Inzichten in Cyber Threat Intelligence

De sleutel tot Proactieve Cyberbeveiliging

Melvin Koelewijn

SURF Security- en Privacyconferentie

27 Juni 2024

Introductie

Melvin Koelewijn

Team Security Techniek

Melvin.Koelewijn@SURF.nl

Agenda

01
Threat actoren & APT’s

02
Cyber Threat Intelligence

03
Wat doet SURF(cert)?

04
Wat kun je als instelling doen?

05
Vragen?

Threat Actoren

- **Script kiddies – (Larven)**
  - Nieuwsgierigheid, uitdaging, het verkrijgen van reputatie binnen een peer groep
- **Hacktivists – (Jackals)**
  - Politieke of sociale verandering, promoten van een agenda
- **Cybercriminals – (Spiders)**
  - Financiële winst (Ransomware / Afpersing)
- **Cyber Espionage groeperingen – (Bear's, Panda's…)**
  - Inlichtingenwinst voor strategisch voordeel
- **Nation-state actors – (APT's)**
  - Politieke of economische voordelen, militaire strategie, spionage
- **Insiders… Terroristen… Concurrenten…**

Advanced Persistent Threat (APT)

- **Advanced:** Gebruik van geavanceerde technieken en middelen, waaronder zero-day exploits, geavanceerde malware, en complexe aanvallen
- **Persistent:** Langdurige aanwezigheid in het doelwitnetwerk, vaak maanden of jaren, waarbij de aanvallers geduldig en methodisch te werk gaan om hun doelen te bereiken.
- **Threat:** Duidelijke intentie en vermogen om aanzienlijke schade aan te richten, zoals het stelen van gevoelige gegevens, verstoren van operaties, of sabotage.

- In de meeste gevallen een **Nation-State** (gesupporterde) **actor**…

➢ **APT1 (Comment Panda):** Geassocieerd met Chinese militaire eenheden.

➢ **APT28 (Fancy Bear)**: Geassocieerd met Russische militaire inlichtingendiensten.

➢ **APT33 (Refined Kitten)**: Geassocieerd met Iraanse overheid.

Threat Actor Naming Conventions

- De meest prominente naam is de **Advanced Persistent Threat (APT).** In 2013 is de eerste APT groep benoemd door Mandiant: **APT1 –** China's Cyber Espionage PLA Unit 61398
- Bijna elke Threat Intel partij gebruikt een eigen benaming voor threat actors…

- Malpedia: 703 threat actor namen

➢ https://malpedia.caad.fkie.fraunhofer.de/actors

- Mitre: 152 threat actor namen

➢ https://attack.mitre.org/groups/

APT40

Article Talk

From Wikipedia, the free encyclopedia

APT40, also known as **BRONZE MOHAWK** (by Secureworks),[1] **FEVERDREAM**, **G0065**, **GADOLINIUM** (formerly by Microsoft),[2] **Gingham Typhoon**[3] (by Microsoft), **GreenCrash**, **Hellsing** (by Kaspersky),[4] **Kryptonite Panda** (by Crowdstrike), **Leviathan** (by Proofpoint),[5] **MUDCARP**, **Periscope**, **Temp.Periscope**, and **Temp.Jumper**, is an advanced persistent threat located in Haikou, Hainan Province, People's Republic of China (PRC), and has been active since at least 2009. APT40 has targeted governmental organizations, companies, and universities in a wide range of industries, including biomedical, robotics, and maritime research, across the United States, Canada, Europe, the Middle East, and the South China Sea area, as well as industries included in China's Belt and Road Initiative.[6] APT40 is closely connected to Hafnium.[7]

Bron: *https://en.wikipedia.org/wiki/APT40*

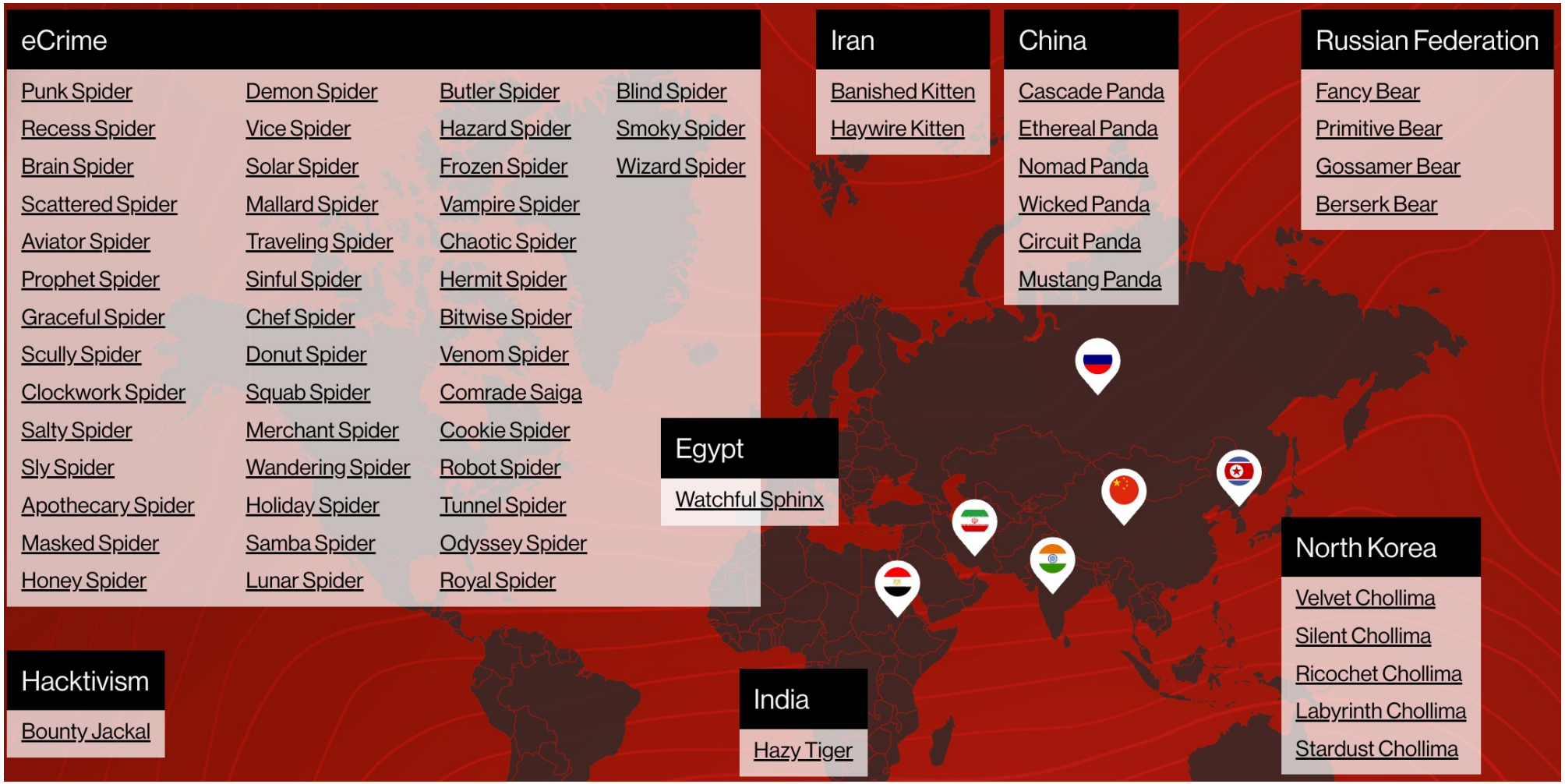
Threat Actor Naming Conventions - Microsoft

