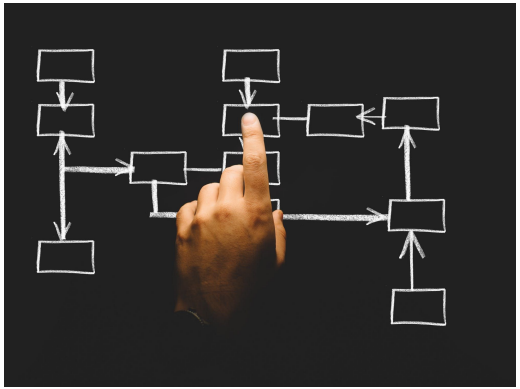
SUNET

SUNET Säkerhetscenter

Nationellt säkerhetscenter för forskning och utbildning

Agenda Onsdag 21/4



1. SUNET Säkerhetscenter - SOC projektet
   - 09:00 - 09:15 Välkomna: Intro projektet och förmågor
   - 09:15 - 09:25 Kort om nytt, ärenden SUNET CERT
   - 09:25 - 09:35 DNS/RPZ, MISP
   - 09:35 - 09:50 Notifieringar och nutida händelser
   - 09:50 - 10:00 Paus
2. Tjänsten och produkter
   - 10:00 - 10:30 Verktygsdemo sårbarhetshantering med Outpost24. Fördjupad presentation kring API för automatisering
   - 10:30 - 11:00 Verktygsdemo Lockbetesteknik från Attivo Networks
   - 11:00 - 11:05 Paus
   - 11:05 - 11:25 Framtid - tjänst och samverkan
3. Krisövning
   - 11:30 - 12:00 MSB keynote
   - 12:00 - 13:00 Lunch
   - 13:00 - Krisövningen under eftermiddagen

SUNET SOC

En förändrad hotbild enligt Säkerhetspolisen

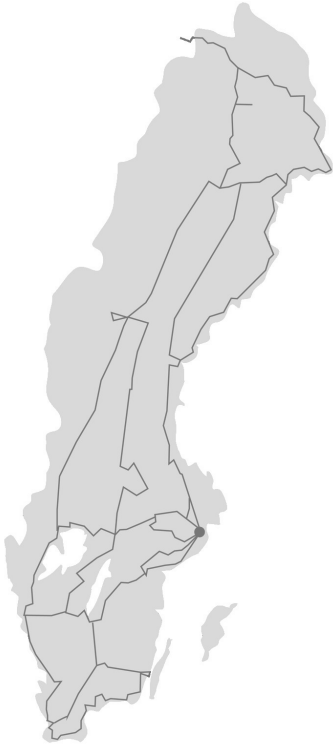
Från Säkerhetspolisens årsbok 2020

- *“ [...] 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

Projektets bakgrund och syfte

- Samverkan med PTS & MSB
- Fokus på **förebyggande arbete**
- Göra sektorn självförsörjande på IT-säkerhet
- Förlänga karriärvägarna i sektorn



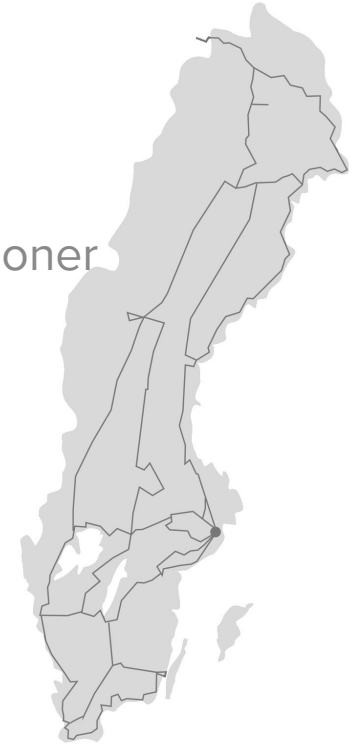
Projektet externt finansierat 2019-2021.

