# SUNET säkerhetscenter

David Heed, samordnare

# Agenda säkerhetsdagen 2022-10-13

10:00 Intro, Svarstidsmätning, incidentstatistik, krisövningar
11:00 Håller ransomware på att försvinna?
LUNCH
13:00 Kalix kommun och attacken december 2021
14:10 Informationspåverkan, Myndigheten för psykologiskt försvar
15:20 Alternativa kommunikationsvägar, Christian Mohr, HB
16:00 Informationssäkerhet och samverkan, Fia Ewald
16:45 Sunetdagarna Afterwork!

# En förändrad hotbild enligt Säkerhetspolisen

*Från Säkerhetspolisens årsbok 2020*

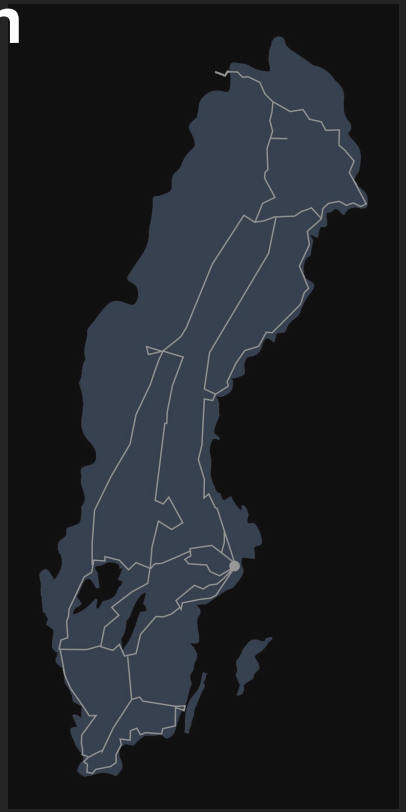
- *“ […] Säkerhetspolisen bedömer att underrättelsehotet kommer att fortsätta vara högt de närmaste åren. Det kommer främst att rikta sig mot kommersiella mål, militära mål, teknik, forskning och utveckling och mot människor som sökt fristad i Sverige.”*

- *“ […] 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.“*

*Från Säkerhetspolisens årsbok 2021*

- *“ […] Sverige ligger i framkant inom områden som spetsteknologi, forskning och innovation och hamnar därför mitt i den globala maktkampen.”*

- *“ […] Ryssland bedriver fortlöpande inhämtning av information och kunskap för att stärka rysk industri och försvarsförmåga bland annat genom industrispionage och cyberspionage mot svenska försvaret, industrin och forskning och utveckling. Det sker genom ständiga försök att hitta och utnyttja sårbarheter.”*



**Syftet med IT-säkerhetsarbetet är att så långt som möjligt *förebygga* framgångsrika IT-attacker mot Sunet och våra kunder**