Blizzard **Russia**	Typhoon **China**	Sandstorm **Iran**	Sleet **North Korea**	Dust **Turkey**	Cyclone **Vietnam**
Rain **Lebanon**	Hail **South Korea**	Tempest **Financially motivated**	Tsunami **Private sector offensive actor**	Flood **Influence operations**	Storm **Groups in development**

***Bron**: https://learn.microsoft.com/en-us/microsoft-365/media/threat-actor-naming/threat-actor-categories-lg.png*

SURF

Threat Actor Naming Conventions - CrowdStrike



Bron: https://www.crowdstrike.com/adversaries/

Russia designates US government as APT Sand Eagle, claims it launched attack on Russian devices

Cyber security firms in Russia have assigned the US government its very own advanced persistent threat (APT) designation after claiming it or government agencies had launched attacks against Russian Federation targets.

Daniel Croft • Mon, 11 Mar 2024 • **SECURITY**

SHARE

Russian intelligence firms are reportedly referring to the US government as "Sand Eagle", according to a document shared by @vxunderground on X (formerly Twitter).

> **Russia-based Cyber Threat Intelligence firms have an APT name designated for the United States government: Sand Eagle pic.twitter.com/4eLuaE1lwJ**
>
> — vx-underground (@vxunderground) March 7, 2024

SURF

Bron: https://www.cyberdaily.au/security/10299-russia-designates-us-government-as-apt-sand-eagle-claims-it-launched-attack-on-russian-devices

R&E Sector Threat Actors

Ongeveer 25% van de threat actors hebben als target categorie: ‘Education’ of ‘Healthcare’

Threat actors die de afgelopen jaren binnen onze sector actief zijn geweest:

- Vice Society (sinds juni 2023: Rhysida)
- Silent Librarian
- TA505 – Clop Ransomware
- APT10 / Stone Panda
- APT29 / Cozy Bear

Succesvolle Ransomware aanvallen (RaaS):

- DoppelPaymer
- LockBit

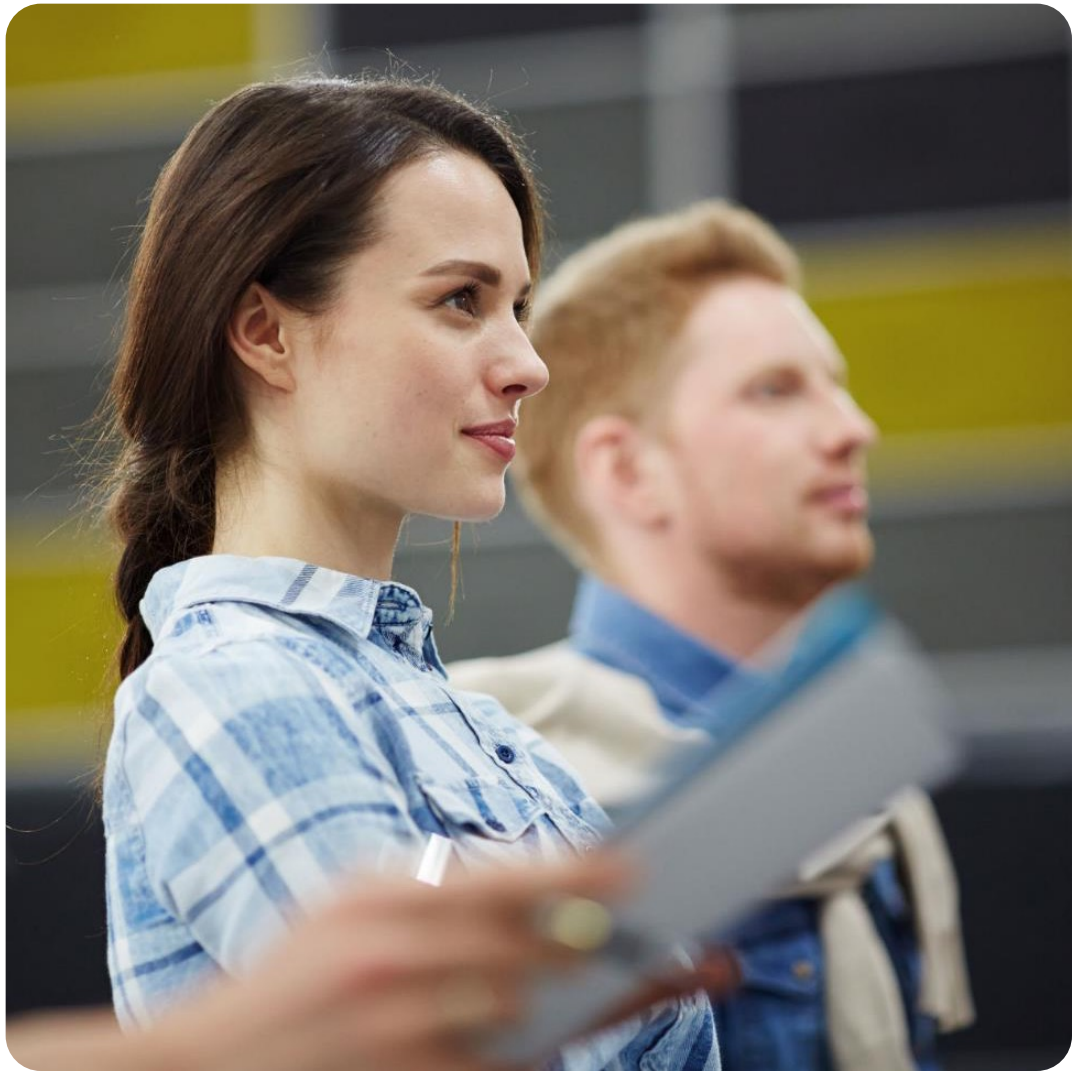
Cyber Threat Intelligence

Dreigingsinformatie in het digitale domein!

