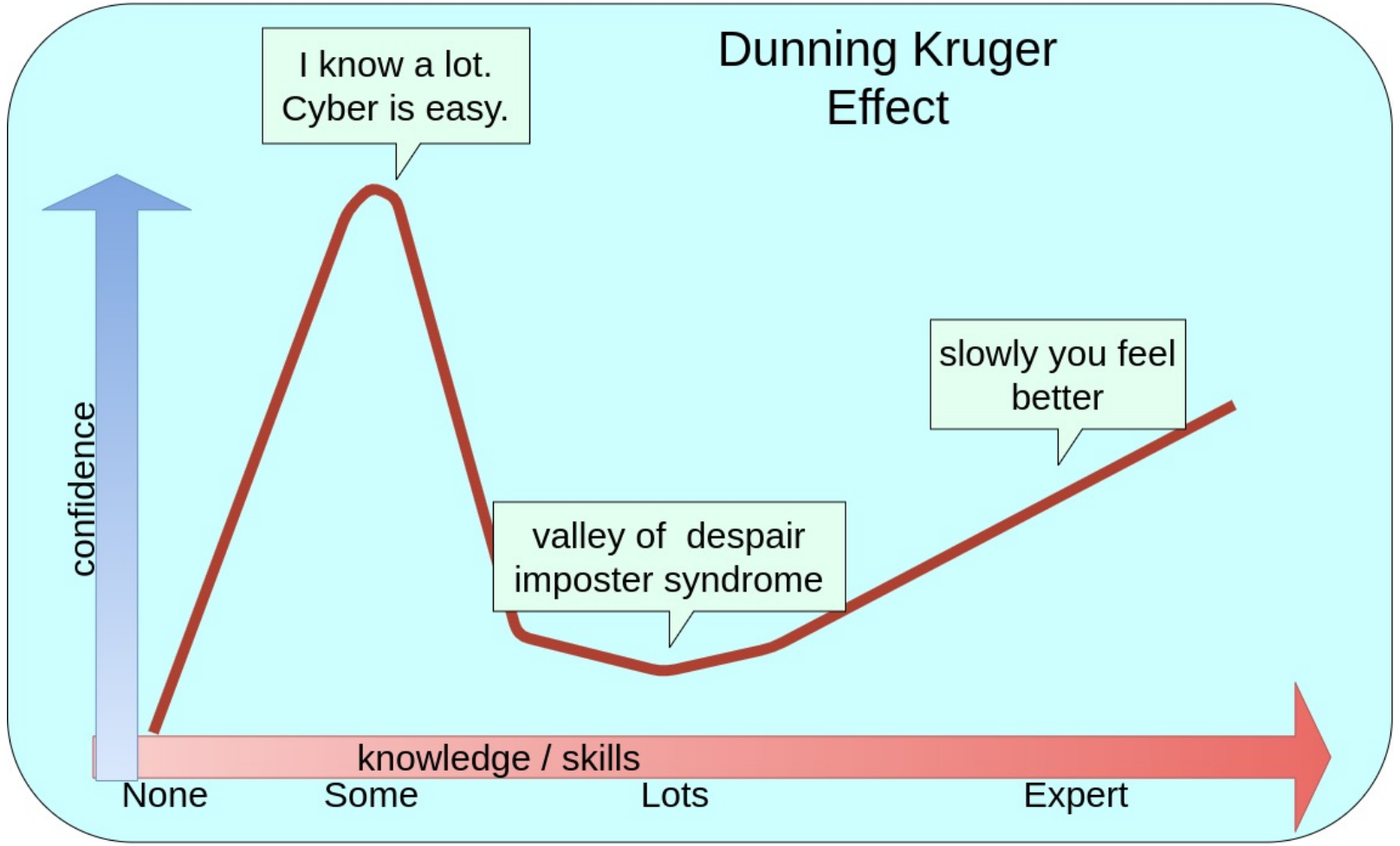
Show – Don't tell!

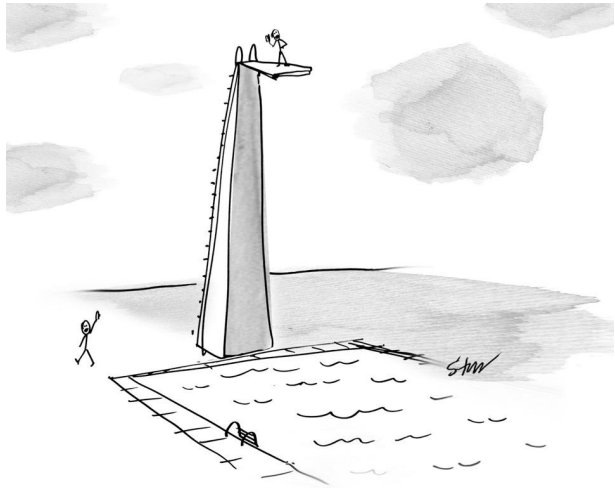
LinkedIn

- Opdater dit CV
- Opdater din LinkedIN
- Opdater din GitHub
- Skriv en blog
- Lav en Youtube
- Lav en Podcast
- Få dig en Twitter-profil (No reposts)

Vær kreativ så du skiller dig ud!

Bedragersyndrom





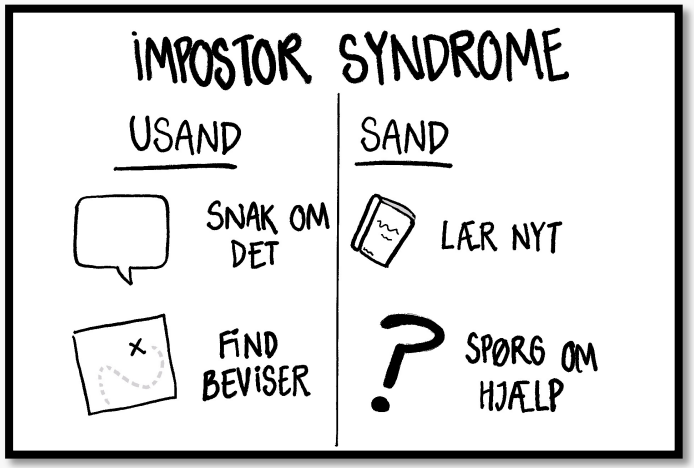
"I'm good."

Tegn på bedragersyndrom

- Frygt for at blive afsløret som inkompetent
- Føle sig succesfuld uværdig
- Afviser positiv feedbach
- Mistroende overfor andre
- Kalder succes for held
- Ekstrem forbereder sig til alt

Håndter bedragersyndrom

- Forhold dig til de ting du ved – fakta!
- Tag fat i branchen for at få støtte
- Lav en liste med dine bedrifter
- Vær realistisk og ikke perfektionistisk
- Hør om andres erfaringer
- Accepter at du kun er menneske




SUCCESS
This Way

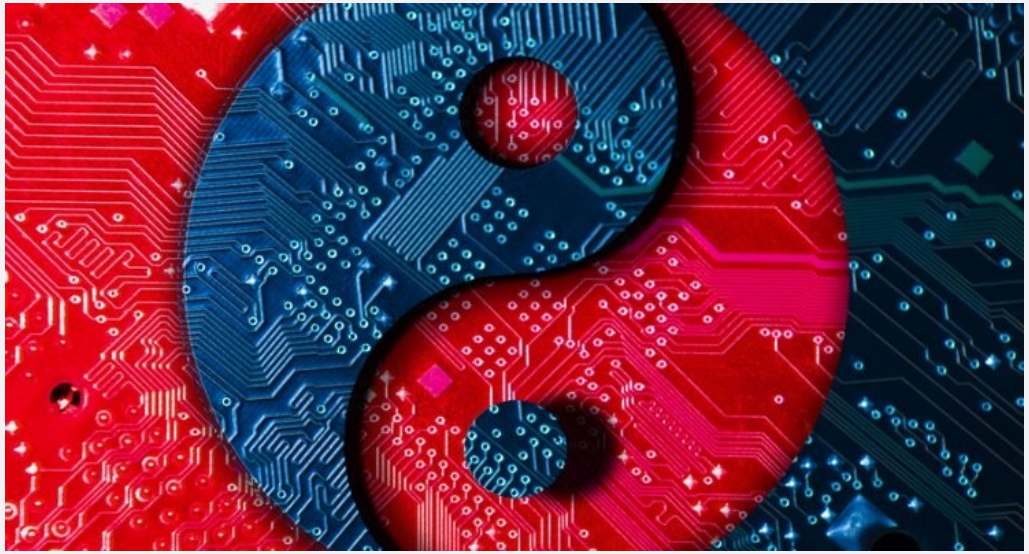

MTV THE
REAL
WORLD

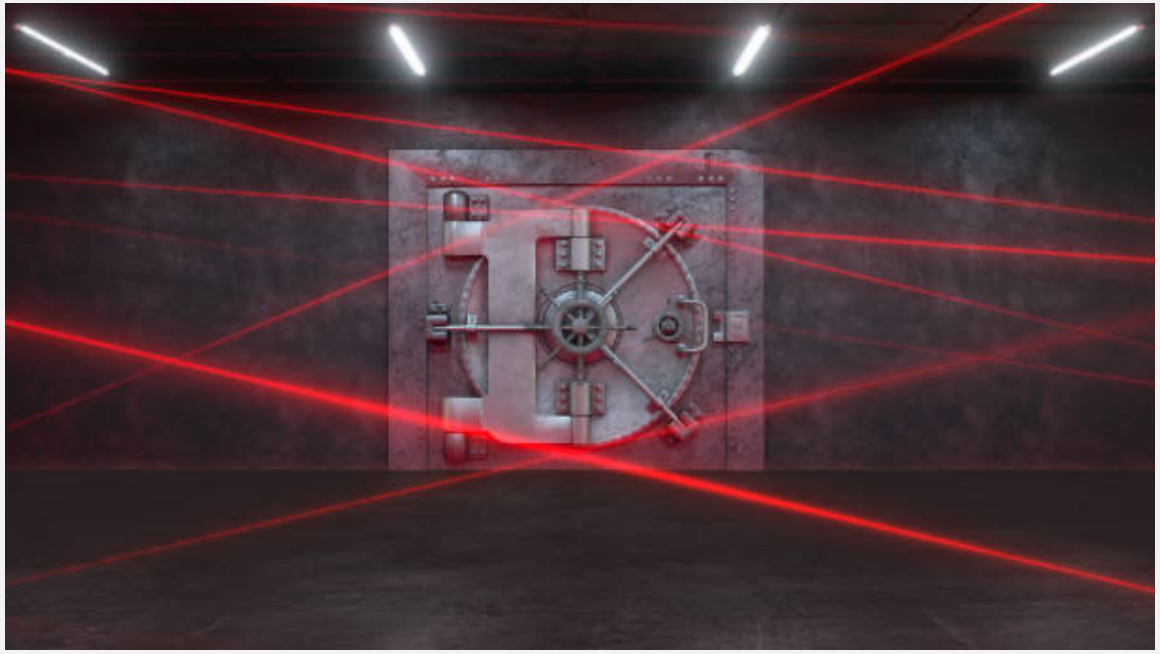
Red vs. Blue

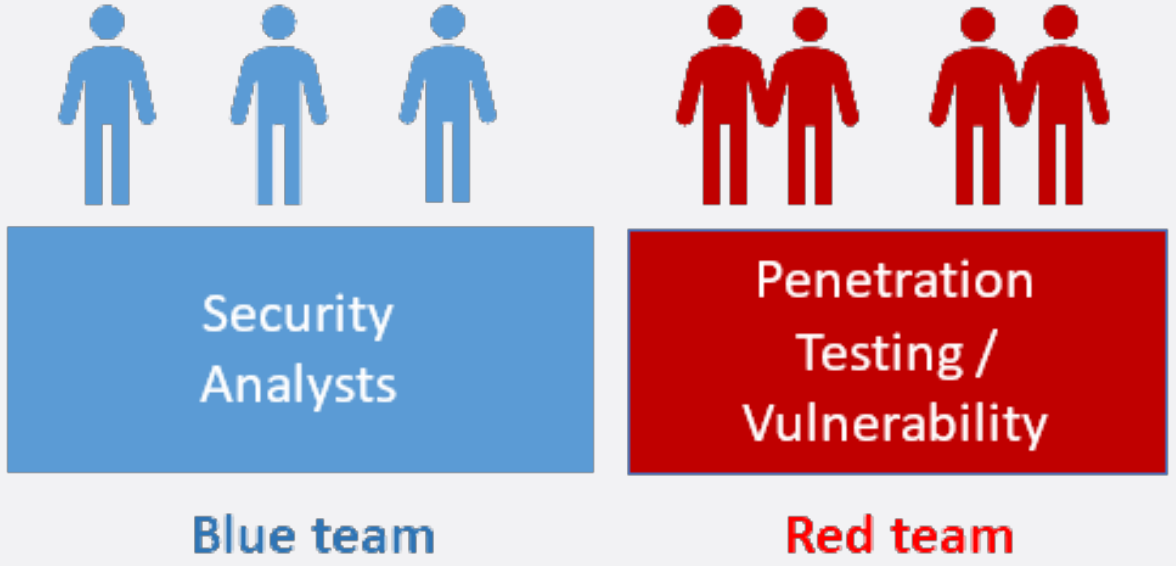
Disclaimer!
Begge dele kræver hårdt arbejde, flid og passion!

