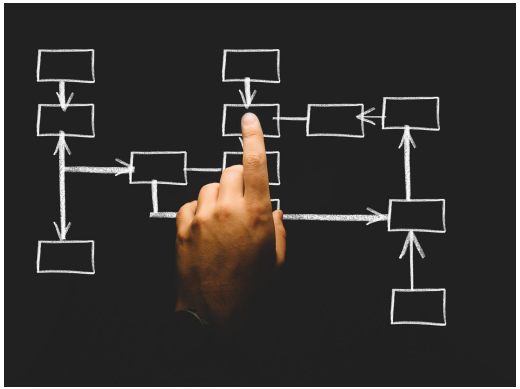
SUNET

SUNET Säkerhetscenter

Nationellt säkerhetscenter för forskning och utbildning

Agenda Onsdag 16/3



1. Förmiddag
   - 09:00 - 09:20 Välkomna: Intro, agenda, samarbete, David
   - 09:20 - 09:55 Svarstidsmätning, IntelMQ och TLP refresher, Maria
   - 10:00 - 10:15 IT-relaterade metoder i kriget mot Ukraina, John
   - 10:15 - 10:25 MISP och informationsdelning, Pettai
   - 10:25 - 10:35 Blockeringar och metodik, Rikard
   - 10:35 - 10:45 SUNET DNS resolver, RPZ och data, Pettai

2. Eftermiddag
   - 13:00 - 13:45 Hur riskmodellerar man i en föränderlig värld, Janne Haldesten
   - 14:00 - 14:10 Info om krisövningar, AMA och Maria
   - 14:10 - 14:45 Verksamhetsstöd och framtid, öppen diskussion

SUNET SOC

En förändrad hotbild enligt Säkerhetspolisen

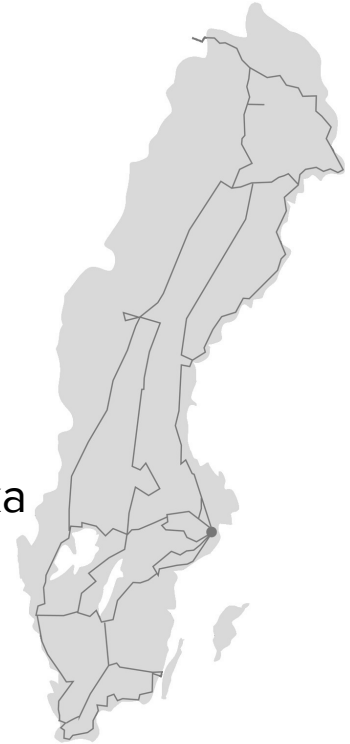
Från Säkerhetspolisens årsbok 2020

- *“ [...] Säkerhetspolisen bedömer att underrättelsehotet kommer att fortsätta vara högt de närmaste åren. Det kommer främst att rikta sig mot kommersiella mål, militära mål, teknik, forskning och utveckling och mot människor som sökt fristad i Sverige.”*
- *“ [...] Angreppen riktas bland annat mot svensk världsledande forskning och innovation med målet att stjäla kunskap och ta över företag för att olovligen bygga kompetens och förmåga. Säkerhetspolisen uppskattar att den information och kunskap som olovligen inhämtas varje år kan värderas till miljardbelopp.“*

SUNET SOC

Fortsatt etablering av vårt säkerhetscenter

- Behov av effektivt informationsutbyte
- Stora mängder attacker och events
- Ökade förväntningar vid distansarbete/digitalisering
- Uppmuntra, utveckla och behålla kompetens inom sektorn
- Det är svårt för små som stora organisationer att övervaka och hantera risker i en global kontext
- Samarbete är en nyckelfaktor



SUNET SOC

Grundoperativ verksamhet - Säkerhetscenter

- Omvärldsbevaka och notifiera kring kritiska sårbarheter
- Samordna incidenthantering mellan organisationer och inom SUNETs egna tjänster
- Facilitera och uppmuntra nätverkande, kunskapsspridning och kompetensdelning
- Rådgivning och informationsdelning - i samarbete med organisationer
- Upprätta och underhålla relationer med andra incidenthanterande organisationer
- Förvalta och vidareutveckla kontaktregister för alla anslutna organisationer