Cyber Threat Intelligence (CTI) omvat het verzamelen, analyseren en delen van informatie met betrekking tot cyberdreigingen.

Doel: Organisaties in staat stellen hun veerkracht tegen cyberaanvallen te vergroten door preventieve maatregelen te nemen.

- **Strategisch**
- **Tactisch**
- **Operationeel / Technisch**



Strategisch

CrowdStrike 2024 Global Threat Report

Analyses en informatie over langetermijntrends en ontwikkelingen in digitale veiligheid!

- Dreigingsrapporten en analyses over opkomende cyberdreigingen en trends.
- Analyse van de impact van nieuwe technologische ontwikkelingen, wetgeving of geopolitieke gebeurtenissen op het cyberdreigingslandschap.

CISO’s & Management kunnen hiermee strategische beslissingen nemen.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cybersecuritybeeld Nederland 2023

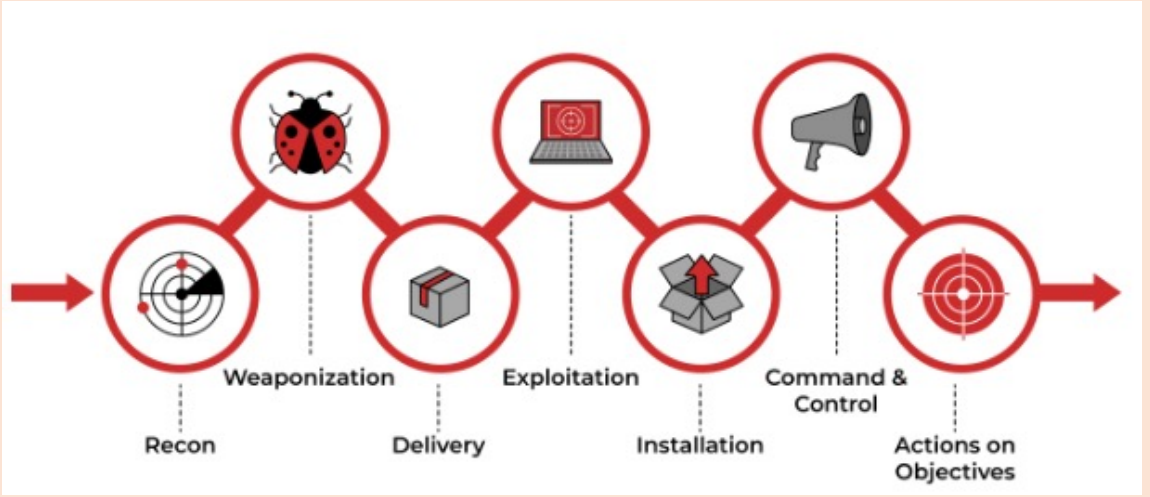
SURF

Tactisch

Identificeren van concrete bedreigingen en het nemen van gerichte maatregelen om deze te neutraliseren of te verminderen!

- Threat actors (APT’s) met een bepaald doel.
- Tactics, Techniques, and Procedures (TTP): informatie hoe aanvallers opereren, welke tools en technieken ze gebruiken.

- ➢ Factsheets SURFcert
- ➢ SURFcert MISP (context bij IoC’s en TTP’s)
- ➢ Security Expertise Centrum



Operationeel / Technisch

Directe ondersteuning van de dagelijkse beveiligingsactiviteiten en incidentrespons!

- SOC | Incident response | malwaredetectie en –analyse | netwerk & host analyse | kwetsbaarheden | threat hunting

Technische informatie:

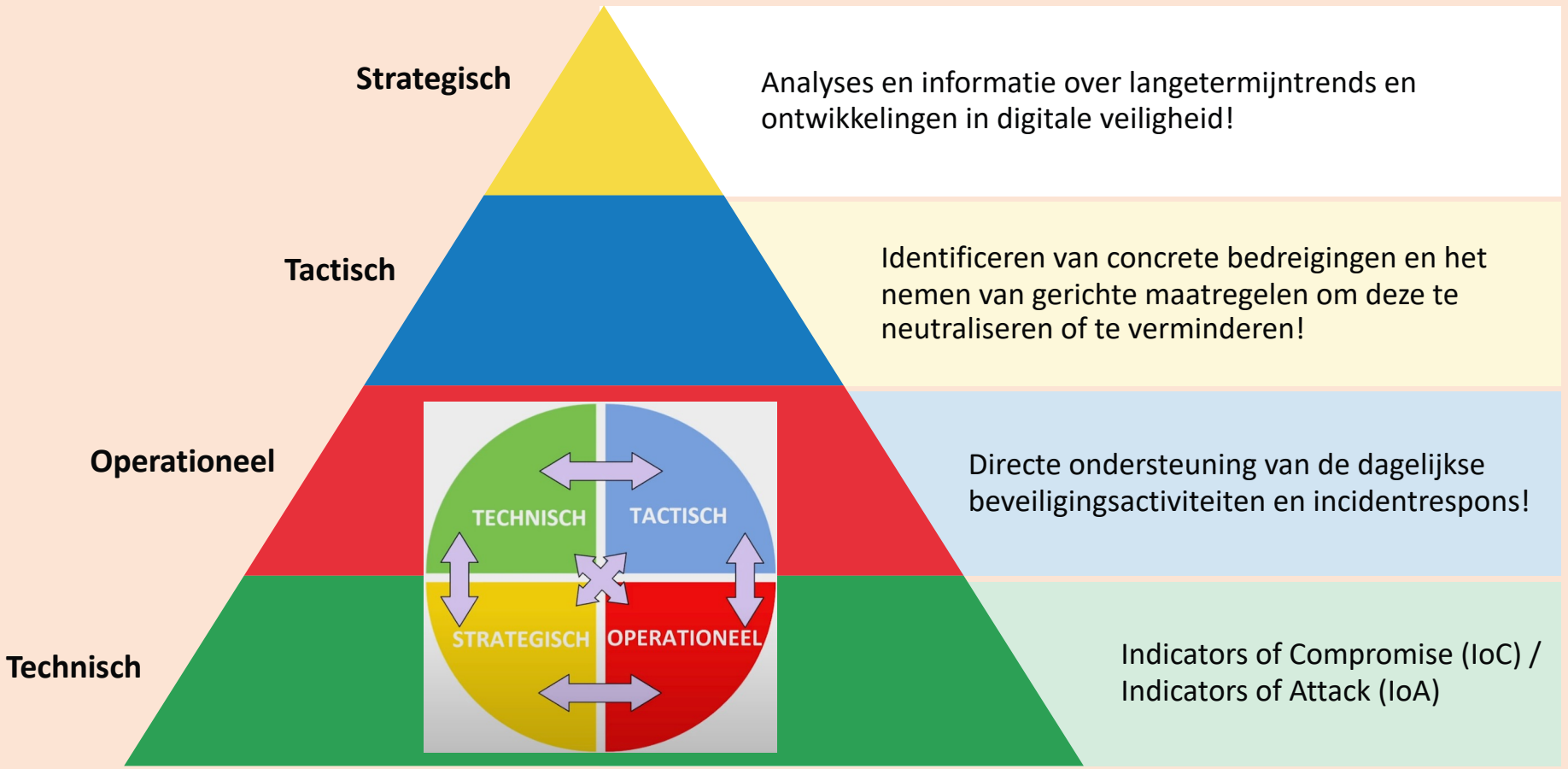
- Indicators of Compromise (IoC) / Indicators of Attack (IoA)
  - O.a: IP's | Domeinen | URL's | Hashes
- Worden verzameld uit actieve campagnes, aanvallen die zijn uitgevoerd op organisaties, of (open source) threat intel feeds.
  - Abuse.ch, Phishtank, The Shadowserver Foundation, The Spamhaus Project, VirustotalShodan.io, Censys.io

SPAMHAUS

SHADOWSERVER

SURF

Overzicht CTI niveaus



CTI initiatieven

Om informatie over cyberdreigingen te verzamelen, analyseren en delen tussen deelnemende organisaties.

Information Sharing and Analysis Center (ISAC)

- Gericht op een specifieke sector of branche en de cyberdreigingsinformatie daarbinnen.
- **Bijv.:** Banken onderling (FI-ISAC) of de haven-ISAC

Information Sharing and Analysis Organization (ISAO)

- Vaak breder dan alleen een specifieke sector en cyberdreigingsinformatie dat algemener geldt. Privaat of publiek.
- **Bijv.:** Het NCSC

Wat doet SURF(cert)?