SUNET SOC

Förändringsresan

Med hjälp av de externa finanserna har vi kunnat:

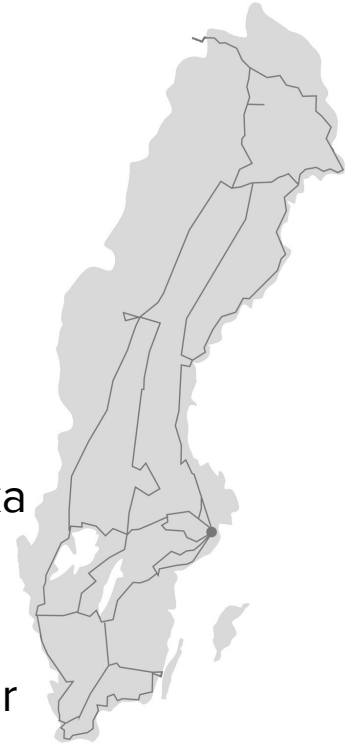
- Frigöra tid för integration och förbättringsarbeten
- Aktivt omvärldsbevakat och notifierat anslutna organisationer
- Stärkt vår förmåga att motstå avancerade angripare
- Prövat och implementerat ny teknik
- Genomfört upphandlingar och avrop inom önskad teknik
- Genomfört workshops / kunskapsspridning



SUNET SOC

Behovsbild / Gå vidare med etableringen

- Fortsatt 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
- Skräddarsytt partnerskap för våra anslutna organisationer



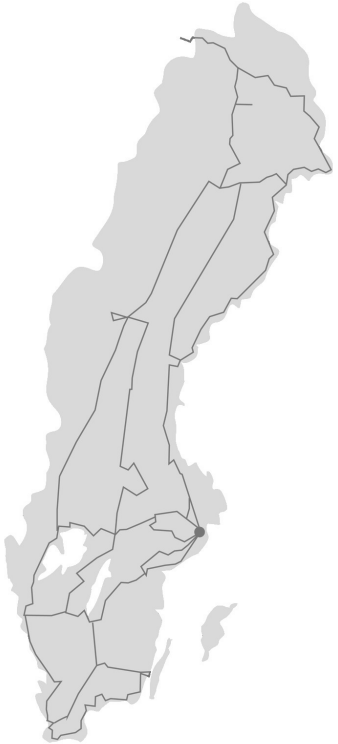
SUNET SOC

Etableringbeslut

Vetenskapsrådet/SUNET 20201202

Att etablera Sunet Säkerhetscenter med följande uppgifter:

a. Ansvara för IT-säkerhetsarbetet i Sunet och i Sunets tjänster.
b. Stödja arbetet med IT-säkerhet hos till Sunet anslutna organisationer.
c. Bygga upp förmågan att motstå avancerade angripare (APT).
d. Arbeta med förebyggande verksamhet inom området.
e. Bistå vid hantering av större IT-säkerhetsrelaterade incidenter.
f. Ansvara för CERT och IRT-verksamhet i Sunet enligt etablerad branschstandard, inklusive arbete med certifieringar, processer och ärendehantering inom detta område



Men vi måste definiera hur vi bäst samarbetar och vilka tillägg som är önskvärda för majoriteten på ett kostnadseffektivt sätt. (fortsättning följer 11:00)

SUNET SOC

Förmågor och utvecklingsarbeten

Hot och riskanalys

Sårbarhetsmonitorering och verifiering - > notifiering

Dela data mellan och om aktörer

Upptäcka intrång och intrångsförsök

Kunskapsspridning och best-practise

SUNET SOC

Informationsdelning mellan CSIRTs

Tillhandahålla möjlighet för informationsutbyte

- Dela data om IOCs
- Tillhandahålla förädlade block-listor
- Threat feeds

MISP Threat Sharing

SUNET SOC

Större investeringar (utöver personal och fasta utgifter)

2019	Sårbarhetsscanner - (Outscan)
2020	Lockbetesteknik - (Attivo Network)
2021	Intrång och anomalidetektering - (Vectra AI)
2022?	Nnnn nnn

Parallella utvärderingar/upphandlingar:

- IDS - Suricata/Tipping Point/Corelight m.fl.
- Threat Feeds - Recorded Future m.fl.
- Loggservrar - Humio/Logpoint/GEL m.fl.