Der er:

- Ingen BLÅ uden RØD
- Og ingen RØD uden BLÅ





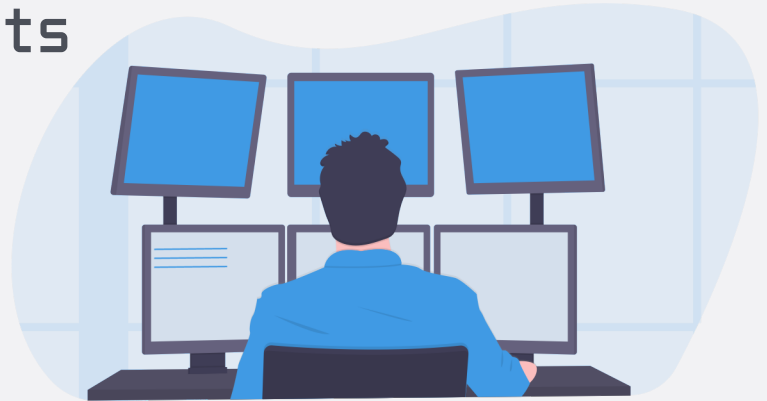


Den rigtige vej for mig, var at få job i et

Cyber Defence Center

Fordelen ved at arbejde i en CDC er, at du får indblik i IT infrastruktur og sikkerhed i bl.a.:

- AV
- Netværk
- Authentication
- Servere og endpoints
- Cloud
- Etc ...



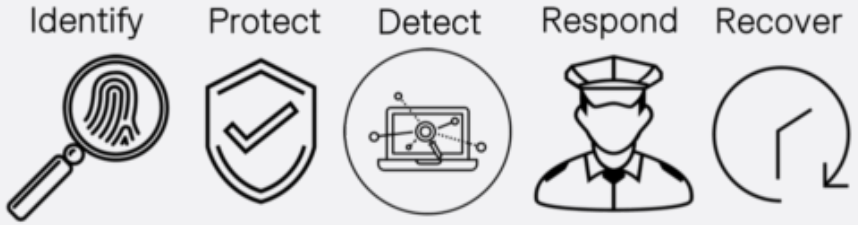
Cyber Defence Center (CDC)

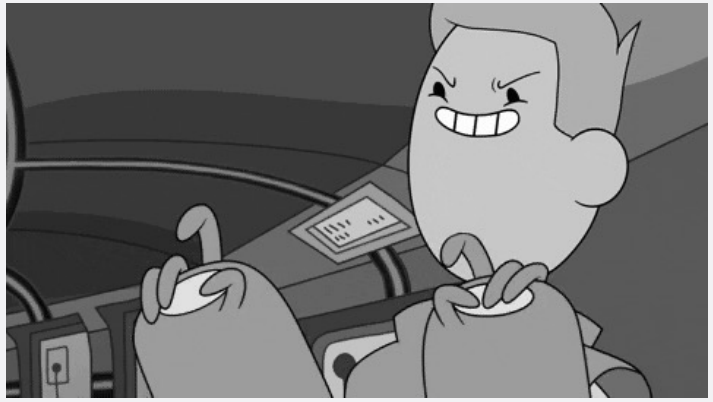
Et Cyber Defence Center består af et hold sikkerhedseksperter med bredt indblik i cybersikkerhed, som:

- Overvåger
- Analyserer
- Håndterer

kritiske hændelser og fejl på netværk og servere

Det er: hands on action!





Hvad er en CDC's opgaver

Forebyggelse

Compliance

Overvåge

Risiko

Detektion

Rapportering

Analysering

Hændelseshåndtering

Respons/reaktion

Forskellige "typer" SOC/CDC's

Sårbarheds drevet SOC/CDC

- Der ledes efter sårbarheder i infrastrukturen
- Der laves sårbarhedsscanninger
- Der ledes efter explations muligheder

Compliance drevet SOC/CDC

- De dokumentere hvad der overvåges
  - så når der kommer audit kan der siges:
    vi overvåger disse her services.

Forskellige "typer" SOC/CDC's

Threat drevet drevet SOC/CDC

- De hele tiden holder sig opdateret på hvad der er af trusler
- Og hvordan de kan detekteres (altså selv udvikle måder at finde disse trusler)

"Helpdesk SOC/CDC"

- Sørger for at håndtere AV, IDS og IPS alarmer
  - Håndtere dem for driften
- er ikke proaktiv i detektering
  - men skal bare alarmere den relevante ansvarlige.

Forskellige roller i en CDC

	Analytiker Lvl. 1	Alarm Analytiker
	Analytiker Lvl. 2	Incident Responder
	Analytiker Lvl. 3	SME/ Threat Hunter
	CDC Manager	Commander
	CDC Engineer	Platform Management

- Overvåger SIEM alarmer, administrerer og konfigurerer sikkerhedsovervågningsværktøjer
- Undersøger om alarmer er falsk positive eller eskalere hændelsen

- Modtager alarmer og foretager grundigere analyse baseret på threat intel for at identificere agrebetsnatur
- Bestemmer baggrund af alarmen trusselsniveaue, strategi for isolering, oprydning og genetablering af de inficerede systemer

- Daglig trusselsvurdering og penetrationstest (POC)
- Aktivt udfører Threat Hunt I systemerne
- Assisterer Lvl. 2 Analytikere med isolering, oprydning og genetablering af de inficerede systemer

- Er ansvarlig for CDC'en, ansættelser og træning af personale, styrer offensiv og defensiv strategi, tildeler ressourcer, prioritet og projekter.
- Har det forretningsmæssige overblik
- Er kontaktperson for SOC'en omkring sikkerhedshændelser, compliance og sikkerhed

- Software eller hardware specialist som fokusere på sikkerhedsaspektet i driftsystemer
- Udvikler løsninger og værktøj til at assistere SOC'en med drift og hændelser
- Kan både være intern og ekstern i SOC'en enten som udvikler eller som analytiker

Essensen i en CDC

”Indsamling, analyse og eskalere af indikationer og advarsler med henblik på at opdage og reagere på indtrængen.” Richard Bejtlich, The Tao Of Network Security Monitoring

Log kilder

Du bliver en mester I logs

```
An account was successfully logged on.

Subject:
    Security ID: SYSTEM
    Account Name: DESKTOP-LLHJ389$
    Account Domain: WORKGROUP
    Logon ID: 0x3E7

Logon Information:
    Logon Type: 7
    Restricted Admin Mode: -
    Virtual Account: No
    Elevated Token: No

Impersonation Level: Impersonation

New Logon:
    Security ID: AzureAD\RandyFranklinSmith
    Account Name: rsmith@montereytechgroup.com
    Account Domain: AzureAD
    Logon ID: 0xFD5113F
    Linked Logon ID: 0xFD5112A
    Network Account Name: -
    Network Account Domain: -
    Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
    Process ID: 0x30c
    Process Name: C:\Windows\System32\lsass.exe

Network Information:
    Workstation Name: DESKTOP-LLHJ389
    Source Network Address: -
    Source Port: -

Detailed Authentication Information:
    Logon Process: Negotiat
    Authentication Package: Negotiate
    Transited Services: -
    Package Name (NTLM only): -
    Key Length: 0
```

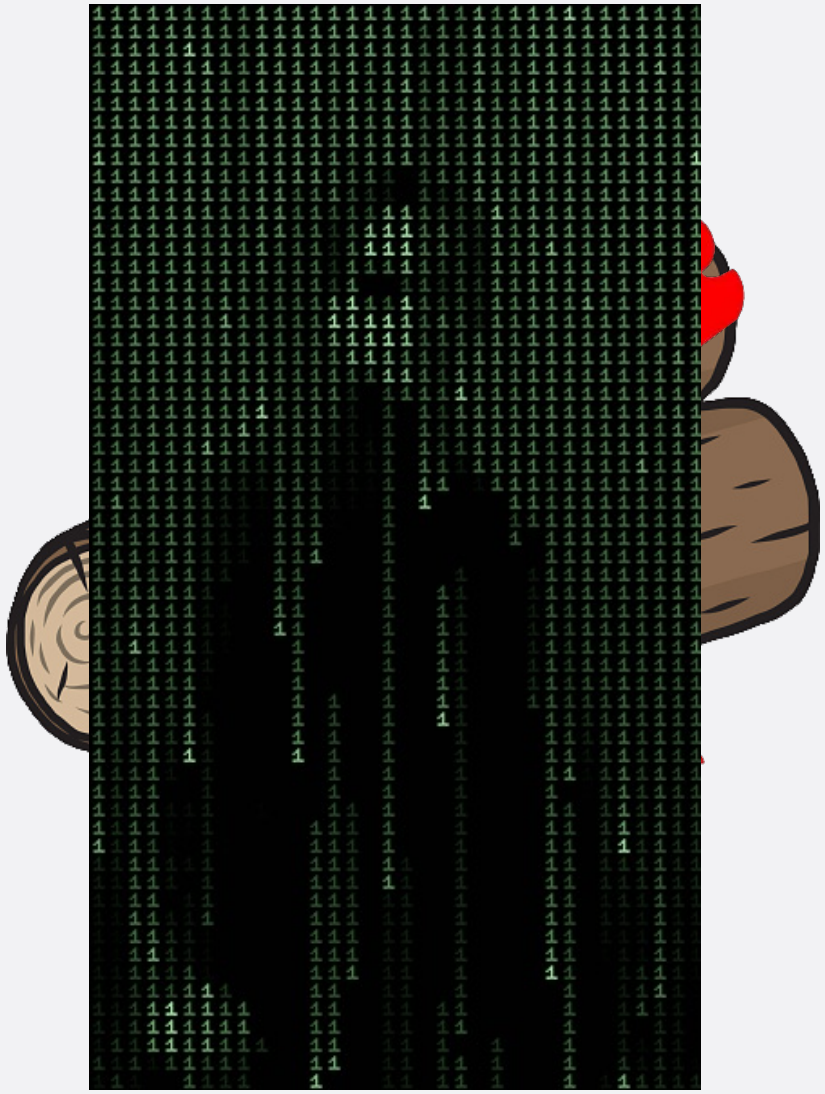
Du bliver en mester I logs

```
<Event
xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider
Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-a5ba-
3e3b0328c30d}'/><EventID>4725</EventID><Version>0</Version><Level>Information</Level>
<Task>User Account Management</Task><Opcode>Info</Opcode><Keywords>Audit
Success</Keywords><TimeCreated SystemTime='2017-03-
15T08:15:25.219602600Z'/><EventRecordID>2159709036</EventRecordID><Correlation/><Exec
ution ProcessID='784'
ThreadID='2772'/><Channel>Security</Channel><Computer>XXXW0023P.xxx.corp.xxxxx.com</C
omputer><Security/></System><EventData>A user account was disabled.

Subject:
Security ID: XXXCORP\SAC_ADMIN
Account Name: SAC_ADMIN
Account Domain: XXXCORP
Logon ID: 0x2CA57400

Target Account:
Security ID: XXXCORP\QHSC
Account Name: QHSC
Account Domain: XXXCORP</EventData></Event>
```