Threat intel bronnen

- SURF community ’s
- Andere CERT’s

- NCSC - Nationaal Detectie Netwerk
- FIRST / TF-CSIRT
- Andere NRENs

- Eigen Scanning
- Shadowserver
- Cymru
- LeakIX

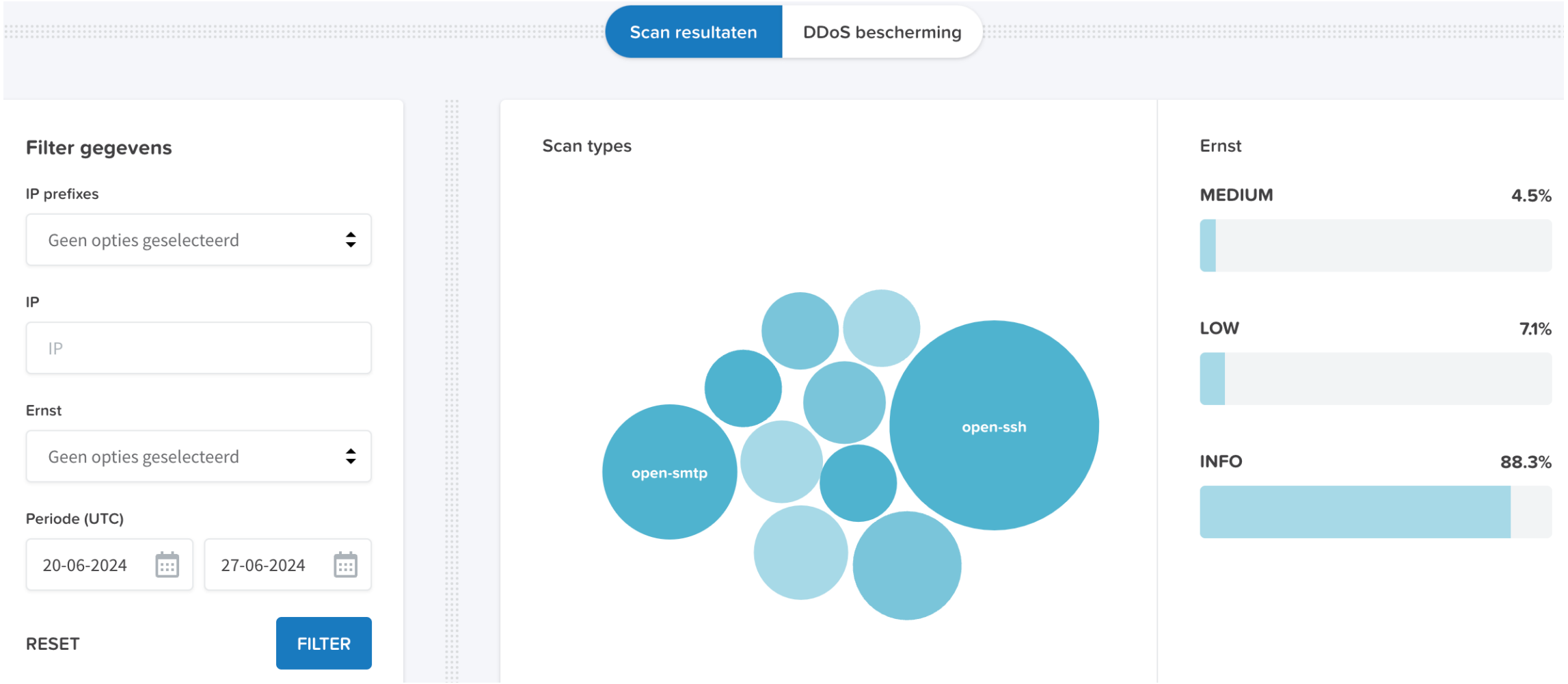
- Incidenten
- Netwerkdashboard

- SCIRT / SCIPR

- MISP

- Netflow
- SURFsoc
- SURFfirewall
- SURF DNS firewall

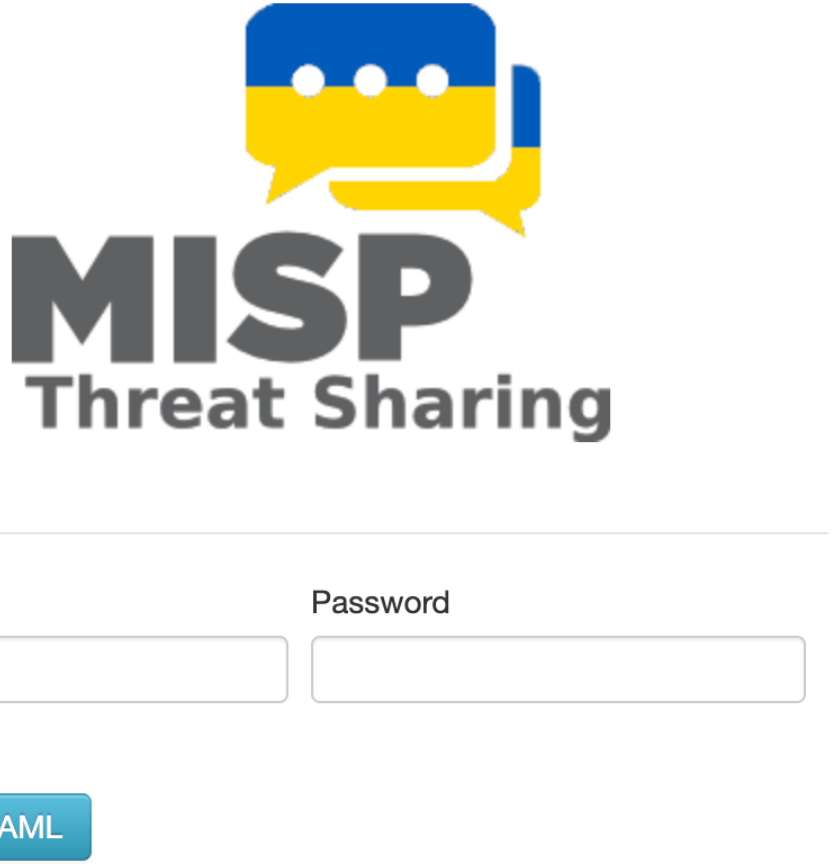
Security (tegel) - Netwerkdashboard

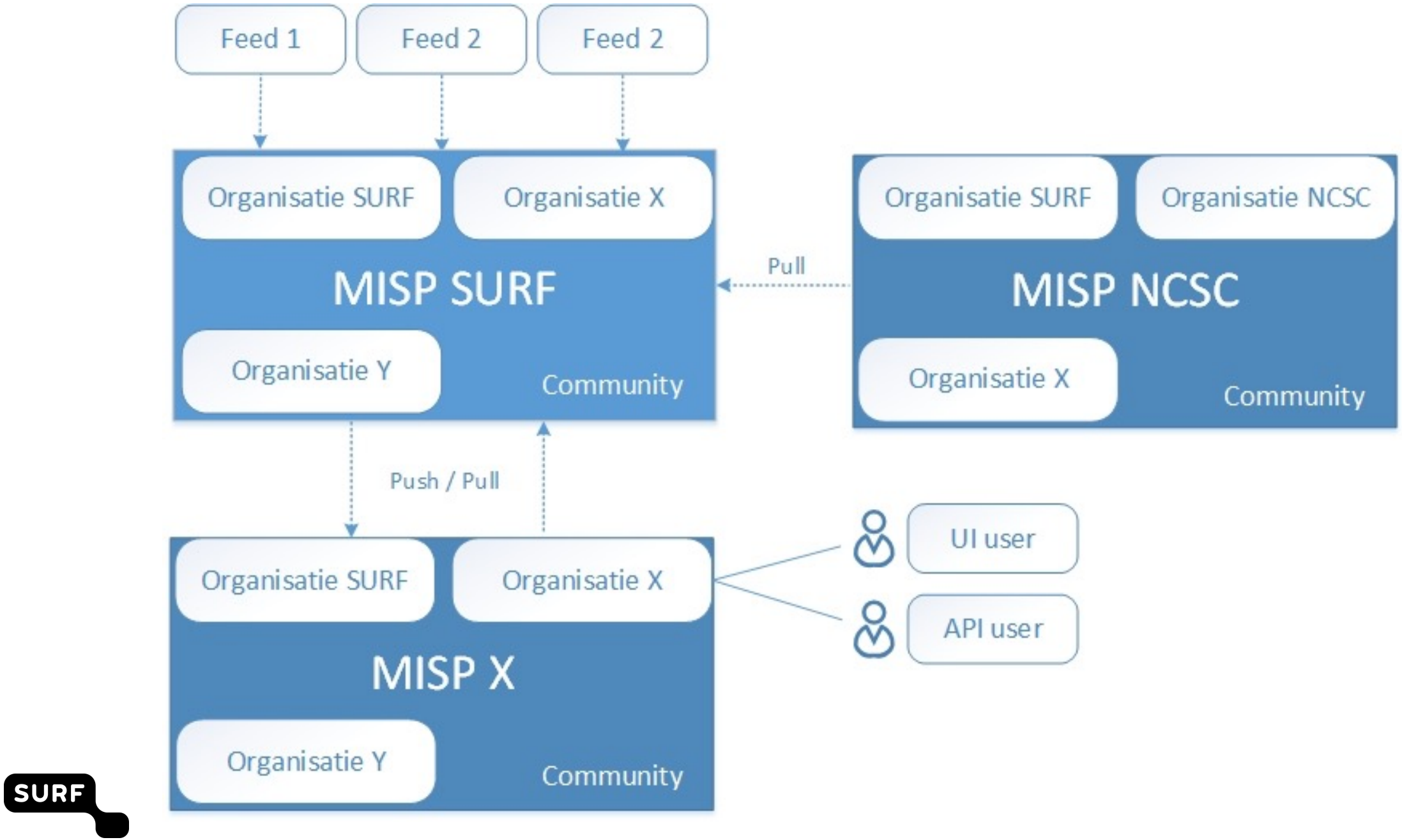


https://netwerkdashboard.surf.nl

Rol nodig in SURF dashboard: Beveiligingsverantwoordelijke

SURFcert MISP




Feed 1
Feed 2
Feed 2
Organisatie SURF
Organisatie X
MISP SURF
Organisatie Y
Community
Pull
Organisatie SURF
Organisatie NCSC
MISP NCSC
Organisatie X
Community
Push / Pull
Organisatie SURF
Organisatie X
MISP X
Organisatie Y
Community
UI user
API user

Geant's GN5.1 Project

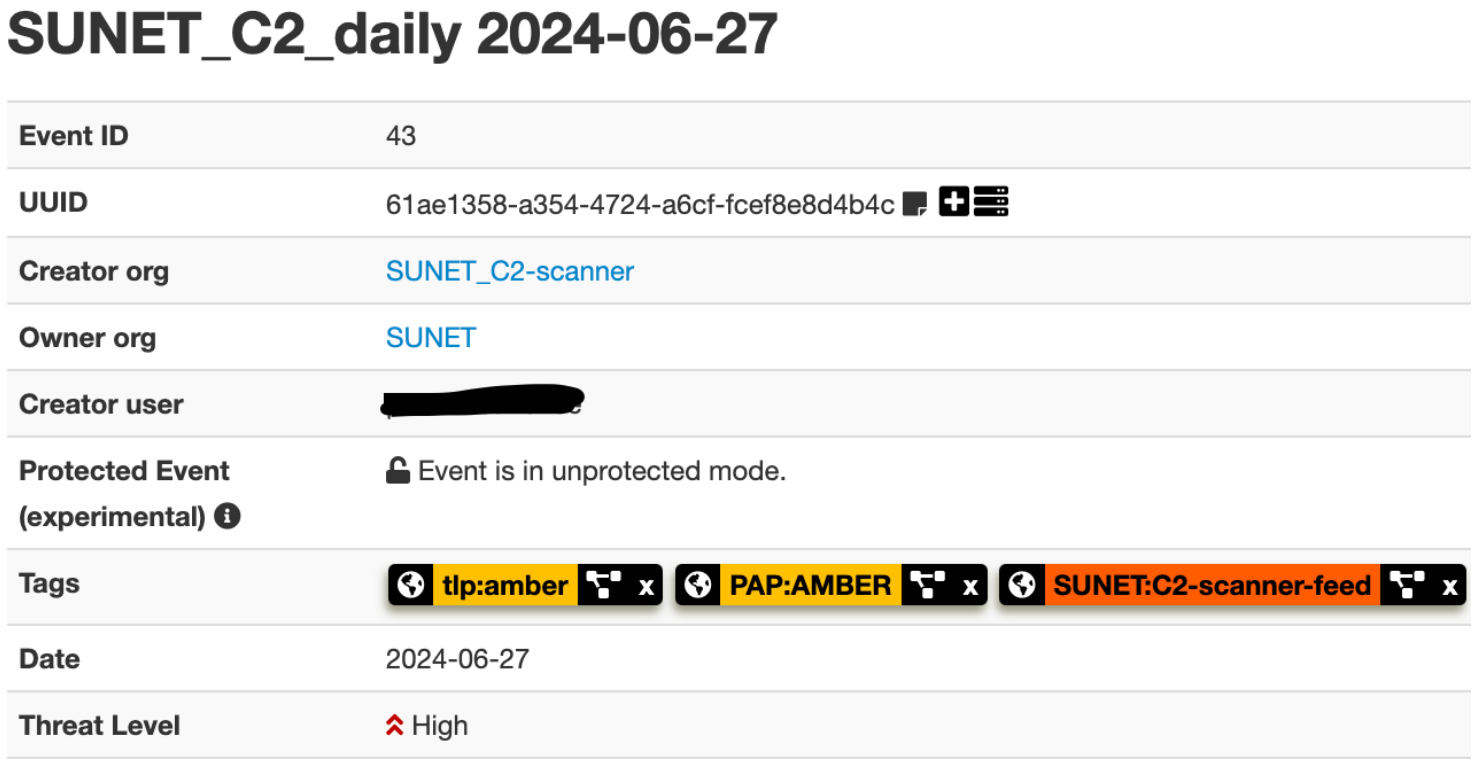