SUNET SOC

Kunskapsspridning

Workshops och utbildningstillfällen

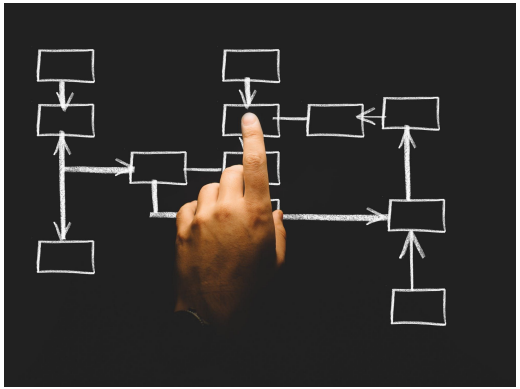
Incidenthantering - TRANSITS

Malware analys - Workshop

Praktisk utbildning / Mentorsprogram för studenter

SUNET SOC

Agenda



1. SUNET Säkerhetscenter - SOC projektet
   - 09:00 - 09:10 Intro projektet och förmågor
   - Kort om nytt, ärenden SUNET CERT
   - DNS/RPZ, MISP
   - Notifieringar och nutida händelser
   - 09:50 - 10:00 Paus
2. Tjänsten och produkter
   - 10:00 - 10:30 Verktygsdemo sårbarhetshantering med Outpost24. Fördjupad presentation kring API för automatisering
   - 10:30 - 11:00 Verktygsdemo Lockbetesteknik från Attivo Networks
   - 11:00 - 11:05 Paus
   - 11:05 - 11:25 Framtid - tjänst och samverkan
3. Krisövning
   - 11:30 - 12:00 MSB keynote
   - 12:00 - 13:00 Lunch
   - 13:00 - Krisövningen under eftermiddagen

SUNET SOC

Paus till 10:00

Utvärdering:

https://sunet.artologik.net/sunet/sunetdagarna2021

(länk i chatten)

SUNET SOC

Leverantörsdemonstrationer

10:00 Outpost24

Vår sårbarhetscanner:
API och automatisering

10:30 Attivo NETWORKS

Vårt decoy/lockbetessystem:
Intro och funktionalitet

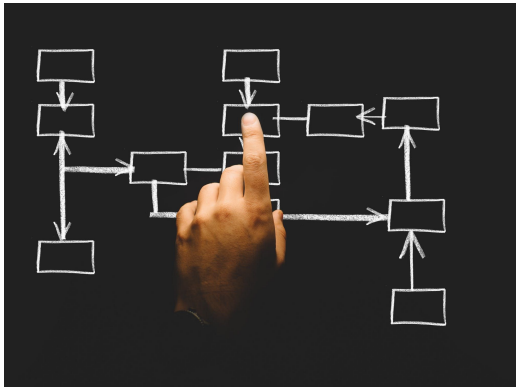
SUNET SOC

Utvärdering och synpunkter

https://sunet.artologik.net/sunet/sunetdagarna2021

(länk i chatten)

Agenda



1. SUNET Säkerhetscenter - SOC projektet
   - 09:00 - 09:15 Välkomna: Intro projektet och förmågor
   - 09:15 - 09:25 Kort om nytt, ärenden SUNET CERT
   - 09:25 - 09:35 DNS/RPZ, MISP
   - 09:35 - 09:50 Notifieringar och nutida händelser
   - 09:50 - 10:00 Paus
2. Tjänsten och produkter
   - 10:00 - 10:30 Verktygsdemo sårbarhetshantering med Outpost24. Fördjupad presentation kring API för automatisering
   - 10:30 - 11:00 Verktygsdemo Lockbetesteknik från Attivo Networks
   - 11:00 - 11:05 Paus
   - 11:05 - 11:25 Framtid - tjänst och samverkan
3. Krisövning
   - 11:30 - 12:00 MSB keynote
   - 12:00 - 13:00 Lunch
   - 13:00 - Krisövningen under eftermiddagen

SUNET SOC

Förmågor och tjänsten

1. Grundoperativ verksamhet - SUNET, SUNET NOC, SUNET CERT (ingår för alla anslutna organisationer)

2. Ökat samarbete - tjänster som kräver upprättade avtal (kostnadsneutralt)
3. Tjänster som kräver tilläggslicenser eller hårdvara (Inköpscentral eller överenskommelse)

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 får tillgång till:

- MISP och generell informationsdelning från andra verktyg/källor
- RPZ med policybaserad blockering
- Sårbarhetsscanner