Du bliver en mester I logs

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'>
    <System>
        <Provider Name='Microsoft-Windows-Security-Auditing'
                  Guid='{54849625-5478-4994-a5ba-3e3b0328c30d}'/>
        <EventID>4625</EventID>
        <Version>0</Version>
        <Level>Information</Level>
        <Task>Logon</Task>
        <Opcode>Info</Opcode>
        <Keywords>Audit Failure</Keywords>
        <TimeCreated SystemTime='2021-07-14T03:57:15.687128800Z'/>
        <EventRecordID>197727456</EventRecordID>
        <Correlation/>
        <Execution ProcessID='688' ThreadID='2928'/>
        <Channel>Security</Channel>
        <Computer>server01.acme.local</Computer>
        <Security/>
    </System>
    <EventData>
        <Data Name='SubjectUserSid'>NULL SID</Data>
        <Data Name='SubjectUserName'>-</Data>
        <Data Name='SubjectDomainName'>-</Data>
        <Data Name='SubjectLogonId'>0x0</Data>
        <Data Name='TargetUserSid'>NULL SID</Data>
        <Data Name='TargetUserName'>johndoe</Data>
        <Data Name='TargetDomainName'>PC1234</Data>
        <Data Name='Status'>0xc000006d</Data>
        <Data Name='FailureReason'>Unknown user name or bad password.</Data>
        <Data Name='SubStatus'>0xc0000064</Data>
        <Data Name='LogonType'>3</Data>
        <Data Name='LogonProcessName'>NtLmSsp </Data>
        <Data Name='AuthenticationPackageName'>NTLM</Data>
        <Data Name='WorkstationName'>PC1234</Data>
        <Data Name='TransmittedServices'>-</Data>
        <Data Name='LmPackageName'>-</Data>
        <Data Name='KeyLength'>0</Data>
        <Data Name='ProcessId'>0x0</Data>
        <Data Name='ProcessName'>-</Data>
        <Data Name='IpAddress'>192.168.50.28</Data>
        <Data Name='IpPort'>2628</Data>
    </EventData>
</Event>
```

Du bliver en mester I logs

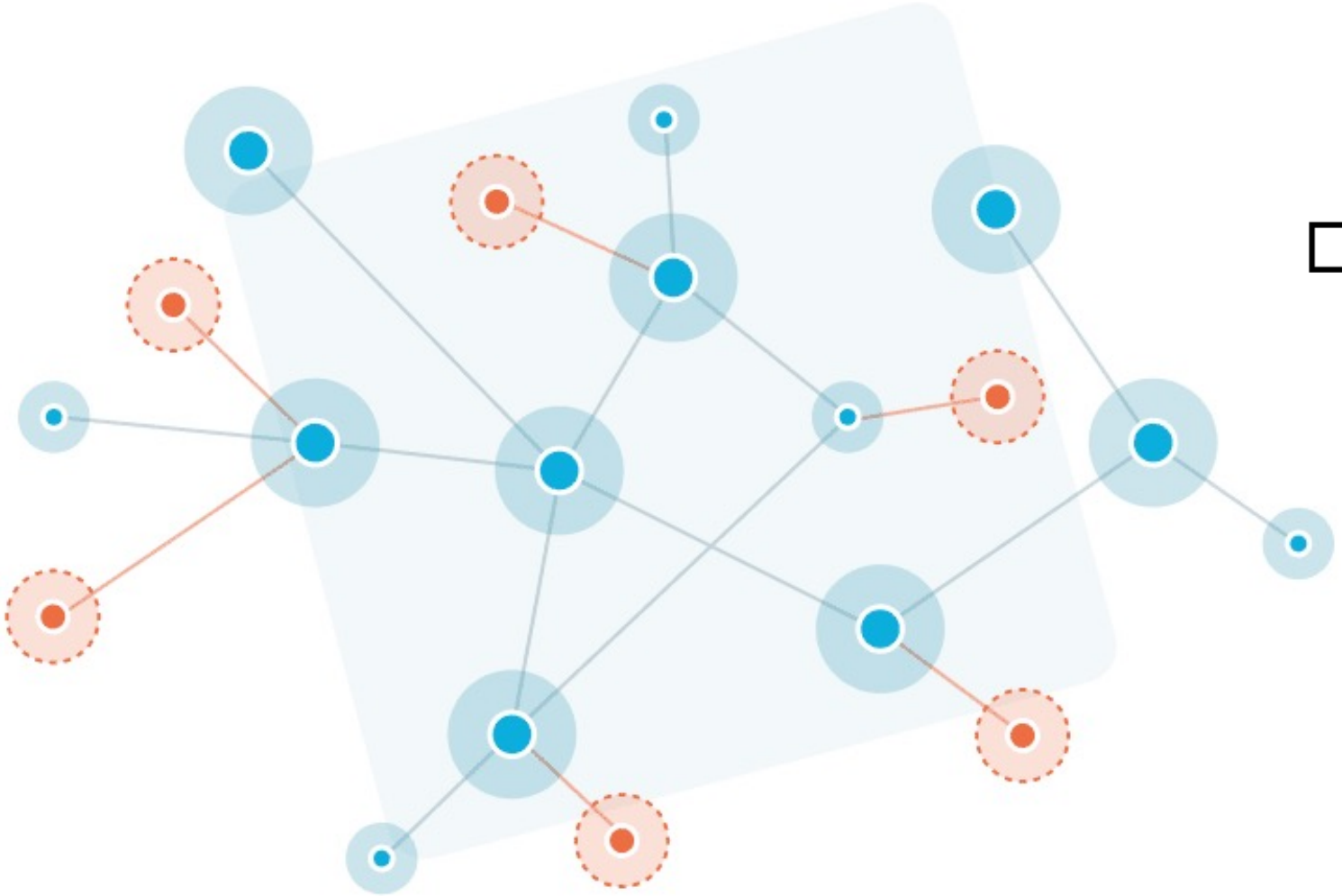


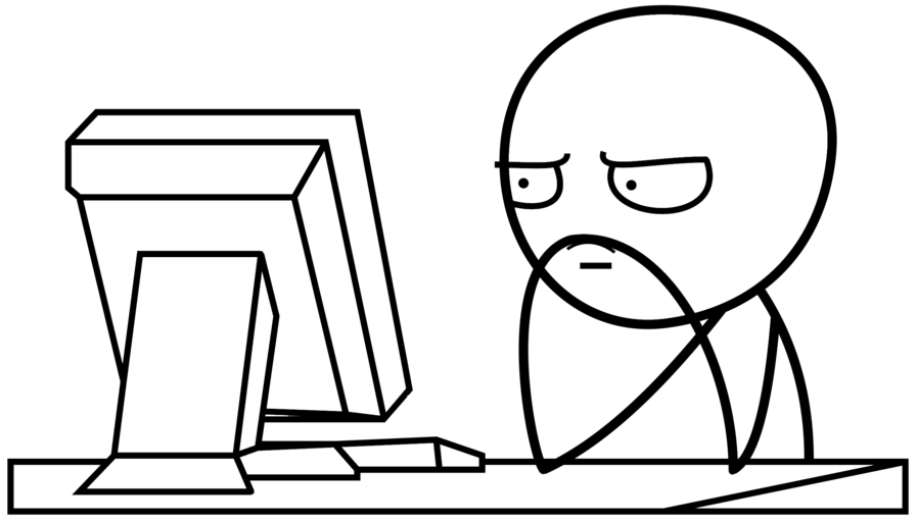
```
Error Message %FTD-6-106102: access-list acl_ID {permitted|denied} protocol for user
username interface_name /source_address source_port interface_name /dest_address
dest_port hit-cnt number {first hit|number -second interval} hash codes
```

```
05 08 2019 16:06:43 10.107.164.50 <LOC4:INFO> May  8 16:06:43 10.107.224.1 %ASA-6-
302015: Built outbound UDP connection 489262606 for outside:176.104.35.212/6881
(176.104.35.212/6881) to inside:10.107.214.27/8621 (191.51.32.6/8621)
```