Teknikstöd som alla anslutna organisationer har tillgång till:

- MISP och generell informationsdelning från andra verktyg/källor
- SUNET DNS Resolver med policybaserad blockering
- Sårbarhetsscanner

Allt ovan ingår i SUNET-anslutningen

SUNET SOC

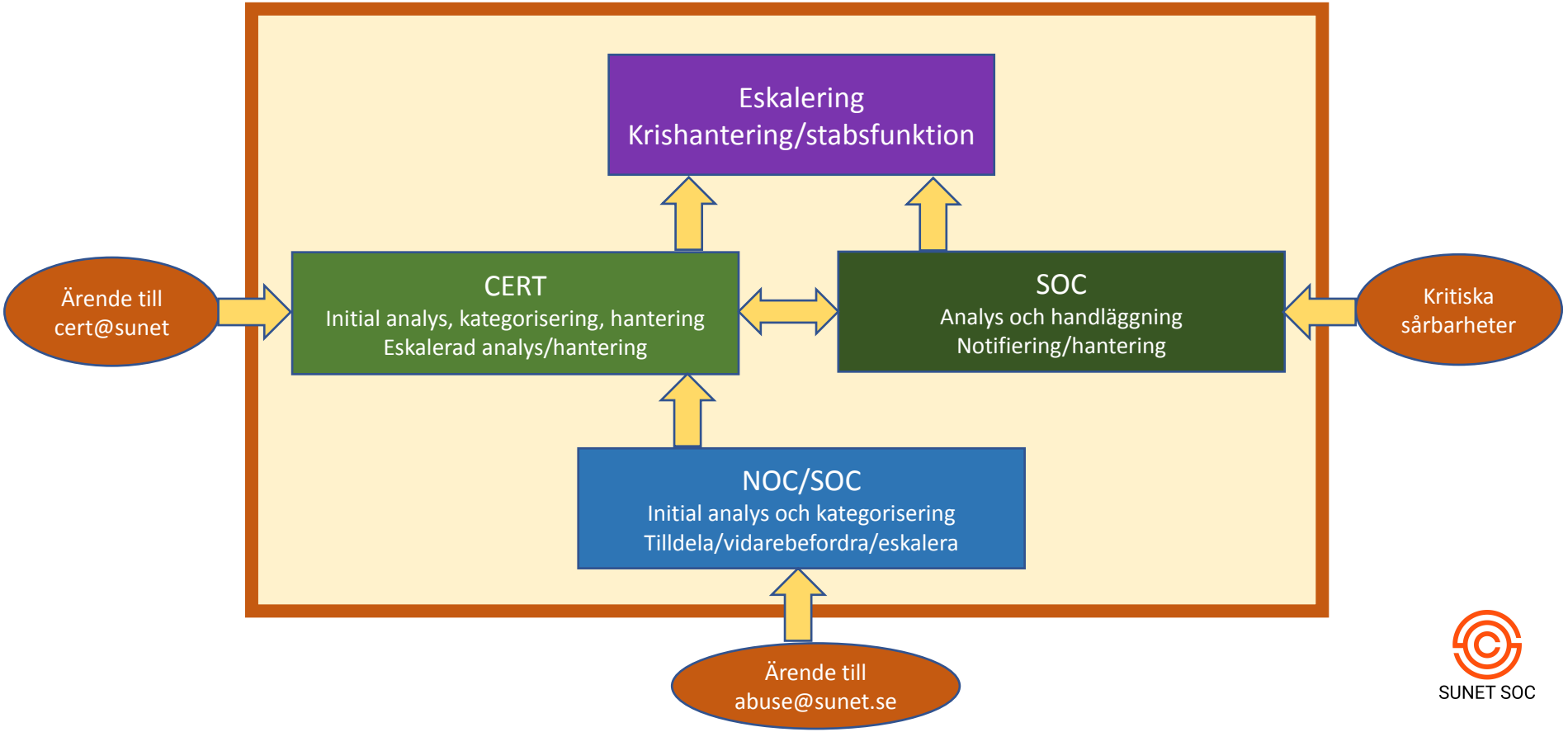
DNSSEC - uppdatering från HT21

JU.SE

DU.SE

SUNET

Ärendehantering



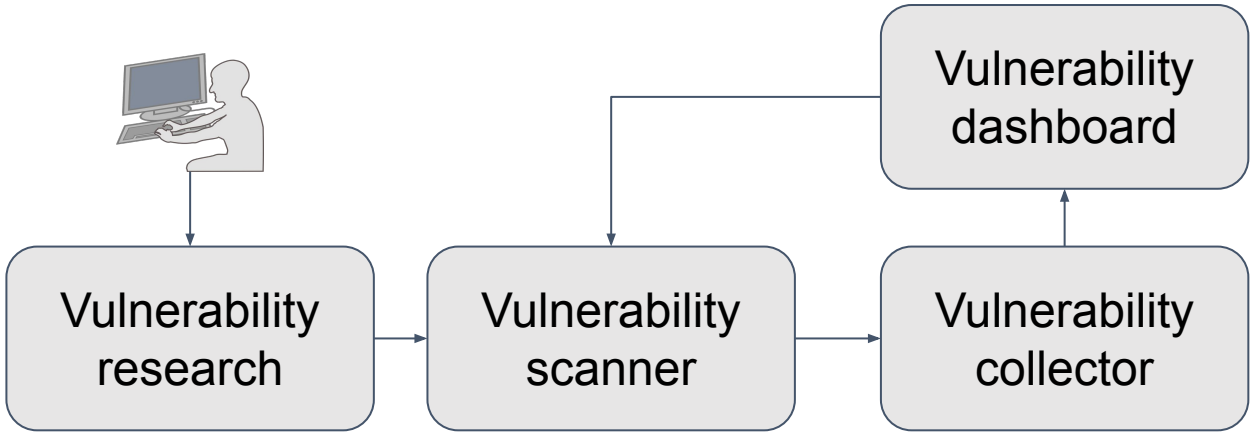
SUNET SOC

Proaktiv sårbarhetsmonitorering - Dashboard

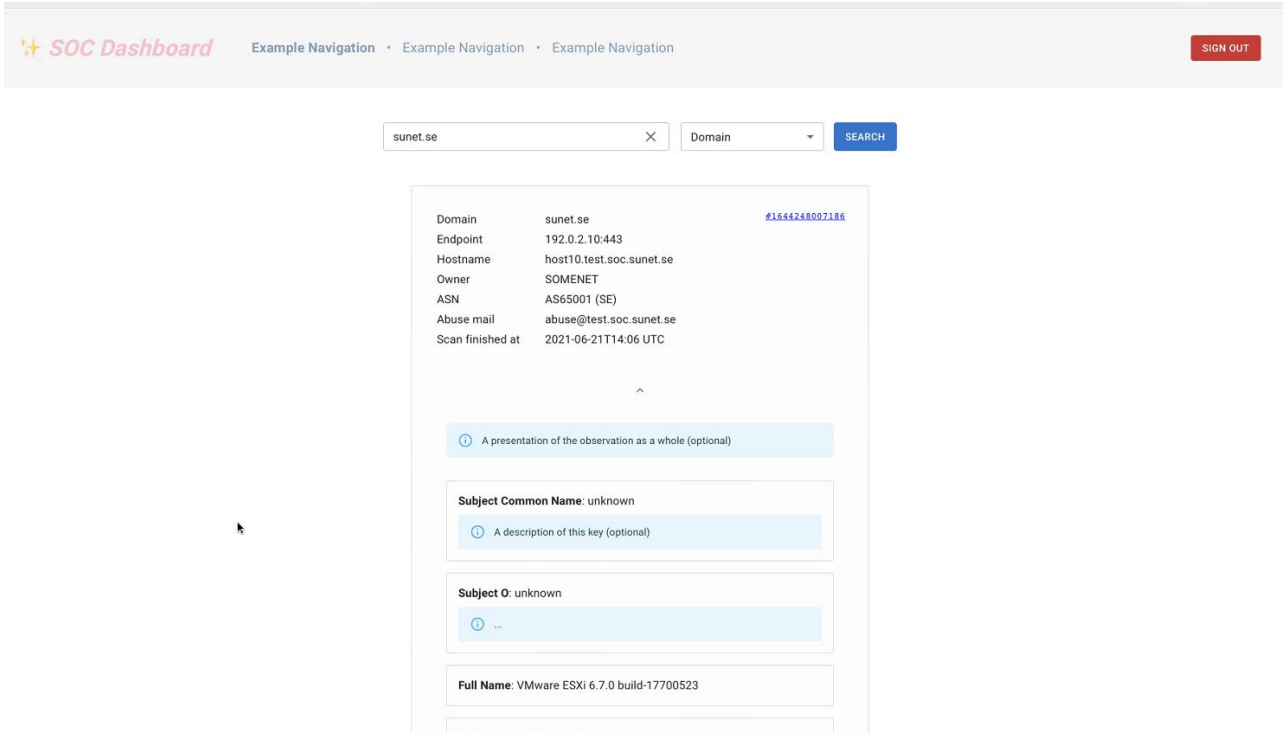
Tidig detektion av nya angreppssätt och sårbarhetsinformation

Skapa ett ramverk för att kunna genomföra verifiering utan kunskap om sårbarhet och programmering

Skapa ett kundanpssat gränssnitt för högprioriterade åtgärder



SOC DASHBOARD



SUNET

Fortsatt lyhördhet och behovsfångst