Allt ovan ingår i SUNET-anslutningen

SUNET SOC

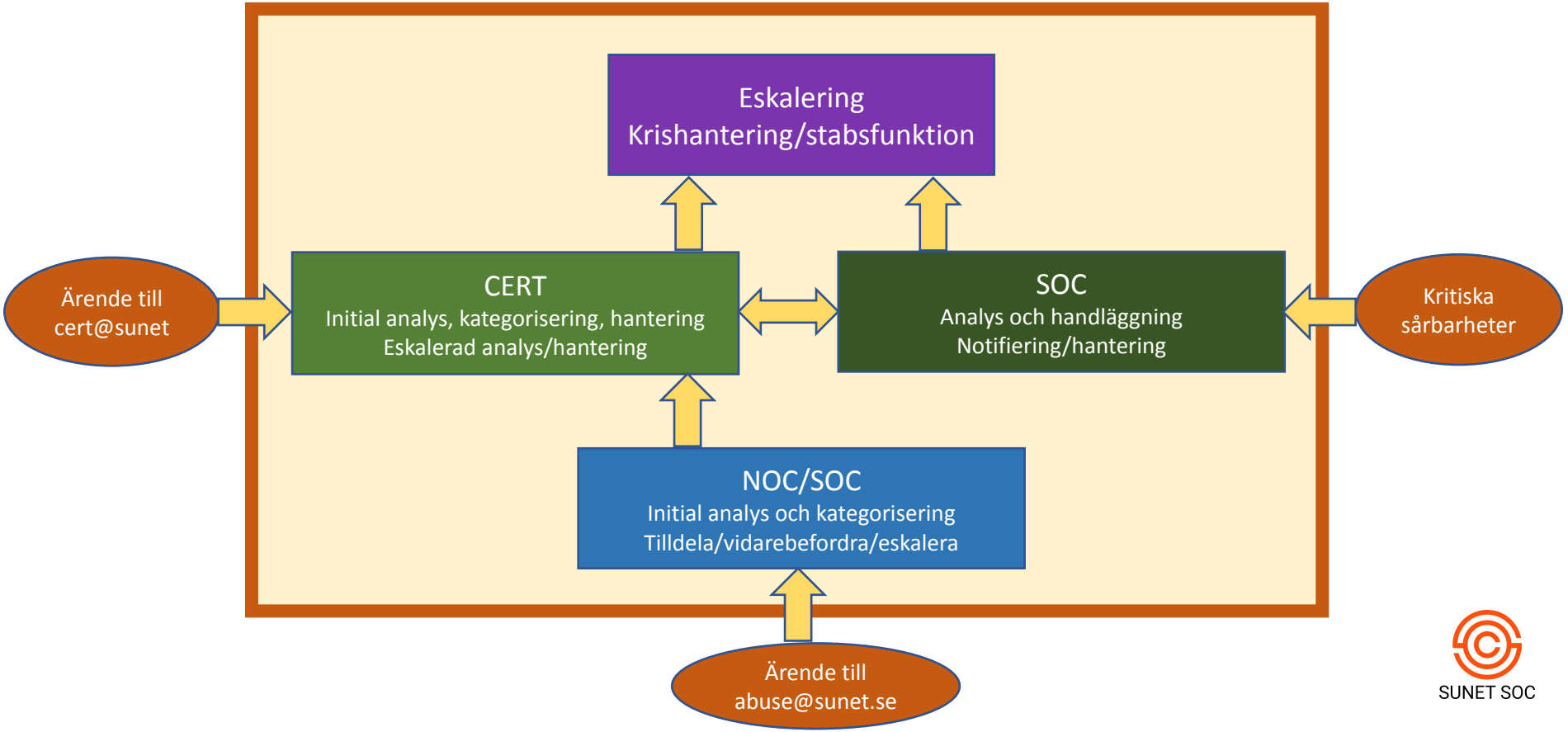
Namnen: SOC / CERT / NOC / Säkerhetscenter

- SUNET NOC - Säkerhetscentrets första linje för ärenden och basdrift
- SUNET SOC - Tilläggstjänsten och internt initierade ärenden
- SUNET CERT - Incidenthantering - expertorganet och eskalering till/från andra organisationer

Bemanning:
Enheten för drift, Nätenheten, Infra-enheten - Linjeorganisationer inom Sunet
+ anställda från lärosäten via kontrakt