```
02 28 2017 10:58:33 10.99.192.4 <LOC4:WARN> %ASA-4-106023: Deny udp src
INSIDE:10.172.92.12/7275 dst OUTSIDE:92.121.115.244/6881 by access-group
"FW_ACL_OUT_OUTSIDE" [0x0, 0x0]
```

Se mønstre

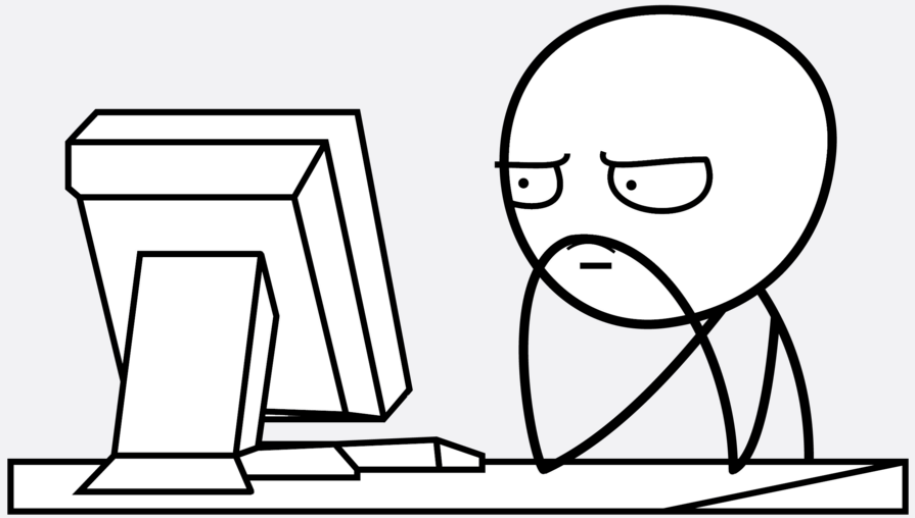


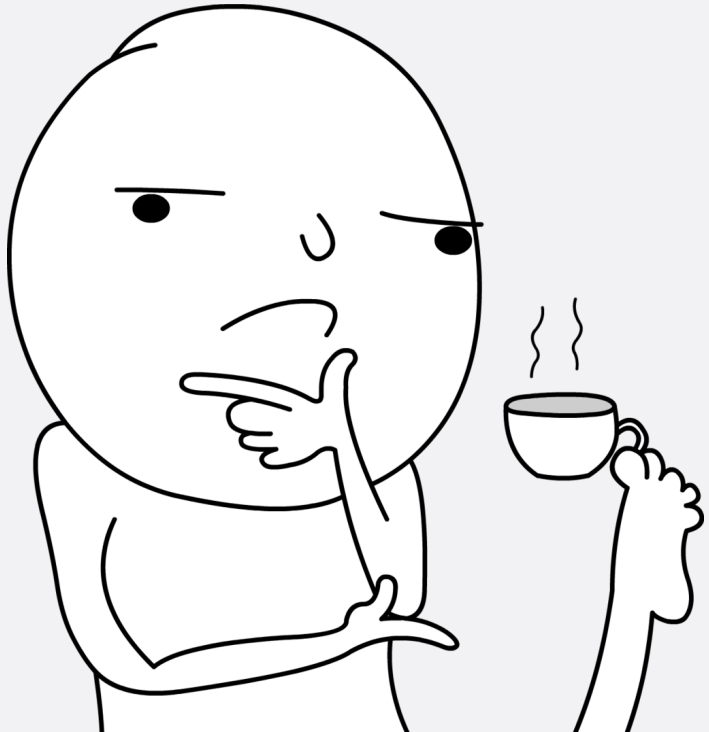


Se mønstre

- Bevis at der er en komprimentering
- Bevis at der ikke er en komprimentering

Hver beslutning tæller...






INFECTIONS / SECOND (2)
LIVE ATTACKS (65442)
BOTNETS (7)
COUNTRIES (19)
Customizable world clock with seconds & World time zones
Search
San Francisco 03:32
New York 06:32
Oslo 14:32
London 14:32
Rio de Janeiro 10:32
Tokyo 23:32
14:33:00
Oslo, Norway
Monday
January 11, 2021

Angreb

- En undersøgelse foretaget i 2003 fandt ud af, at der i gennemsnit er et angreb hvert 39. sekund på nettet.
  Kilde: https://patchstack.com/website-hacking-statistics/
- I slutningen af 2021 forventes cyberkriminalitet at koste verden $ 6 billioner.
  Kilde: https://www.packetlabs.net/cybersecurity-statistics-2021/
- Cybercrime Up 600% Due To COVID-19 Pandemic
  Kilde: https://purplesec.us/resources/cyber-security-statistics/

IT angreb

Automatiseret + Specialiseret

Firmaer i Danmark

Angreb

- DoS and DDoS Attacks
- MITM Attacks
- Phishing Attacks
- Whale-phishing Attacks
- Spear-phishing Attacks
- Ransomware
- Password Attack
- SQL Injection Attack
- URL Interpretation
- DNS Spoofing
- Session Hijacking
- Brute force attack
- Web Attacks
- Insider Threats
- Trojan Horses
- Drive-by Attacks
- XSS Attacks
- Eavesdropping Attacks
- Birthday Attack
- Malware Attack

IT angreb

Automatiseret + Specialiseret

Firmaer i Danmark

Dubex:
Cyber Defence Center

- I Dubex Cyber Defence Center (CDC) overvåger og analyserer erfarne specialister din infrastruktur med henblik på at identificere unormale hændelser, fejl, angrebsmønstre og alarmer.
- CDC-teamet kan også sende kritiske alarmer eller fejl direkte videre til behandling i Dubex' Security Operations Center (SOC) eller Dubex Incident Response Team (DIRT).

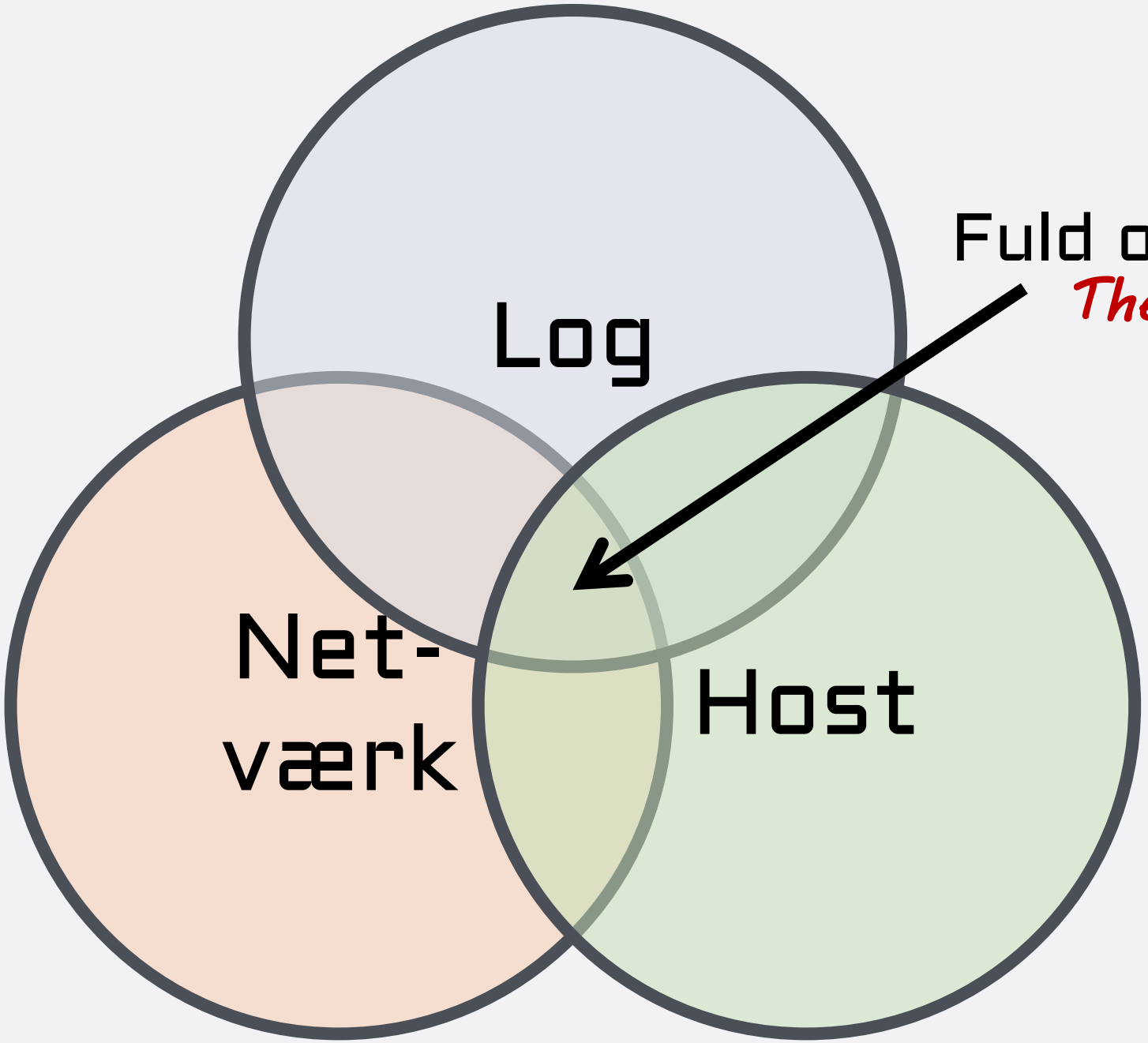
IT angreb

Automatiseret + Specialiseret

Dubex:

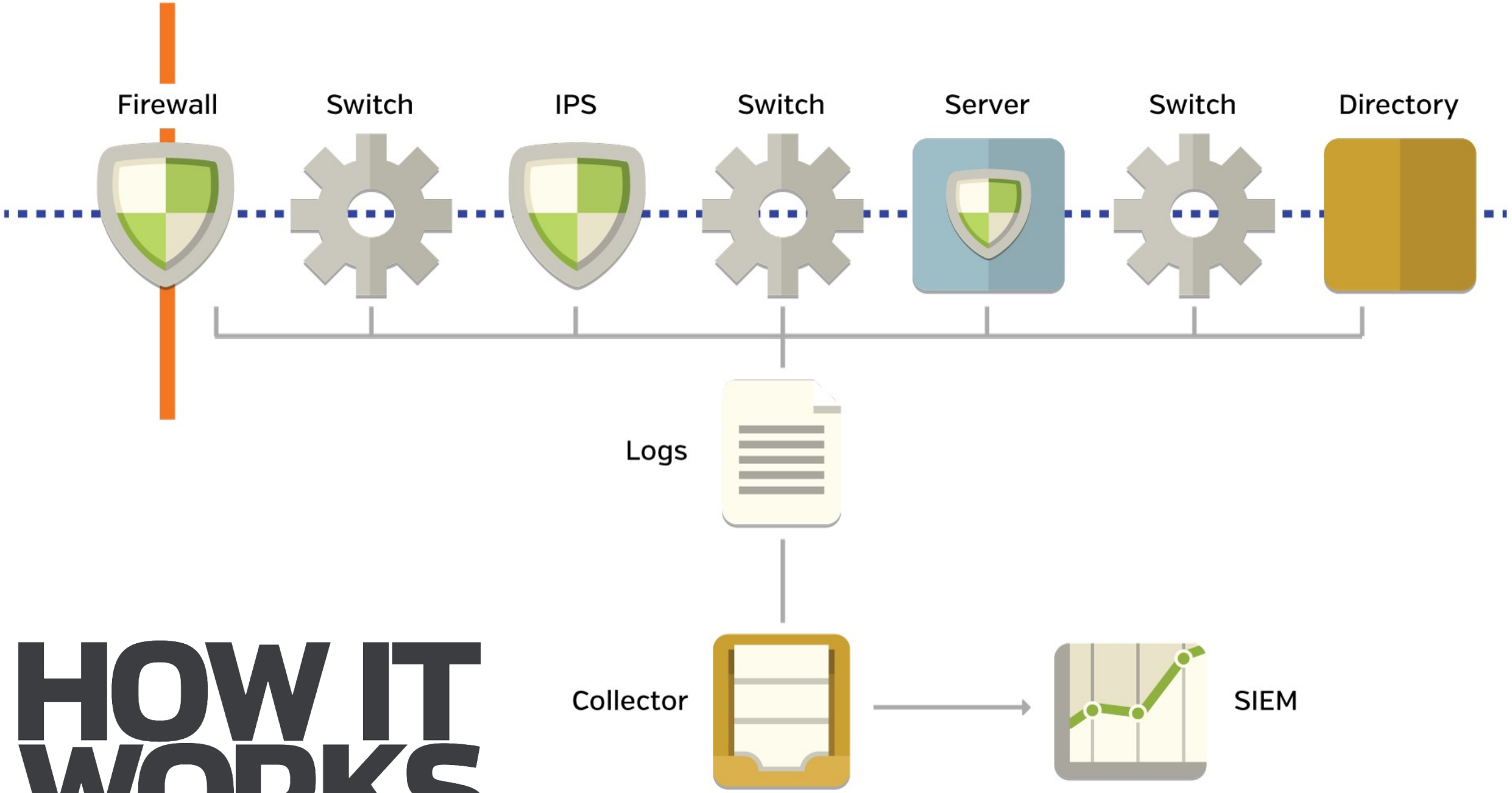
Cyber Defence Center

Ekstra bekyttelse



Fuld overvågning

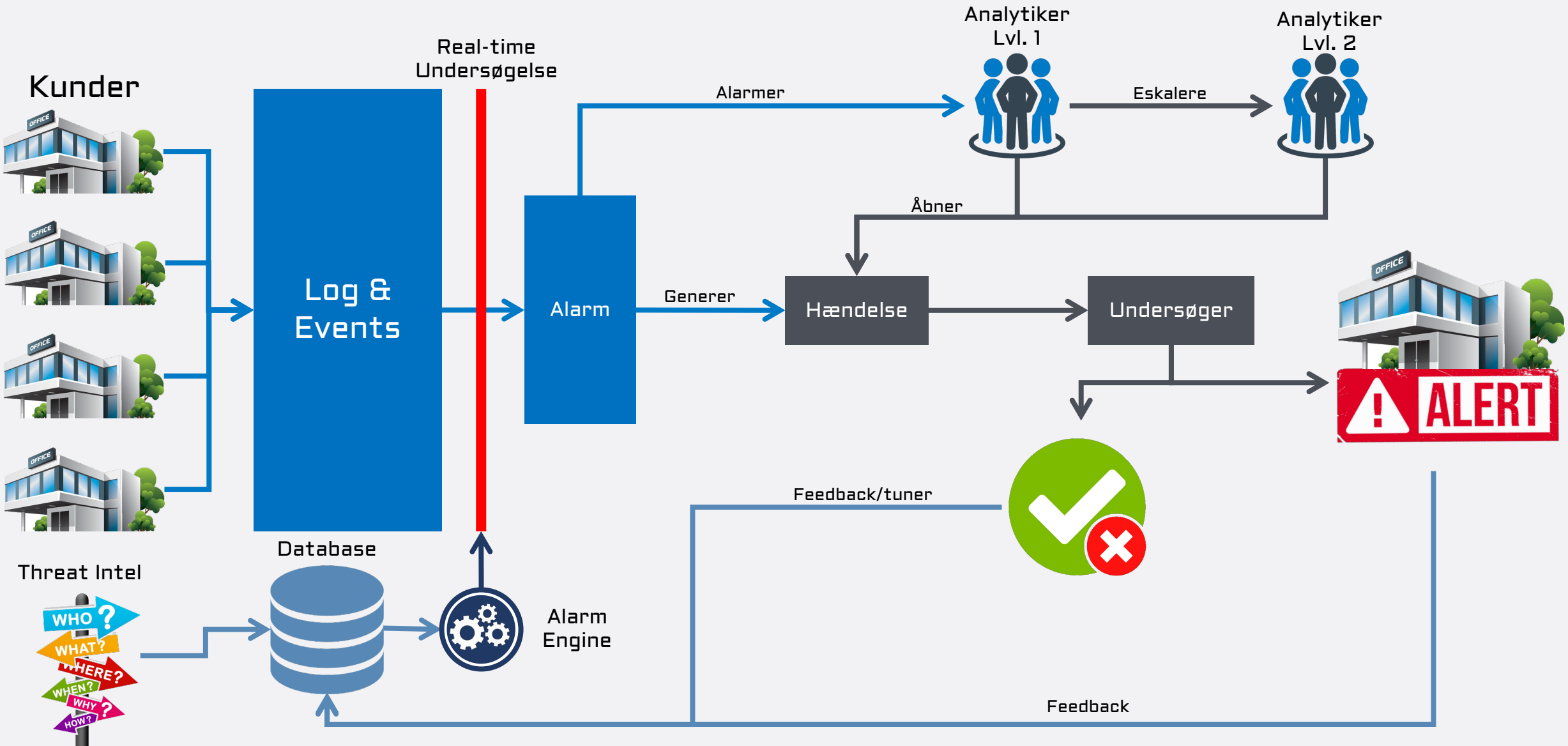
The sweet spot



HOW IT WORKS

Data centre monitoring visualized by @marknca

Workflow i CDC



Gaining access – Trojan - billede

- Mail – Se billede af min kat!
- I billedet var der nemlig gemt en reverse shell

- *06-04-2021 - Hiding Msfvenom backdoor in JPG image - David Artykov*
  Kilde: https://medium.com/purple-team/hiding-msfvenom-backdoor-in-jpg-image-8fa9dd18c924

Praktisk eksempelt

MISP

Open Source Threat Intelligence Platform

MISP – DIGI-TALKS 2021

Dubex:

MISP

=

Malware Information Sharing Platform

Dubex:

Hvad er en MISP

MISP er en:

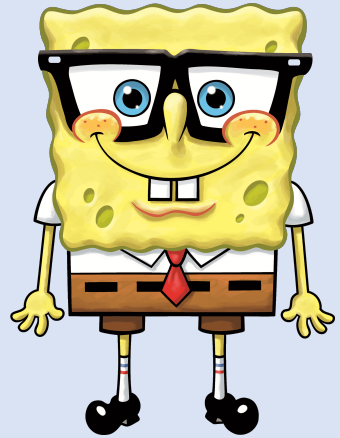
Gratis open source platform

Mere end **6000** firmaer omkring
i verdenen benytter sig af MISP

MISP – Introduktion

2012