Vi fortsätter efter dagens presentationer med en dialog om nutid och framtid

~ 14:10

SUNET SOC

Rekommenderade åtgärder (SÄPO)

1. Installera säkerhetsuppdateringar så fort det går
2. Förvalta behörigheter och använd starka autentiseringsfunktioner
3. Begränsa och skydda användningen av systemadministrativa behörigheter
4. Inaktivera oanvända tjänster och protokoll (härda systemen)
5. Gör säkerhetskopior och testa om informationen går att läsa tillbaka
6. Tillåt endast godkänd utrustning i nätverket
7. Säkerställ att endast godkänd mjukvara får köras (vitlistning)
8. Segmentera nätverken och filtrera trafiken mellan segmenten
9. Uppgradera mjuk- och hårdvara
10. Säkerställ en förmåga att upptäcka säkerhetshändelser

SUNET SOC

Rekommenderade åtgärder ENISA

1. Ensure remotely accessible services require multi-factor authentication (MFA).
2. Ensure users do not re-use passwords, encourage users to use Multiple Factor Authentication (MFA) whenever supported by an application (on social media for instance)
3. Ensure all software is up-to-date
4. Tightly control third party access to your internal networks and systems
5. Pay special attention to hardening your cloud environments
6. Review your data backup strategy
7. Change all default credentials
8. Employ appropriate network segmentation
9. Conduct regular training
10. Create a resilient email security environment
11. Organise regular cyber awareness events
12. Protect your web assets from denial-of-service attacks
13. Block or severely limit internet access for servers
14. Make sure you have the procedures to reach out and swiftly communicate with your CSIRT.