- EU Project met Europese National Research and Education Networks (NREN)
- Samen werken aan oplossingen zoals DDoS tooling, firewalling, vulnerability management en ook Cyber Threat Intelligence

➢ **'Business model for a European RE security intelligence hub'**

➢ **Onderzoeken TI Feeds en Tooling**

➢ **Genereren van threat intel**

➢ **Delen van TI tussen NRENS**



SUNET_C2_daily 2024-06-27

Event ID	43
UUID	61ae1358-a354-4724-a6cf-fcef8e8d4b4c
Creator org	SUNET_C2-scanner
Owner org	SUNET
Creator user	[redacted]
Protected Event (experimental)	Event is in unprotected mode.
Tags	tlp:amber x PAP:AMBER x SUNET:C2-scanner-feed x
Date	2024-06-27
Threat Level	High

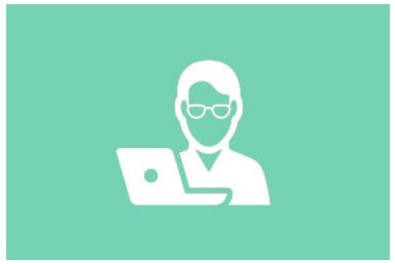
https://resources.geant.org/wp-content/uploads/2023/11/GN5-1_M8.2_Business-Model-for-a-European-RE-Security-Intelligence-Hub.pdf

SURF

Wat kun je als instelling doen?