- Oprindelige forfatter(e): Christophe Vandeplas
- Udvikler(e): Andras Iklody (hovedudvikler) m.fl.
- Stabil udgave: 2.4.148[1] / 5. august 2021
- Skrevet i PHP
- Licens: GNU Affero GPLv3
- Repository https://github.com/MISP/MISP
- Websted: misp-project.org

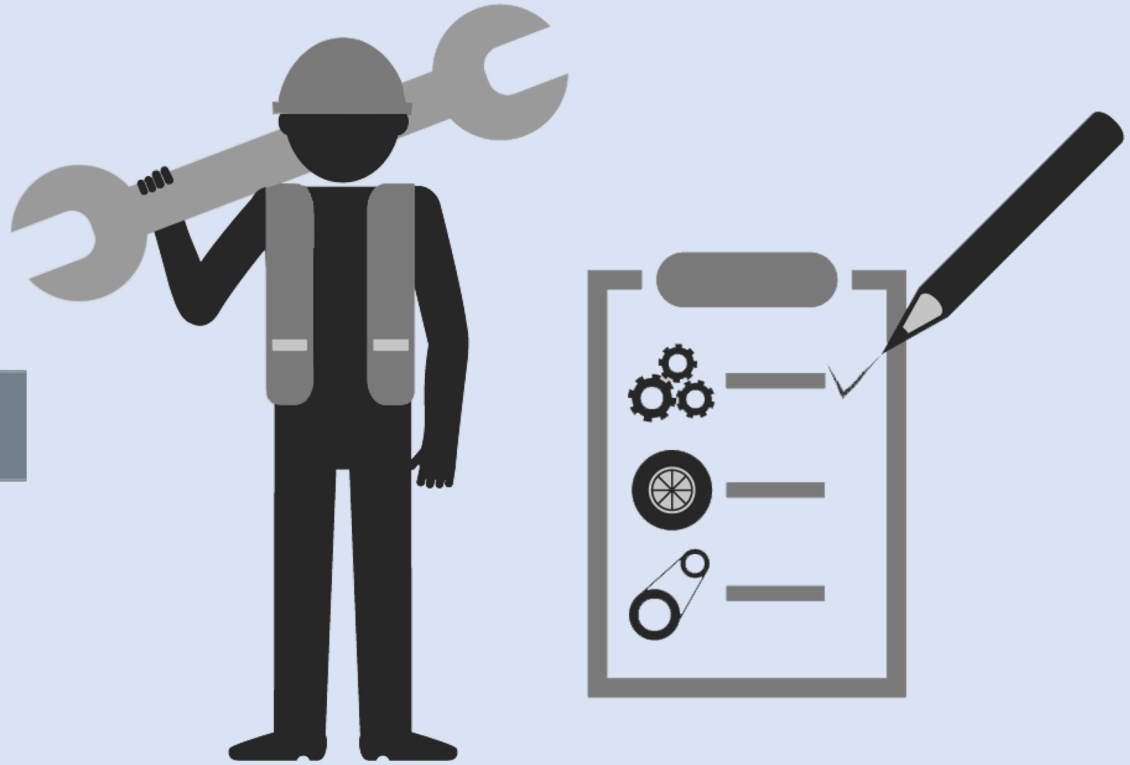


Co-financed by the European Union
Connecting Europe Facility

Drevet og vedligeholdt af

circl.lu

Computer Incident
Response Center
LUXEMBOURG



CIRCL MISP Threat Sharing

CIRCL DMA Dynamic Malware Analysis

CIRCLean USB Sanitizer

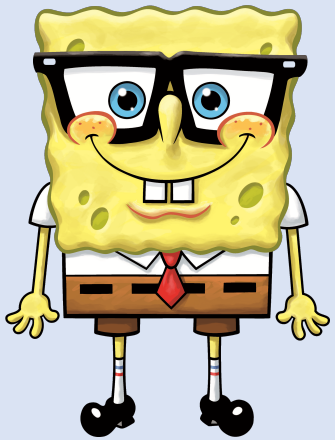
CIRCL Passive DNS

Hvad er en MISP

MISP er en trusselsinformationsplatform til:

- Deling
- Lagring
- Korrelering

af indikatorer for kompromittering (IOC) af målrettede angreb.



Co-financed by the European Union
Connecting Europe Facility


UI User
API
Database
MISP
Threat Sharing
IP
EVENT A
EVENT B

Hvem benytter sig af MISP?

Malware responders

Sikkerhedsanalytikere

Efterretningsanalytikere

Myndigheder

Risikoanalysehold

Svindelanalytikere

List Events
Add Event
Import from...
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals
View delegation requests

Export
Automation

Events

« previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next »

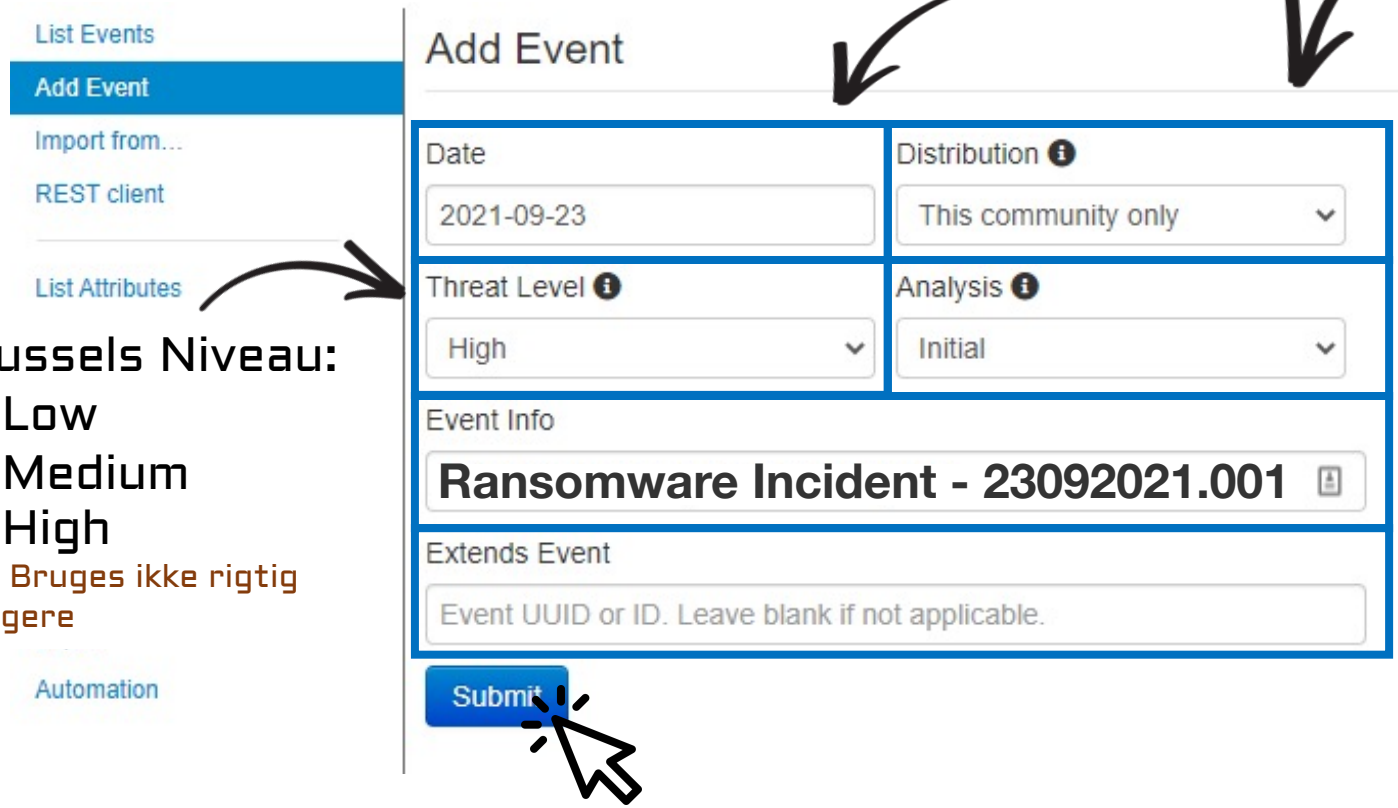
My Events | Org Events | Enter value to search | Filter

Published	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
✓	DBX_Admin	DBX_Admin	1		osint:source-type="block-or-filter-list" DBX: DIRT Sync	2192	47	admin@admin.test	2021-08-09	Metasploit exploits with CVE assigned feed	Organisation	
✓	CthulhuSPRL.be	DBX_Admin	2		type:OSINT tlp:green tlp:white	1067	3	admin@admin.test	2014-10-02	OSINT ShellShock scanning IPs from OpenDNS	All	
✓	CthulhuSPRL.be	DBX_Admin	3		type:OSINT tlp:green	29	2	admin@admin.test	2014-10-03	OSINT New Indicators of Compromise for APT Group Nitro Uncovered blog post by Palo Alto Networks	All	
✓	CthulhuSPRL.be	DBX_Admin	4		type:OSINT tlp:green	225	3	admin@admin.test	2014-10-09	OSINT Evolution of the Nuclear Exploit Kit by Cisco Talos group	All	
✓	CthulhuSPRL.be	DBX_Admin	5		type:OSINT tlp:green	65	4	admin@admin.test	2014-10-09	OSINT Democracy in Hong Kong Under Attack blog post from Volexity (Steven Adair)	All	
✓	CthulhuSPRL.be	DBX_Admin	6		type:OSINT tlp:green	1817	8	admin@admin.test	2014-09-01	OSINT Watching Attackers Through Virustotal blog post by Brandon Dixon (9bplus)	All	
✓	CthulhuSPRL.be	DBX_Admin	7		type:OSINT tlp:green	31		admin@admin.test	2014-10-11	OSINT Shellshock exploitation from Red Sky Weekly blog post	All	
✓	CthulhuSPRL.be	DBX_Admin	8		type:OSINT tlp:green	98	1	admin@admin.test	2014-10-20	OSINT OrcaRAT - A whale of a tale blog post by PWC	All	
✓	CthulhuSPRL.be	DBX_Admin	9		type:OSINT tlp:green	414	11	admin@admin.test	2014-10-23	Expansion on OSINT Operation Pawn Storm: The Red in SEDNIT from Trend Micro	All	
✓		DBX_Admin	10	Threat Actor Axiom	tlp:green tlp:white osint:source-type="blog-post" type:OSINT	20970	14	admin@admin.test	2014-10-28	OSINT - Operation SMN (Novetta)	All	