SUNET SOC

CIS Critical controls

1. Inventory and Control of Enterprise Assets
2. Inventory and Control of Software Assets
3. Data Protection
4. Secure Configuration of Enterprise Assets and Software
5. Account Management
6. Access Control Management
7. Continuous Vulnerability Management
8. Audit Log Management
9. Email Web Browser and Protections
10. Malware Defenses
11. Data Recovery
12. Network Infrastructure Management
13. Network Monitoring and Defense
14. Security Awareness and Skills Training
15. Service Provider Management
16. Application Software Security
17. Incident Response Management
18. Penetration Testing

SUNET SOC

Informationskanaler och samarbete

Webforum

- https://forum.sunet.se/s/sakerhetscenter

Slack-kanal

- #EXT-SUNET-SOC

Mailinglista

- cert-diskussion@lists.sunet.se

Signal-grupp

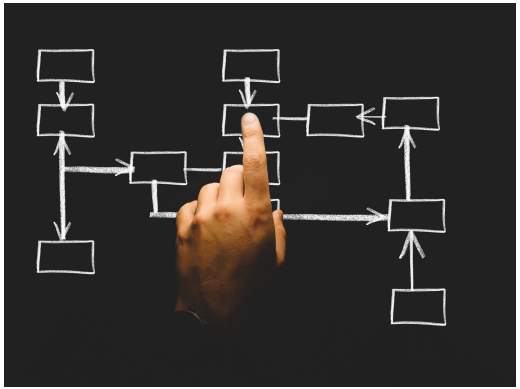
- SUNET SOC EXT

Wiki-sidor

- https://wiki.sunet.se

SUNET SOC

Agenda Onsdag 16/3



1. Förmiddag
   - 09:00 - 09:20 Välkomna: Intro, agenda, samarbete, David
   - 09:20 - 09:55 Svarstidsmätning, IntelMQ och TLP refresher, Maria
   - 10:00 - 10:15 IT-relaterade metoder i kriget mot Ukraina, John
   - 10:15 - 10:25 MISP och informationsdelning, Pettai
   - 10:25 - 10:35 Blockeringar och metodik, Rikard
   - 10:35 - 10:45 SUNET DNS resolver, RPZ och data, Pettai

2. Eftermiddag
   - 13:00 - 13:45 Hur riskmodellera i en föränderlig värld, Janne Haldesten
   - 14:00 - 14:10 Info om krisövningar, AMA och Maria
   - 14:10 - 14:45 Verksamhetsstöd och framtid, öppen diskussion

SUNET SOC

MISP - Threat sharing platform

https://misp.cert.sunet.se

(Se https://wiki.sunet.se/display/SUNETCERT/MISP)

Har generella Threat feeds + “manuellt” inrapporterat data

Förenklad “Frontend” till MISP: https://IOC-lookup.sunet.se för snabbsökning av de vanligaste attributen, även förenklad rapportering, samt “sightings” rapportering.

Ska upprustas + byta Openstack-site

SUNET SOC

MISP forts.

Statistics

Usage data | Organisations | User and Organisation statistics | Tags | Attribute histogram | Sightings toplists | Galaxy Matrix

Organisation list

Quick overview over the organisations residing on or known by this instance.