Wat kun je doen?

- Zorg dat de basismaatregelen op orde zijn!
- Gebruik de security inzichten in het netwerkdashboard om je aanvalsoppervlak te beperken.
- Maak effectief gebruik van MISP en de threat intel die gedeeld wordt.
- **Deel (incident) informatie met SURFcert en de community!**



Richt risicomanagement in

Pas sterke authenticatie toe

Bepaal wie toegang heeft tot uw data en diensten

Beperk het aanvalsoppervlak

Gebruik versleuteling

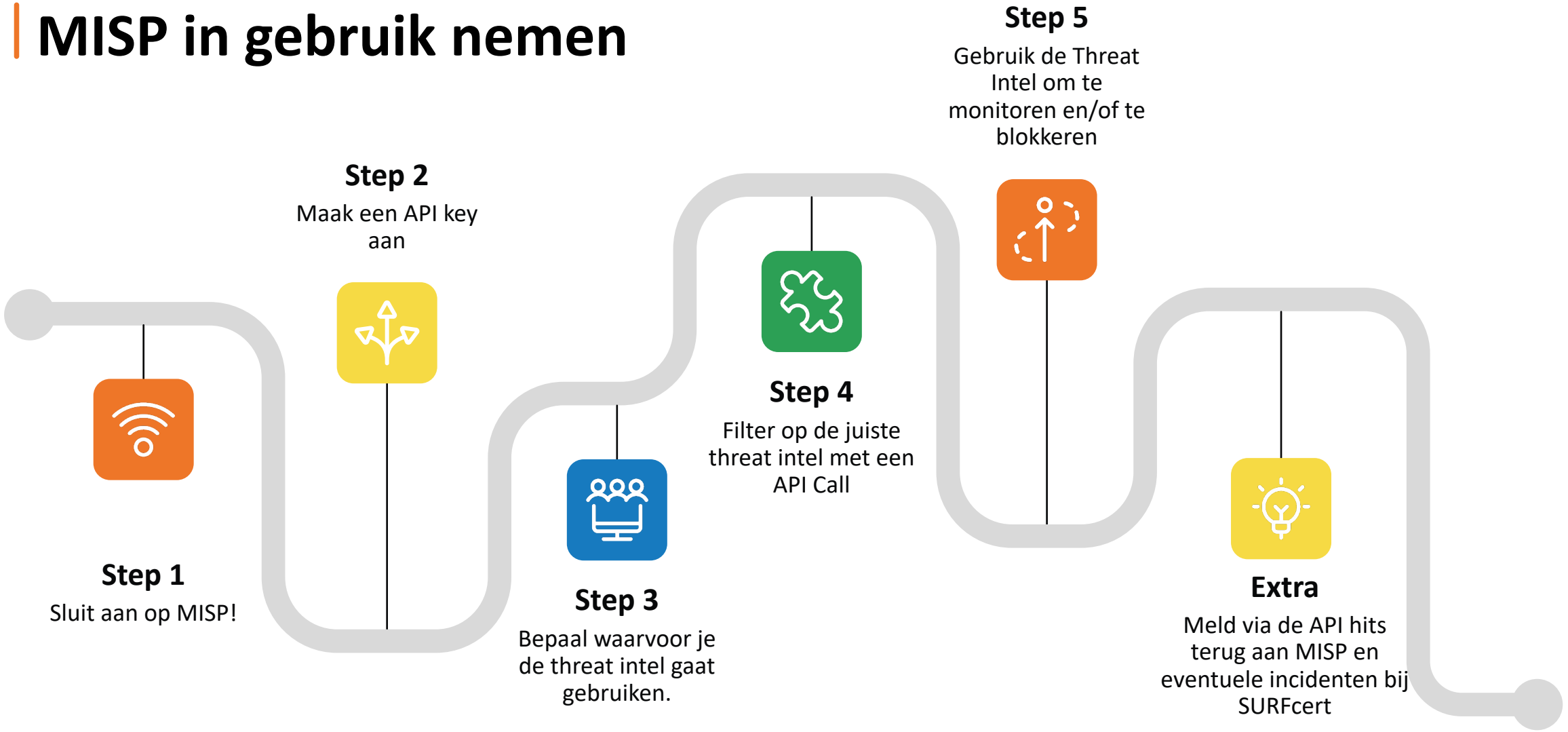
Bescherm je organisatie tegen verlies van gegevens