✓	CthulhuSPRL.be	DBX_Admin	11	Threat Actor Sofacy	tlp:green type:OSINT	114	17	admin@admin.test	2014-10-27	OSINT APT28: A Window into Russiaâ€™s Cyber Espionage Operations? blog post by FireEye	All	
✓	CthulhuSPRL.be	DBX_Admin	12		type:OSINT tlp:green	25	3	admin@admin.test	2014-10-23	OSINT Emerging Threat Alert - CVE-2014-4114 blog post by Cylance	All	
✓	CthulhuSPRL.be	DBX_Admin	13		type:OSINT tlp:green	34	2	admin@admin.test	2014-11-05	OSINT Banking Trojan DRIDEX Uses Macros for Infection blog post from Trend Micro	All	
✓	CthulhuSPRL.be	DBX_Admin	14		type:OSINT tlp:green	74	14	admin@admin.test	2014-10-30	OSINT The Rotten Tomato Campaign	All	
✓	CthulhuSPRL.be	DBX_Admin	15		type:OSINT tlp:green	39	3	admin@admin.test	2013-02-08	OSINT Adobe Zero-day Used in LadyBoyle Attack blog post by Symantec	All	
✓	CthulhuSPRL.be	DBX_Admin	16		type:OSINT tlp:green	27		admin@admin.test	2014-10-30	OSINT Black Energy 2 malware analysis blog post by Joseph Mlodzianowski	All	
✓	CthulhuSPRL.be	DBX_Admin	17		type:OSINT tlp:green	32	3	admin@admin.test	2014-11-13	OSINT Expansion on Rotten Tomato campaign	All	
✓	CthulhuSPRL.be	DBX_Admin	18	Threat Actor Turla Group	type:OSINT tlp:green	53	6	admin@admin.test	2014-11-13	OSINT Expansion on Snake	All	
✓	CthulhuSPRL.be	DBX_Admin	19		type:OSINT tlp:green	70	14	admin@admin.test	2014-11-12	OSINT Korplug military targeted attacks: Afghanistan & Tajikistan blog post from ESET	All	

MISP - Events

Deling – hvor langt:
- Your organisation only
- This community only
- Connected communities
- All communities

Dato



Trussels Niveau:
- Low
- Medium
- High

NB. Bruges ikke rigtig længere

Status:
- Initial
- Ongoing
- Completed

- Navn

NB. Vigtigt at man bruger et sigende navn – Ikke et sagsbehandling nummer

- Sammenhængende events

MISP - Events


View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Add Event Report
Populate from...
Enrich Event
Merge attributes from...
Publish Event
Publish (no email)
Delegate Publishing
Contact Reporter
Download as...
List Events
Add Event
Ransomware Incident - 23092021.001
Event ID 1227
UUID 004e07da-4b62-4b6a-9bd1-ed0e186410aa
Creator org DBX_Admin
Owner org DBX_Admin
Creator user admin@admin.test
Tags
Date 2021-09-23
Threat Level High
Analysis Initial
Distribution Your organisation only
Info Ransomware Incident - 23092021.001
Published No
#Attributes 0 (0 Objects)
First recorded change
Last change 2021-09-23 10:27:58
Modification map
Sightings 0 (0) - restricted to own organisation only.
+Pivots +Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports +Attributes +Discussion

- View Event
- View Correlation Graph
- View Event History
- Edit Event
- Delete Event
- Add Attribute
- Add Object
- Add Attachment
- Add Event Report
- Populate from...
- Enrich Event
- Merge attributes from...
- Publish Event
- Publish (no email)
- Delegate Publishing
- Contact Reporter
- Download as...
- List Events
- Add Event

Add Attribute