Local organisations | Known remote organisations | All organisations

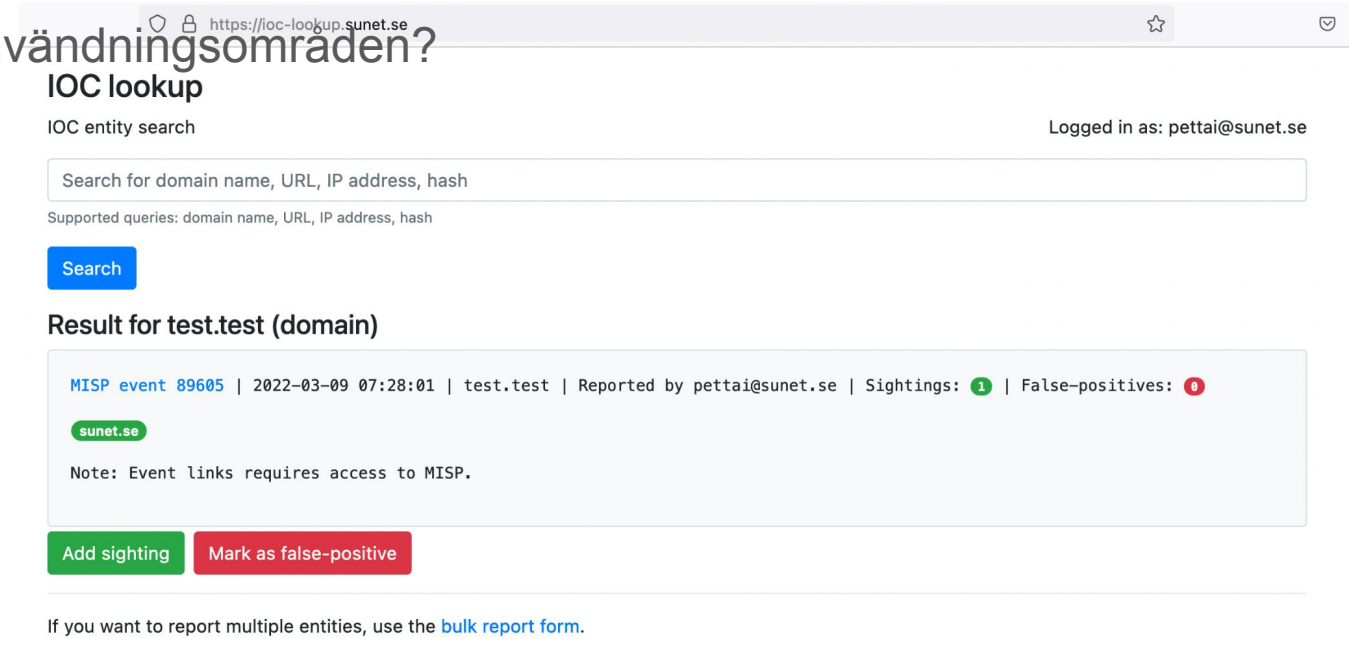
Logo	Name	Users	Events	Attributes	Nationality	Type	Sector	Activity (1 year)
BTH.SE	BTH.SE	1	0	0				
CHALMERS.SE	CHALMERS.SE	6	4	7				
DU.SE	DU.SE	3	0	0				
EDUID.SE	EDUID.SE	1	0	0				
FHS.SE	FHS.SE	2	0	0				
GU.SE	GU.SE	3	0	0				
HB.SE	HB.SE	3	0	0				
HIG.SE	HIG.SE	2	0	0				
HJ.SE	HJ.SE	3	1	20				
HKR.SE	HKR.SE	2	0	0				
IRF.SE	IRF.SE	1	1	1				
KAU.SE	KAU.SE	2	0	0				
KI.SE	KI.SE	4	0	0				
KTH.SE	KTH.SE	6	0	0				
LIU IRT	LIU IRT	1	0	0				
LIU.SE	LIU.SE	6	3	45				
LNU.SE	LNU.SE	2	0	0				
LTU.SE	LTU.SE	11	0	0				
LU.SE	LU.SE	6	19	226				
MDH.SE	MDH.SE	5	0	0				
MIUN.SE	MIUN.SE	2	0	0				
NONE	NONE	0	0	0				
ORU.SE	ORU.SE	3	0	0				
SLU.SE	SLU.SE	1	0	0				
SMHI.SE	SMHI.SE	1	0	0				
SU.SE	SU.SE	7	3	4				
SUNET.SE	SUNET.SE	17	205	67705				
UMU.SE	UMU.SE	7	0	0				
USER.UU.SE	USER.UU.SE	3	1	8				
UU-CSIRT	UU-CSIRT	1	2	54				
UU.SE	UU.SE	0	0	0				

MISP forts.

Hur använder ni datat i MISPen idag?

(tex Johns listor på Cobaltstrike / C&C)

Finns det andra/nya användningsområden?



MISP - forts.