Richt Patchmanagement in

Centraliseer en analyseer loginformatie

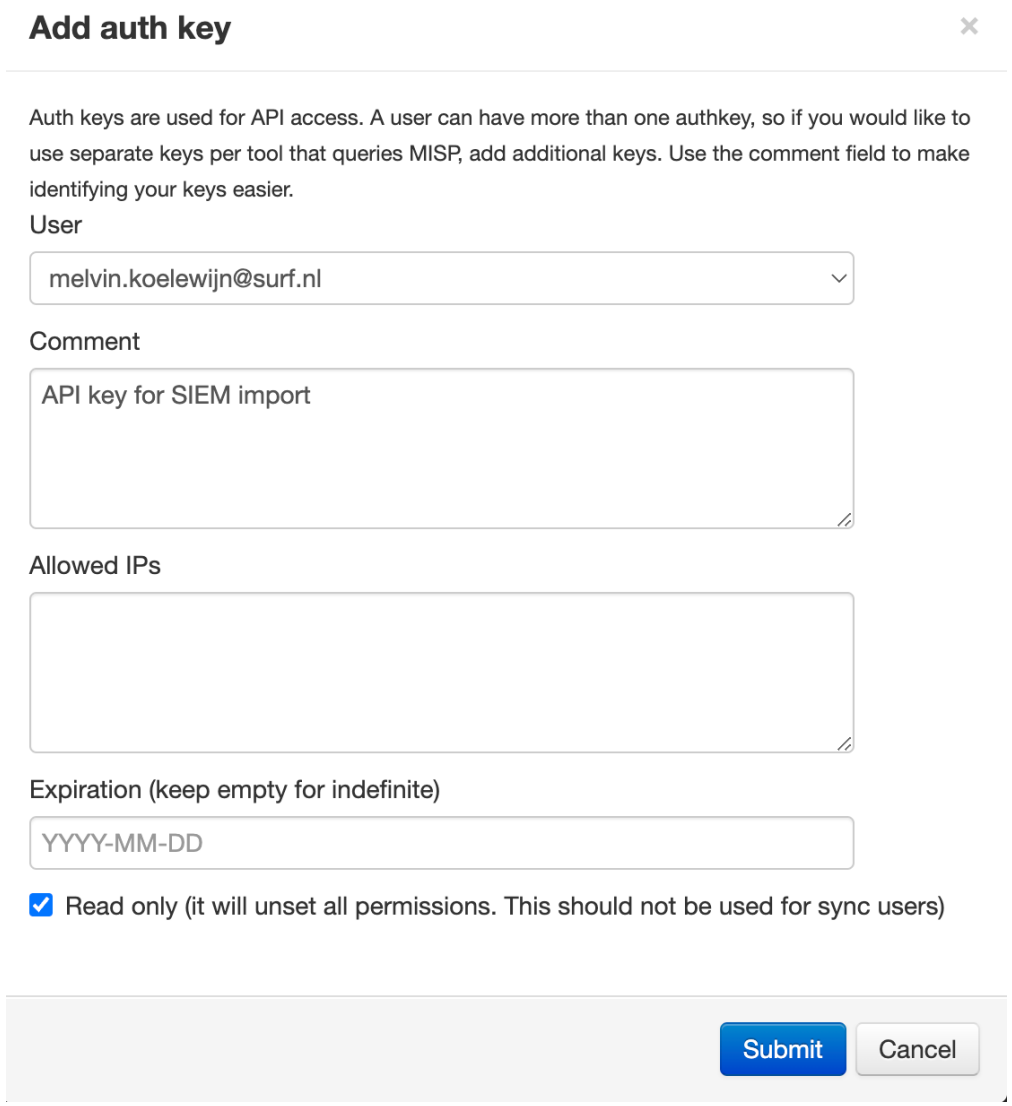
Bron: https://www.ncsc.nl/wat-kun-je-zelf-doen/weerbaarheid/beschermen/basismaatregelen-cybersecurity

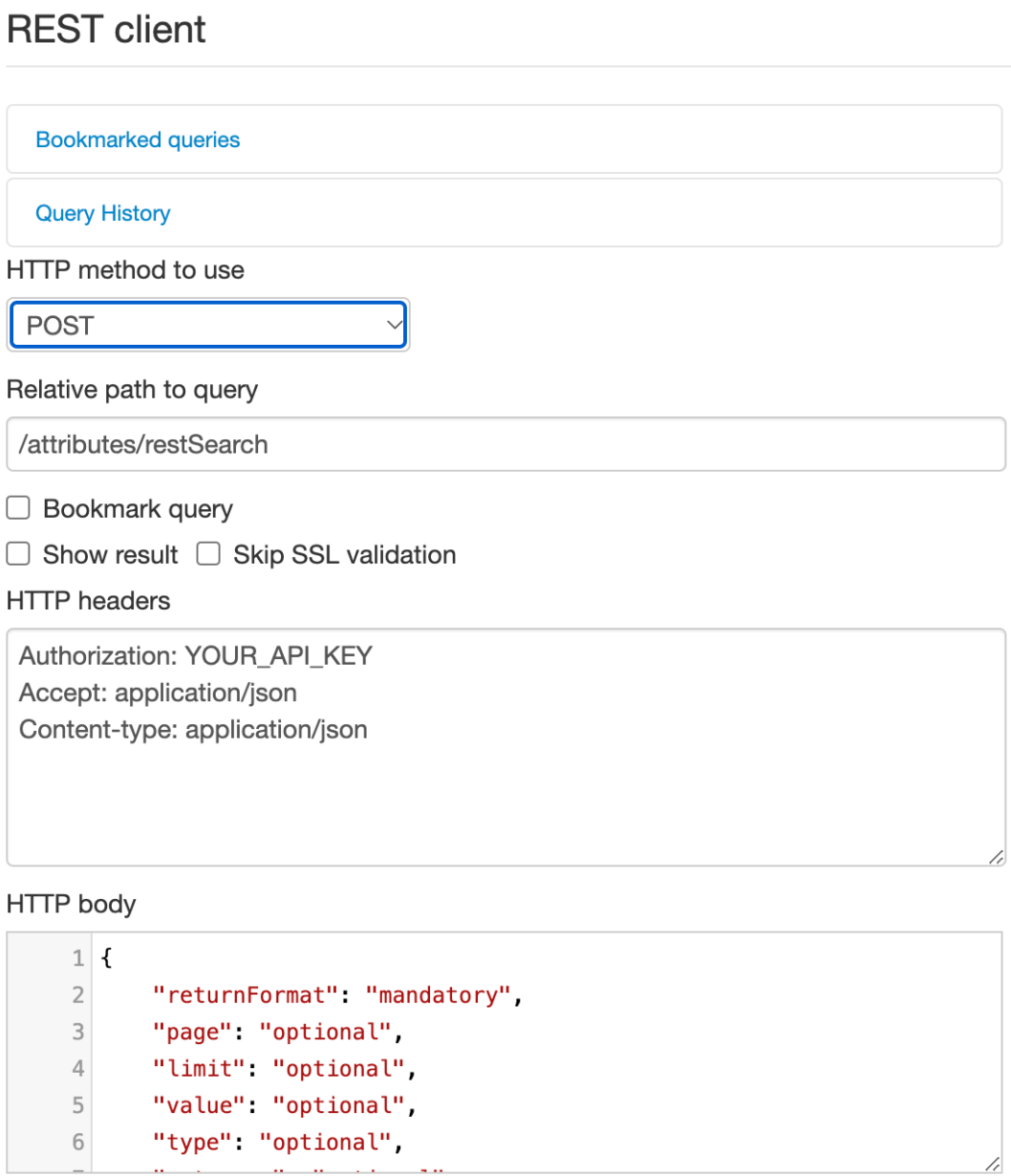
MISP in gebruik nemen



MISP informatie: https://wiki.surfnet.nl/pages/viewpage.action?pageId=35798225

Voorbeeld API key en query





Vragen?

Melvin Koelewijn

Team Security Techniek

Melvin.Koelewijn@SURF.nl

Einde