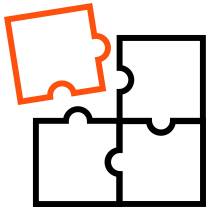
SUNET SOC

Ärendehantering



SUNET SOC

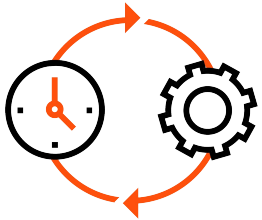
Processen



Identifiera

Förebygga

Analysera



Agera

Rapportera

SUNET SOC

RUTINER

SUNET SOC - valbara tilläggstjänster

- Loggning som tjänst (obegränsad datamängd)
- Dataanalys LAN (applikation och säkerhetsloggar)
- Lockbetesteknik, decoys och påhittade resurser
- Threat Feeds
- Mailfilter-NG

SUNET SOC - ökat samarbete

- Verifiera och notifiera aktuella sårbarheter. Ökad omvärldsbevakning
- Dataanalys WAN (säkerhetsevents)
- Trafikdataanalys WAN (metadata)

SUNET Säkerhetscenter för anslutna organisationer

- Bevaka 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

TEKNISKT STÖD

SUNET SOC - kundanpassat

- Loggning som tjänst
- IDS/Events - Vectra / Suricata / Zeek etc...
- Lockbetsteknik - Attivo Networks
- Recorded Future
- Halon

Verktygsstöd - tilläggspaket

- Egenutvecklade script/utveckling
- IDS/Events - Vectra / Suricata / Zeek etc...
- Netflow - Kentik

Verktygsstöd SUNET Säkerhetscenter

- Kontaktregister - SUNET SRI
- Ärendehanteringssystem - OTRS/JIRA, IntelMQ
- Sårbarhetscanner - Outscan,Openvas,Nessus m.m.
- Datainsamling, rapporter - CERT.SE, Shadowserver
- MISP
- DNS resolver - RPZ

SUNET SOC

Förslag “ökat samarbete” och informationsutbyte = SUNET SOC

- Verifiera och notifiera specifikt om aktuella lokala sårbarheter
- Ökad omvärldsbevakning
- Dataanalys WAN (säkerhetsevents)
- Trafikdataanalys WAN (metadata) gentemot IOC (C2, botnet, DDOS m.m.)
- “Uppdraget” - alltså att behandla och lagra IP-adresser/personuppgifter
- Automatiserad bevakning och larmhantering
- Kompetensstöd vid incidenthantering

Storlek	Organisationens FTE	Månadsavgift
X-small	->100	TBD
Small	101-750	TBD
Medium	750-1500	TBD
Large	1501-3999	TBD
X-Large	4000->	TBD

Vi står inför tre val:

1. Låta gemensamma lösningar ingå i anslutningen (driver generell kostnad)
2. Genomföra avtalstecknanden och månadsfaktureringar (administrativ hantering)
3. Lägga ned den ökade ambitionsnivån

SUNET SOC

SUNET SOC - tilläggstjänster

- Loggning som tjänst (on-premise eller MSSP)
  - Upphandling på gång genom inköpscentral
- Dataanalys LAN (applikation och säkerhetsloggar)
  - Utöver automatiserade larm kan anpassning ske utifrån system/infoklassificering och riskanalys
- Lockbetesteknik, decoys och påhittade resurser
  - Vi har initialt 1000 endpoint licenser samt tillhörande botsinks
- Websårbarhetstester - Detectify
  - Vi har initialt ett dussin teamlicenser
- Threat Feeds
  - SUNET SOC arbetar fram och bevakar eget material
    Upphandling Recorded Future eller motsvarande
- Mailfilter
  - Halon igång som separat tjänst. Kontakta Tomas Liljebergh för mer information.

SUNET SOC

Frågor/synpunkter/kommentarer?

Svara gärna både kring webinaret hur det var samt tankegångar kring tjänsten

https://sunet.artologik.net/sunet/sunetdagarna2021

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

SUNET SOC

Paus till 11:30 - fyll gärna i utvärderingen

Svara gärna både kring webinaret hur det var samt tankegångar kring tjänsten

https://sunet.artologik.net/sunet/sunetdagarna2021

Kommande aktiviteter andra dagar

23:e 10:00 CSIRT-forum

29:e 09:00 eduSign - nutid och framtid

SUNET SOC