Nytt/nya samarbeten på gång med tex UNINETT/SIKT

IOC-lookup kommer pekas om på nya MISPen

Inga generella “publika” threat feeds, endast “verifierad” data

Kommer replikeras till “gamla” MISPen

Endast API-access (samt IOC-lookup)

SUNET SOC

Blockeringar och metodik

(Rikard presenterar…)

SUNET SOC

SUNET DNS resolver

89.32.32.32 / 2001:6b0:89::32:32:32

Startade Q1 2019

“Publik”

“Internet hardened” / DDoS-mitigering

RPZ (via MISP) samt SWITCH & SURBL

SUNET SOC

SUNET DNS resolver forts.

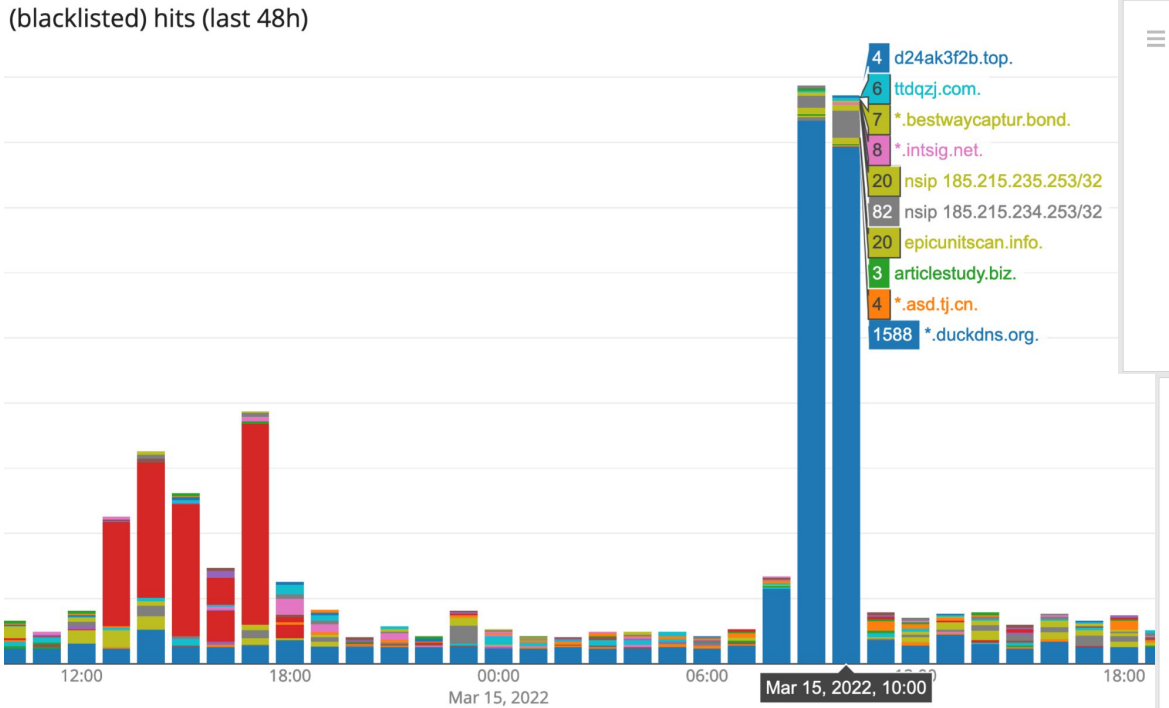
Prestandaförbättringar

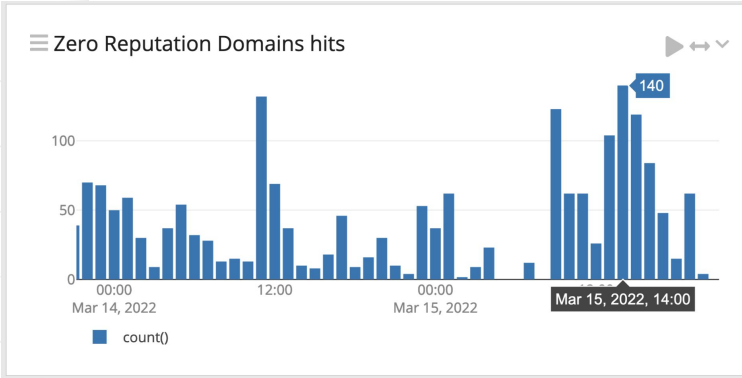
Förbättringar kring DoT & DoH, nu även möjligt att konfigurera sin macOS/iOS device att använda DoT/DoH för “alla” DNS-förfrågningar (https://wiki.sunet.se/pages/viewpage.action?pageId=93979181#S%C3%A5konfigurerarduDoHidinwebbl%C3%A4sare/Appleenhet-macOS(BigSur++)&iPhone(kr%C3%A4veriOS14++)