Category (choose one)

Type (choose category first)

Distribution Inherit event

Value

Contextual Comment

- [ ] For Intrusion Detection System
- [ ] Batch Import
- [ ] Disable Correlation

First seen date

Last seen date

First seen time HH:MM:SS.ssssss+TT:TT

Expected format: HH:MM:SS.ssssss+TT:TT

Last seen time HH:MM:SS.ssssss+TT:TT

Expected format: HH:MM:SS.ssssss+TT:TT

Submit

MISP - Attributes

Category

- Antivirus detection
- Artifacts dropped
- Attribution
- External analysis
- Financial fraud
- Internal reference
- Network activity
- Other
- Payload delivery
- Payload installation
- Payload type
- Persistence mechanism
- Person
- Social network
- Support Tool
- Targeting data

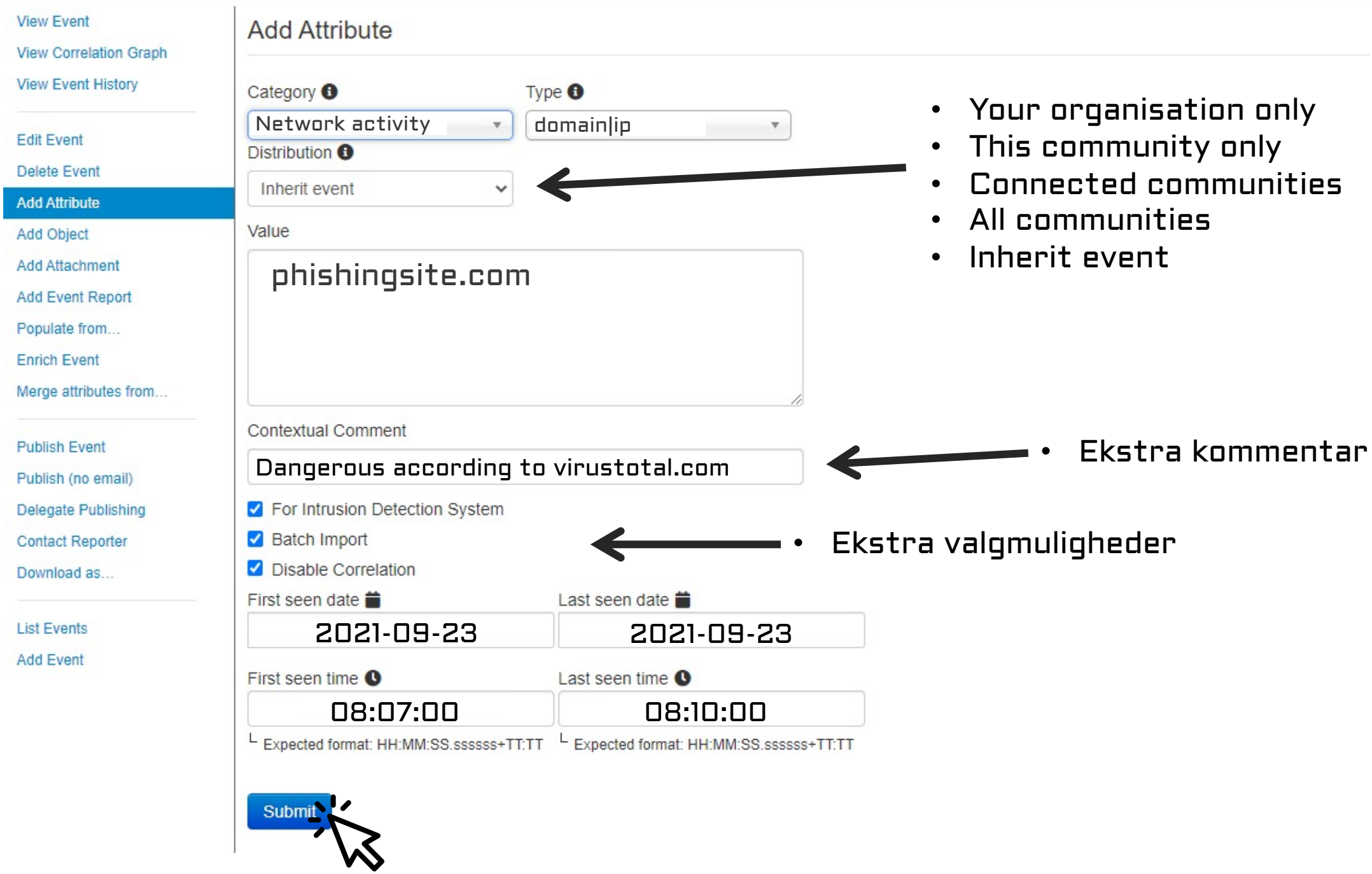
Type

- domain
- domain|ip
- hostname
- ip-dst
- ip-dst|port
- ip-src
- ip-src|port
- md5
- sha1
- sha256
- sha512
- url
- Mange flere...

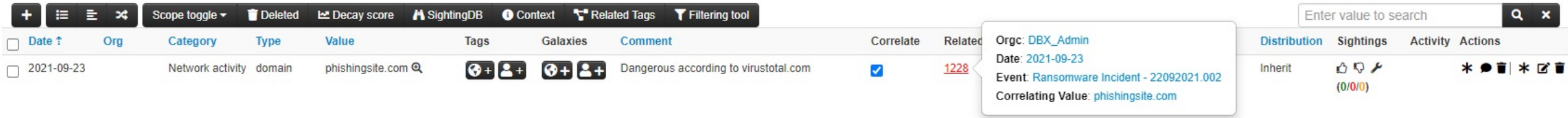
MISP - Attributes

Type

- AS
- anonymised
- attachment
- bro
- comment
- community-id
- cookie
- dkim
- dkim-signature
- domain
- domain|ip
- email
- email-dst
- email-src
- email-subject
- eppn
- favicon-mmh3
- hassh-md5
- hasshserver-md5
- hex
- hostname
- hostname|port
- http-method
- ip-dst
- ip-dst|port
- ip-src
- ip-src|port
- ja3-fingerprint-md5
- jarm-fingerprint
- mac-address
- mac-eui-64
- other
- pattern-in-file
- pattern-in-traffic
- port
- snort
- stix2-pattern
- text
- uri
- url
- user-agent
- x509-fingerprint-md5
- x509-fingerprint-sha1
- x509-fingerprint-sha256
- zeek

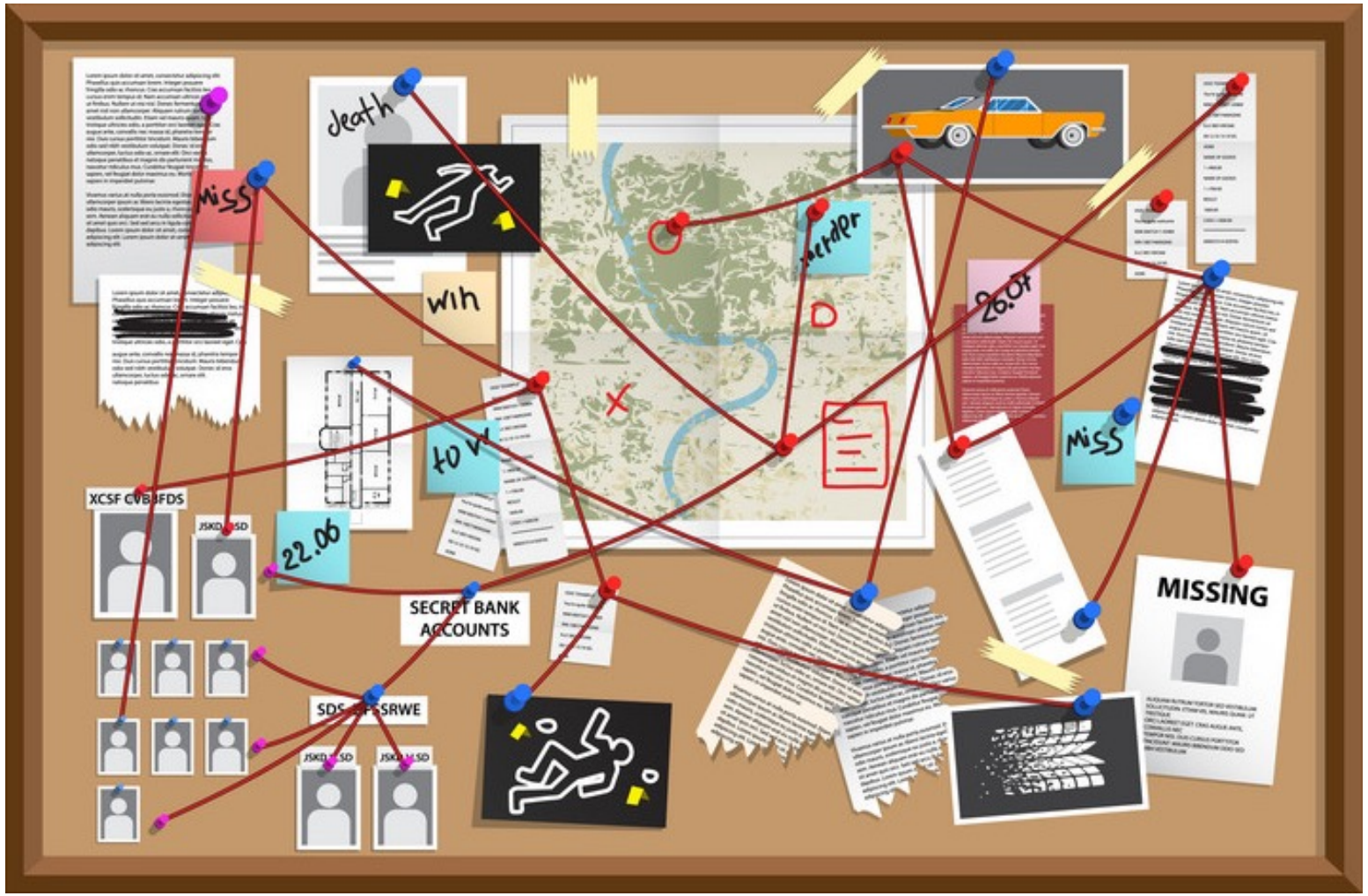

View Event
View Correlation Graph
View Event History
Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Add Event Report
Populate from...
Enrich Event
Merge attributes from...
Publish Event
Publish (no email)
Delegate Publishing
Contact Reporter
Download as...
List Events
Add Event
Add Attribute
Category
Network activity
Type
domain|ip
Distribution
Inherit event
Value
phishingsite.com
Contextual Comment
Dangerous according to virustotal.com
For Intrusion Detection System
Batch Import
Disable Correlation
First seen date
2021-09-23
Last seen date
2021-09-23
First seen time
08:07:00
Last seen time
08:10:00
Expected format: HH:MM:SS.ssssss+TT:TT
Expected format: HH:MM:SS.ssssss+TT:TT
Submit
• Your organisation only
• This community only
• Connected communities
• All communities
• Inherit event
• Ekstra kommentar
• Ekstra valgmuligheder

MISP - Attributes



MISP

- Skaber sammenhæng i data
- Grupperer attributter
- Giver et overblik



MISP ER AWESOME

MISP - In the beginning of times

Before June 2011

MISP
Threat Sharing

Livet inden MISP

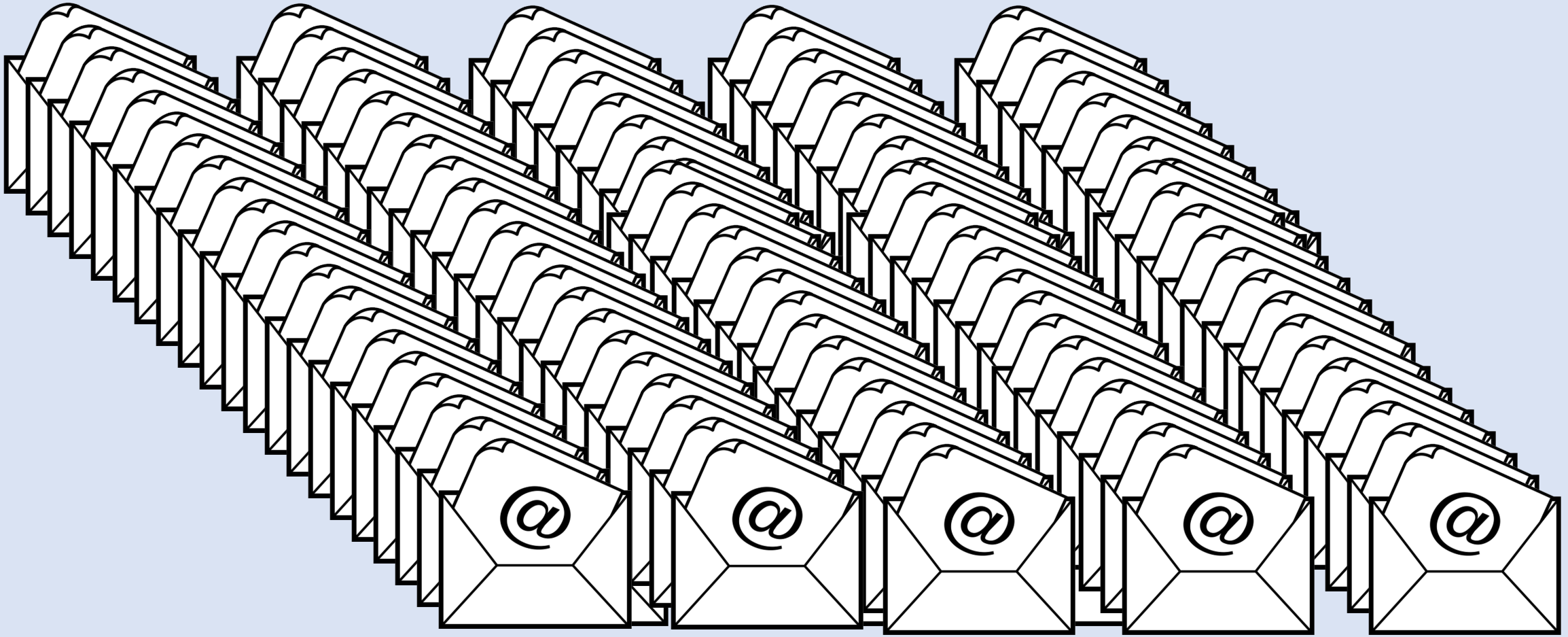
IT Trussel

Christopher

Sharing is caring


=
Karsten
Email
Livet inden MISP

Livet inden MISP




Not on the list.
Stop

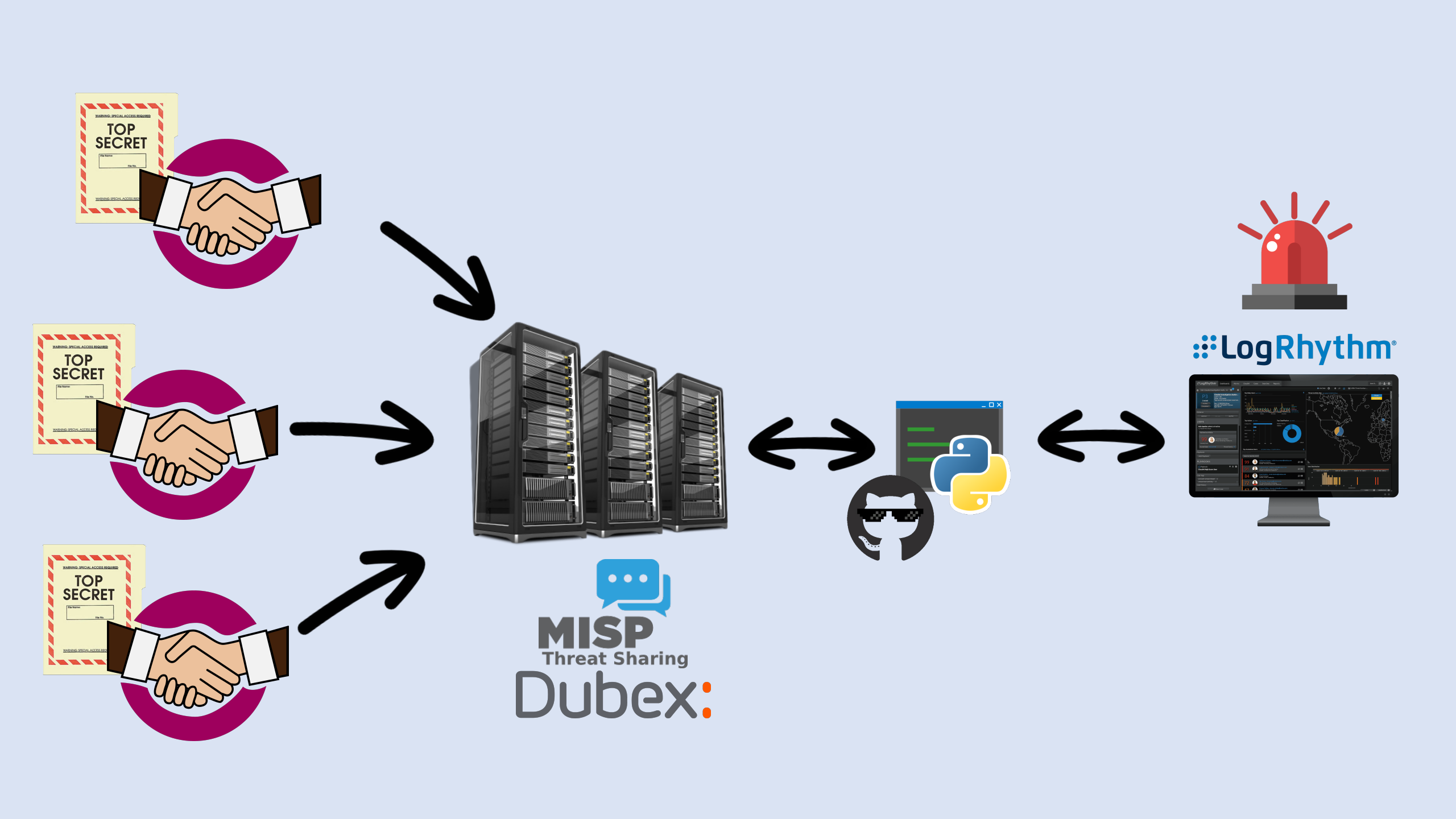
Livet inden MISP

Work smarter - Not harder

MISP

Threat Sharing

Dubex:


TOP SECRET
TOP SECRET
TOP SECRET
MISP
Threat Sharing
Dubex:
LogRhythm

Python Script

```
┌──(kpp㉿DBX_MISP)-[/MISP_Code]
└─$
```

View Event
View Correlation Graph
View Event History

Edit Event
Delete Event
Add Attribute
Add Object
Add Attachment
Add Event Report
Populate from...
Enrich Event
Merge attributes from...

Publish Event
Publish (no email)
Delegate Publishing
Contact Reporter
Download as...

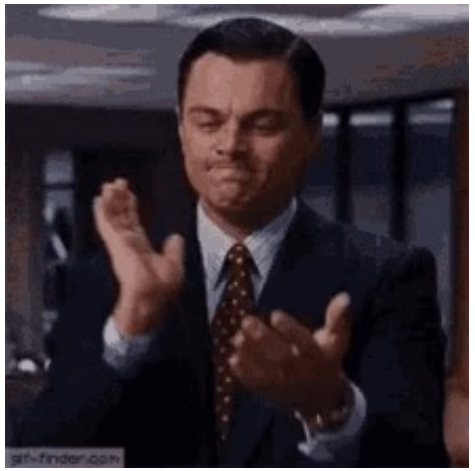
List Events
Add Event

Ransomware Incident - 13092021.001

Event ID	1223
UUID	8266583a-601c-467d-9734-50d6acfba888
Creator org	DBX_Admin
Owner org	DBX_Admin
Creator user	admin@admin.test
Tags	DBX: LR Sync x
Date	2021-09-13
Threat Level	High
Analysis	Initial
Distribution	Your organisation only
Info	Ransomware Incident - 13092021.001
Published	No
#Attributes	2 (0 Objects)
First recorded change	2021-09-13 12:46:57
Last change	2021-09-21 14:53:00
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Related Events

DB... Ransomware Incident - 06082021.001
2021-08-09 **1**



−Pivots −Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports −Attributes −Discussion

× 1223: Ransomware...

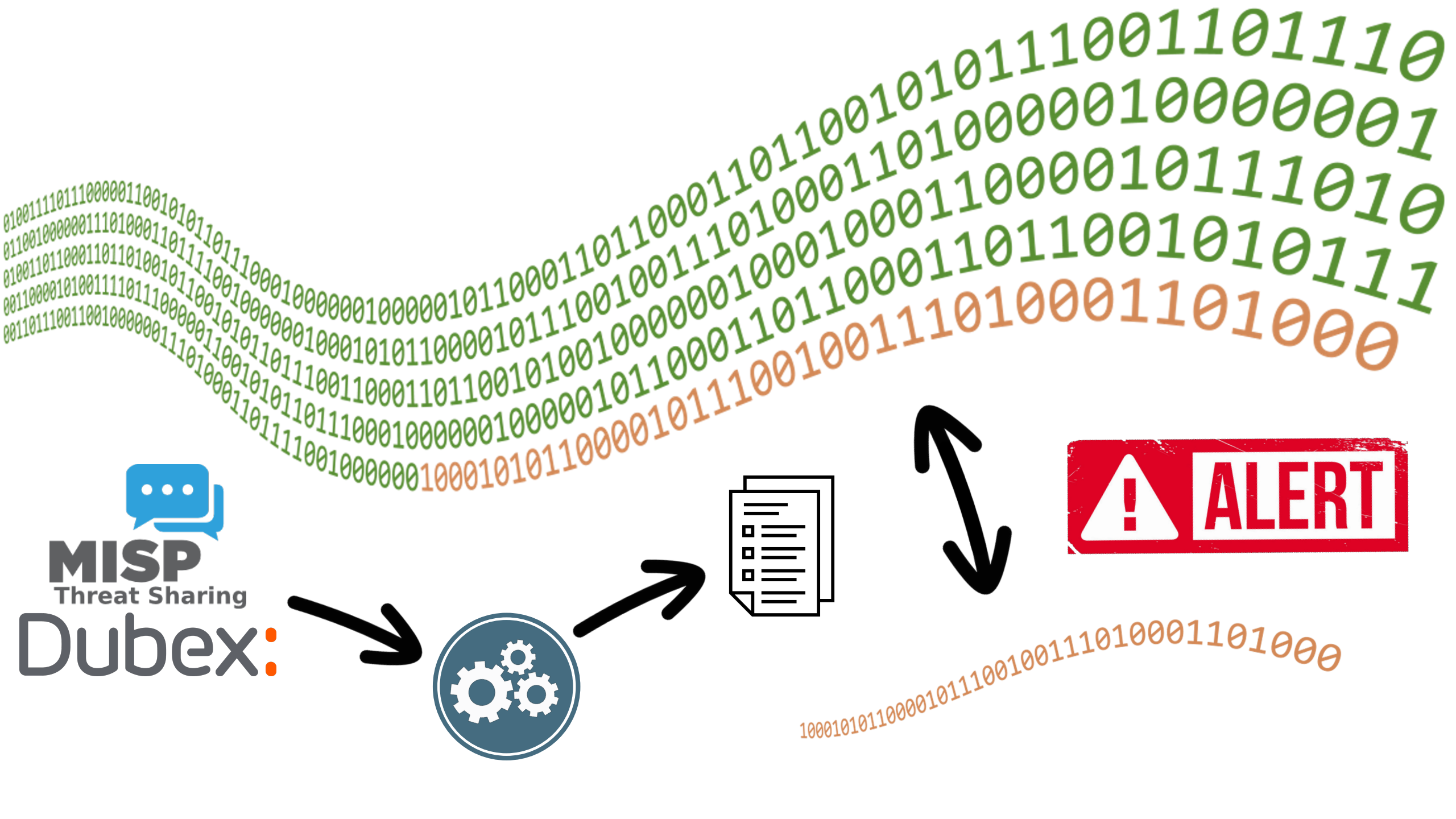
Galaxies

« previous | next » | view all

Hacker

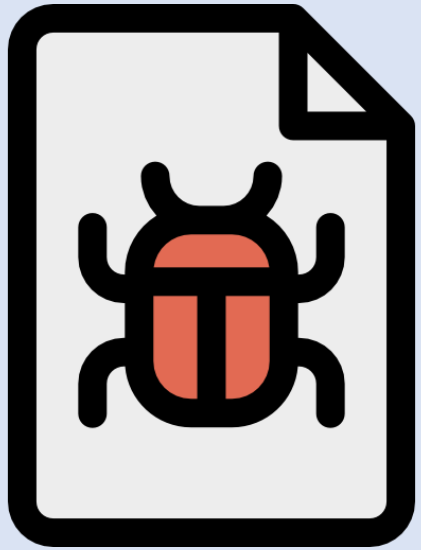
Angreb

Dubex kunder


MISP
Threat Sharing
Dubex:
ALERT

MISP DIRT

- Søgning på malware



- SHA256
- 16d007d650d117c68da0057
  47378f16cebe820e75a2565b
  e70602fad2cb6e1fe

- MD5
  9afcbf6f4f13a40791d368df76
  7b4304

List Events
Add Event
Import from...
REST client

List Attributes
Search Attributes

View Proposals
Events with proposals
View delegation requests

Export
Automation

Search Attribute

You can search for attributes based on contained expression within the value, event ID, submitting organisation, category and type.
For the value, event ID and organisation, you can enter several search terms by entering each term as a new line. To exclude things from a result, use the NOT operator (!) in front of the term.
For string searches (such as searching for an expression, tags, etc) - lookups are simple string matches. If you want a substring match encapsulate the lookup string between "%" characters.

Containing the following expressions

9afcbf6f4f13a40791d368df767b4304

Having tag or being an attribute of an event having the tag

Being attributes of the following event IDs, event UUIDs or attribute UUIDs

From the following organisation(s)

Type: ALL

Category: ALL

☐ Only find IOCs flagged as to IDS ☐ Alternate Search Result (Events)

First seen and Last seen

Attributes not having first seen or last seen set might not appear in the search

First seen date | Last seen date | Submit

First seen time: HH:MM:SS.ssssss+TT:TT
└ Expected format: HH:MM:SS.ssssss+TT:TT

Last seen time: HH:MM:SS.ssssss+TT:TT
└ Expected format: HH:MM:SS.ssssss+TT:TT

List Events
Add Event
Import from...
REST client

List Attributes
Search Attributes

Download as...

View Proposals
Events with proposals
View delegation requests

Export
Automation

Attributes

Results for all attributes with the value containing 9afcbf6f4f13a40791d368df767b4304

« previous | next »

Date	Event	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2019-10-07	1137	MISOC	Artifacts dropped	**malware-sample:** malware-sample	pixelproc.exe 9afcbf6f4f13a40791d368df767b4304		Tool Emotet		☑			☑	Inherit	(0/0/0)		
2019-10-07	1137	MISOC	Artifacts dropped	**md5:** md5	9afcbf6f4f13a40791d368df767b4304				☑			☑	Inherit	(0/0/0)		

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

« previous | next »

2019-10-07	Artifacts dropped	**sha1:** sha1	10dae0bced984456d3d7a2b059cd71a4762f1c5b	☑	☑	Inherit	(0/0/0)		
2019-10-07	Artifacts dropped	**sha256:** sha256	4cbe34dc9928a6b93786a69bea92b3df0e04fd67d116fc1746d817496314de9e	☑	☑	Inherit	(0/0/0)		
2019-10-07	Other	**size-in-bytes:** size-in-bytes	393309						
2019-10-07	**Object name: file** **References: 0**								
2019-10-07	Artifacts dropped	**malware-sample:** malware-sample	pixelproc.exe 9afcbf6f4f13a40791d368df767b4304						
2019-10-07	Artifacts dropped	**filename:** filename	pixelproc.exe						
2019-10-07	Artifacts dropped	**md5:** md5	9afcbf6f4f13a40791d368df767b4304						
2019-10-07	Artifacts dropped	**sha1:** sha1	019a178ee95b34980a2f07ee624528de5f4eae44						
2019-10-07	Artifacts dropped	**sha256:** sha256	16d007d650d117c68da005747378f16cebe820e75a2565be70602fad2cb6e1fe						
2019-10-07	Other	**size-in-bytes:** size-in-bytes	221184						
2019-10-07	**Object name: file** **References: 0**								
2019-10-07	Payload delivery	**malware-sample:** malware-sample	26017e97acce09276f3b4c6800dec256_unzipped_decoded.zip 0e8c5174646dcd87ac893271b80c9633						
2019-10-07	Network activity	url	https://drewnianazagroda.pl/c0nm/PtlOolWOzs/						
2019-10-07	Network activity	url	https://edealsadvisor.com/wp-includes/ZqLAroEkK/						
2019-10-07	Network activity	url	https://kurumsalinternetsitesi.com/wp-content/wgSCKDCIY/						
2019-10-07	Network activity	url	http://latestgovernment.com/pramodchoudhary.examqualify.com/CKBOIhWtjs/						

Lookup results:

Hashdd:

Error: Enrichment service not reachable.

Yara Query:

import "hash" rule SHA256 { condition: hash.sha256(0, filesize) == "16d007d650d117c68da005747378f16cebe820e75a2565be70602fad2cb6e1fe" }

Urlhaus:

Object: virustotal-report

detection-ratio	7 / 69
permalink	https://www.virustotal.com/file/16d007d650d117c68da005747378f16cebe820e75a2565be70602fad2cb6e1fe/analysis/1570466330/

Object: file

md5	9afcbf6f4f13a40791d368df767b4304
size-in-bytes	221184
filename	ifbikhtz9_0155945363.exe
filename	p1mdraces_117620674.exe
filename	auy_9704598196.exe
filename	h_934554.exe
filename	r_0410503297.exe
filename	a5kgay_90.exe
filename	k0hv_940.exe
filename	mc6_9126.exe
filename	jn_389.exe
filename	y0uf3hf8_62079.exe
filename	z_3.exe
filename	4 305949977.exe

16d007d650d117c68da005747378f16cebe820e75a2565be70602fad2cb6e1fe

Sign in | Sign up

58 / 70

Community Score

58 security vendors and 3 sandboxes flagged this file as malicious

16d007d650d117c68da005747378f16cebe820e75a2565be70602fad2cb6e1fe
udb7n_051.exe
invalid-rich-pe-modified-iat | peexe

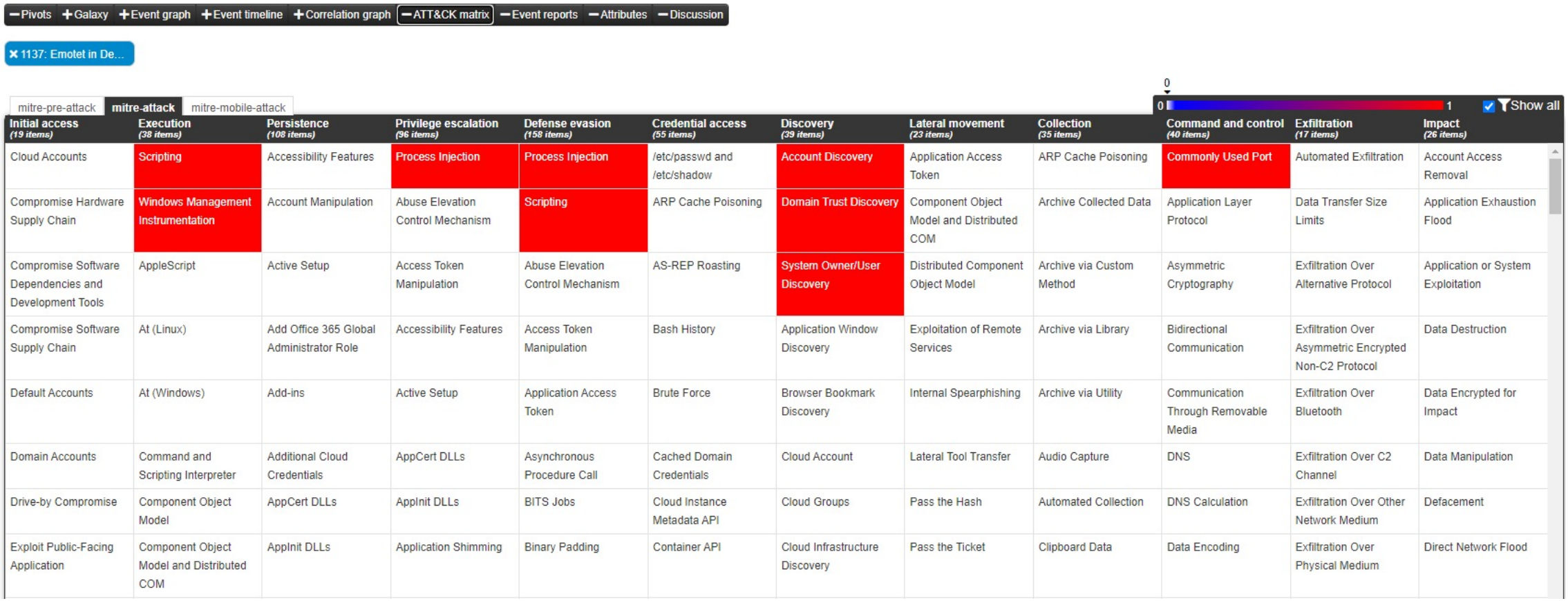
216.00 KB
Size

2020-11-26 06:16:56 UTC
10 months ago

EXE

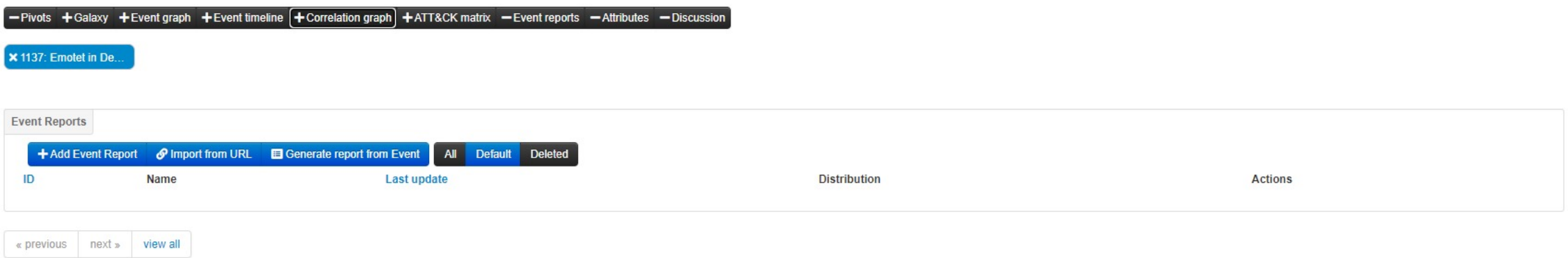
DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 9

Ad-Aware	Trojan.Autoruns.GenericKD.32673732	AegisLab	Trojan.Win32.Emotet.tqPK
AhnLab-V3	Malware/Win32.Generic.C3505079	Alibaba	Trojan:Win32/Emotet.554a86e2
ALYac	Trojan.Agent.Emotet	Antiy-AVL	Trojan[Banker]/Win32.Emotet
SecureAge APEX	Malicious	Arcabit	Trojan.Autoruns.Generic.D1F28FC4
Avast	Win32:MalwareX-gen [Trj]	AVG	Win32:MalwareX-gen [Trj]
Avira (no cloud)	TR/AD.Emotet.ownoz	BitDefender	Trojan.Autoruns.GenericKD.32673732
BitDefenderTheta	Gen:NN.ZexaF.34658.nqW@aKr9iTdi	Bkav Pro	W32.AIDetectVM.malware1
Comodo	Malware@#29ib41qfm3mjd	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 85)
Cyren	W32/Kryptik.AHW.gen!Eldorado	DrWeb	Trojan.Siggen8.50640
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Emotet (A)



Initial access (19 items)	Execution (38 items)	Persistence (108 items)	Privilege escalation (96 items)	Defense evasion (158 items)	Credential access (55 items)	Discovery (39 items)	Lateral movement (23 items)	Collection (35 items)	Command and control (40 items)	Exfiltration (17 items)	Impact (26 items)
Cloud Accounts	Scripting	Accessibility Features	Process Injection	Process Injection	/etc/passwd and /etc/shadow	Account Discovery	Application Access Token	ARP Cache Poisoning	Commonly Used Port	Automated Exfiltration	Account Access Removal
Compromise Hardware Supply Chain	Windows Management Instrumentation	Account Manipulation	Abuse Elevation Control Mechanism	Scripting	ARP Cache Poisoning	Domain Trust Discovery	Component Object Model and Distributed COM	Archive Collected Data	Application Layer Protocol	Data Transfer Size Limits	Application Exhaustion Flood
Compromise Software Dependencies and Development Tools	AppleScript	Active Setup	Access Token Manipulation	Abuse Elevation Control Mechanism	AS-REP Roasting	System Owner/User Discovery	Distributed Component Object Model	Archive via Custom Method	Asymmetric Cryptography	Exfiltration Over Alternative Protocol	Application or System Exploitation
Compromise Software Supply Chain	At (Linux)	Add Office 365 Global Administrator Role	Accessibility Features	Access Token Manipulation	Bash History	Application Window Discovery	Exploitation of Remote Services	Archive via Library	Bidirectional Communication	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Data Destruction
Default Accounts	At (Windows)	Add-ins	Active Setup	Application Access Token	Brute Force	Browser Bookmark Discovery	Internal Spearphishing	Archive via Utility	Communication Through Removable Media	Exfiltration Over Bluetooth	Data Encrypted for Impact
Domain Accounts	Command and Scripting Interpreter	Additional Cloud Credentials	AppCert DLLs	Asynchronous Procedure Call	Cached Domain Credentials	Cloud Account	Lateral Tool Transfer	Audio Capture	DNS	Exfiltration Over C2 Channel	Data Manipulation
Drive-by Compromise	Component Object Model	AppCert DLLs	AppInit DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Groups	Pass the Hash	Automated Collection	DNS Calculation	Exfiltration Over Other Network Medium	Defacement
Exploit Public-Facing Application	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Binary Padding	Container API	Cloud Infrastructure Discovery	Pass the Ticket	Clipboard Data	Data Encoding	Exfiltration Over Physical Medium	Direct Network Flood


Pivots
Galaxy
Event graph
Event timeline
Correlation graph
ATT&CK matrix
Event reports
Attributes
Discussion
1137: Emotet in De...
Time scope
Display
Timezone: : +02:00
Select an Option
ip-port
dst-port 443
ip 91.200.102.245
http://45.123.3.54/site/
http://45.123.3.54/badge/
http://201.184.105.242/ban/
http://201.184.105.242/cone/dma/arizona/
http://201.184.105.242/health/
http://201.184.105.242/iplk/enable/loadan/
http://201.184.105.242/loadan/
http://201.184.105.242/sess/pnp/ringin/merge/
https://github.com/Hestat/intel-sharing/blob/master/powershell-e[...]
21
26
1
6
11
16
21
26
1
6
11
16
21
26
1
6
11
16
21
26
September 2019
October 2019
November 2019
December 2019
?


Pivots
Galaxy
Event graph
Event timeline
Correlation graph
ATT&CK matrix
Event reports
Attributes
Discussion
1137: Emotet in De...
Event Reports
Add Event Report
Import from URL
Generate report from Event
All
Default
Deleted
ID
Name
Last update
Distribution
Actions
« previous
next »
view all


Are We THERE Yet?

MISP i Danmark

#SammenSikrerViDanmark

MISP
Threat Sharing

Kendte fællesskaber:

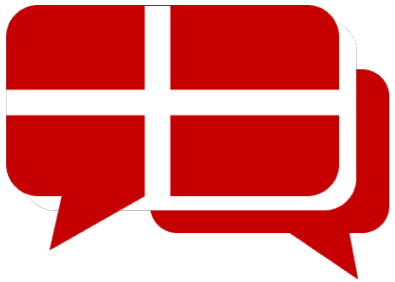
- DKCert
- Tele-DCIS
- Nordic Financial CERT (NFCERT)
- Sundhedssikringstyrelsen CERT
- EnergiCERT
- eCrimelabs (Danish MISP community)
- ”Invite only” I de forskellige brancher

CERT (Computer Emergency Response Team)

Tak for jeres opmærksomhed!

Dubex:

MANAGING RISK. ENABLING GROWTH.



MISP

Threat Sharing

#SammenSikrerViDanmark

/danishmisp

Nyt projekt!

INDSAMLING AF THREAT INTEL MED HONEYPOTS

Spørgsmål?

Dubex:

MANAGING RISK. ENABLING GROWTH.

#SammenSikrerViDanmark

KPP@dubex.dk

@KimHot

/in/kimppedersen/

@KimHotDK