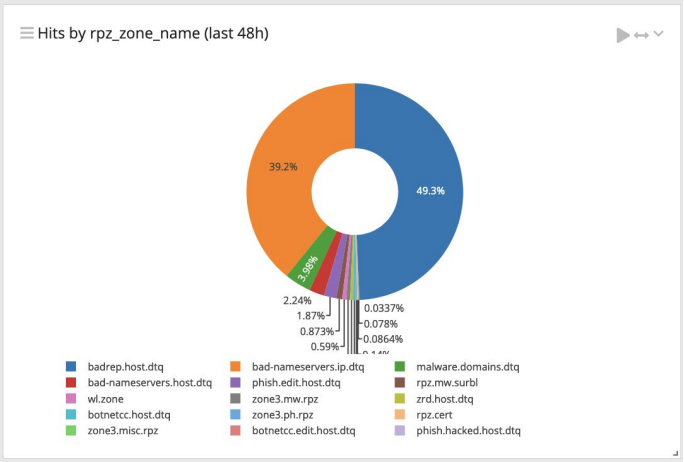
Ytterligare RPZ tillagda (från Spamhaus)

SUNET SOC

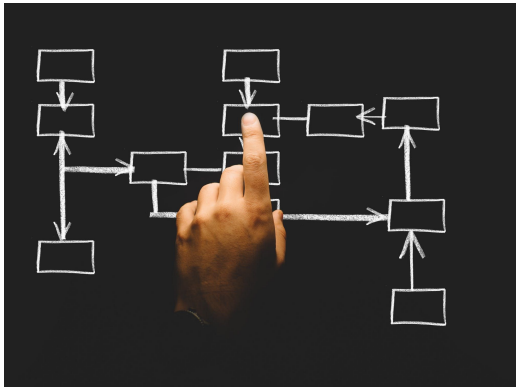
SUNET DNS resolver forts.







Agenda Onsdag 16/3



1. Förmiddag
   - 09:00 - 09:20 Välkomna: Intro, agenda, samarbete, David
   - 09:20 - 09:55 Svarstidsmätning, IntelMQ och TLP refresher, Maria
   - 10:00 - 10:15 IT-relaterade metoder i kriget mot Ukraina, John
   - 10:15 - 10:25 MISP och informationsdelning, Pettai
   - 10:25 - 10:35 Blockeringar och metodik, Rikard
   - 10:35 - 10:45 SUNET DNS resolver, RPZ och data, Pettai

2. Eftermiddag
   - 13:00 - 13:45 Hur riskmodellera i en föränderlig värld, Janne Haldesten
   - 14:00 - 14:10 Info om krisövningar, AMA och Maria
   - 14:10 - 14:45 Verksamhetsstöd och framtid, öppen diskussion

SUNET SOC

Kommande aktiviteter

Torsdag:

09:00 Visselblåsarfunktion och Securedrop

13:00 CSIRT forum med PGP signering

15:00 eduSIGN meetup

MISP genomgång från CIRCL.LU

TRANSITS utbildning på svenska i Sverige?

SUNET

Vad tyckte du om passet?
Svara på frågorna i pollen!

Obs. Har du en äldre version av din Zoom-klient kan du inte svara på pollen i Zoom.
Skriv i chatten om du vill dela med dig av dina tankar!

SUNET

LUNCH PAUS ses 13:00

SUNET