# Grundoperativ verksamhet - Säkerhetscenter

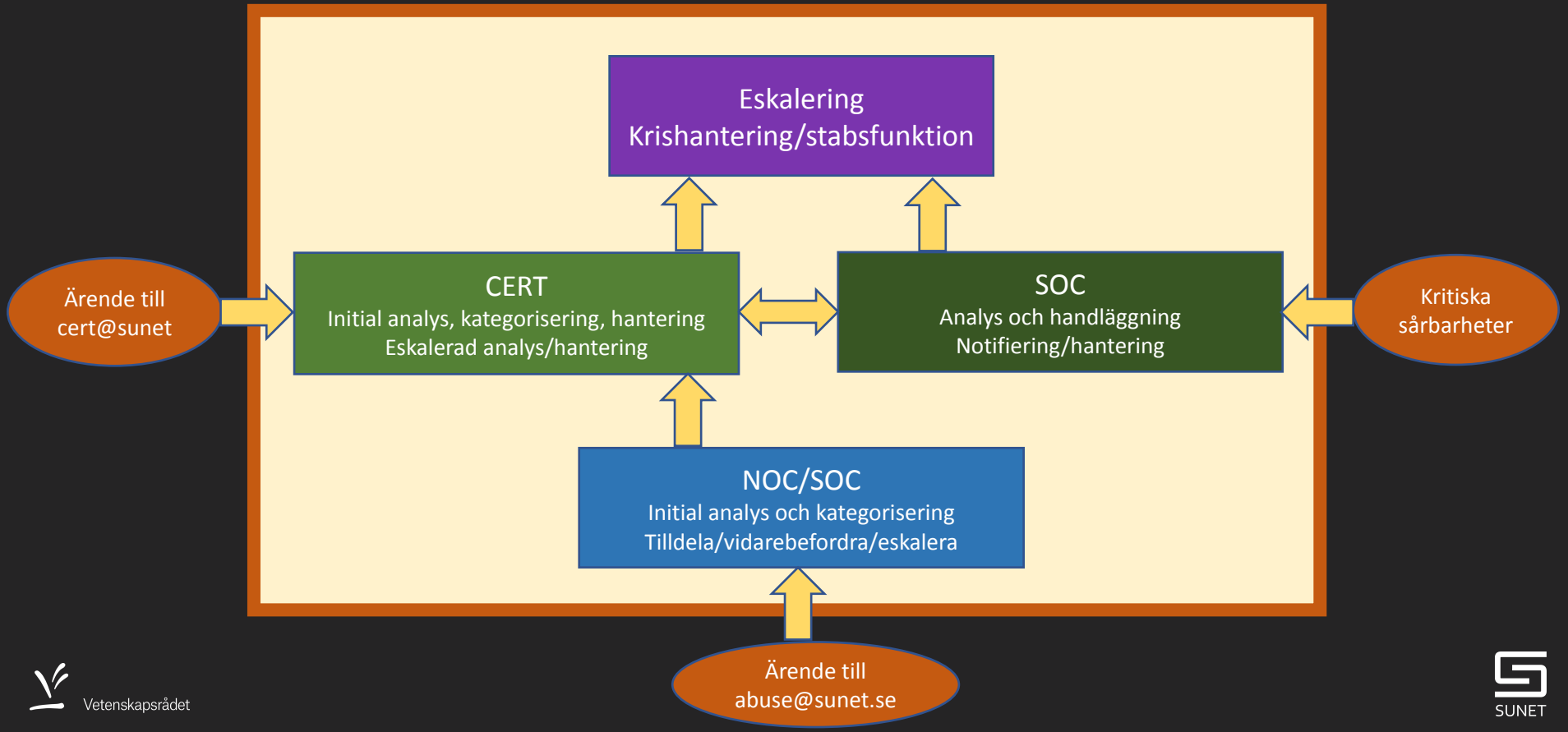
- Omvärldsbevaka och notifiera kring kritiska sårbarheter
- Samordna incidenthantering mellan organisationer och inom SUNETs egna tjänster
- Facilitera och uppmuntra nätverkande, kunskapsspridning och kompetensdelning
- Rådgivning och informationsdelning - i samarbete med organisationer
- Upprätta och 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
- Sårbarhetsscanners

Allt ovan ingår i SUNET-anslutningen

# Ärendehantering



# Några av aktiviteterna sedan sist

Utöver att stötta och analysera händelser samt följa hotbilden

- Fortsatt egen utveckling av scanners för multipla sårbarheter
- Utvärderingar och utveckling kring “dashboard för säkerhet”
- Slutförd upphandling för ny (samma) sårbarhetsscanner (GÉANT)
- Fysiskt CSIRT-forum, första på tre år
- Ny MISP-server installerad som skall fyllas med verifierat data
- Flertal krisövningar lokalt på lärosäten (mer info kommer)
- En fysisk/hybrid kurs i nätverksforensik, vad vill ni göra nästa gång?
- Pågående upphandling för brandväggar (tillsammans med Nätenheten/Campusnät)
- Internt arbete kring SIM3-certifiering, Trusted Introducer
- Internt arbete kring genererade skyddsprofiler utifrån ISO27002
- Internt arbete kring policys, anvisningar och förbättrade rutiner

# Informationskanaler och samarbete

(främst för it/infosäkerhets personal, kontaktpersoner och IRT-personal)

- Öppethus: Vanligtvis zoommöte varannan vecka
  (ofta Torsdagar 10:00)
- CSIRT-forum (2-4 gånger per år, community-drivet)
- 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

# Prioriterade åtgärder för it-ansvariga

- Säkerställ att ni har en fungerande säkerhetskopia
- Segmentera nätverket
- Installera säkerhetsuppdateringar skyndsamt
- Begränsa behörigheter till relevanta roller, inte allmänna skrivrättigheter i stora utdelningar
- Inaktivera oanvända tjänster och protokoll (härda systemen)
- Separera och skydda användningen av högre rättigheter
- Tillåt endast godkänd utrustning i nätverket
- Aktivera multifaktorsinloggning, återanvänd inte lösenord
- Genomför utbildning i informationssäkerhetsmedvetande
- Testa er säkerhet, skall vi....?

# Andra delar av presentationer

Svarstidsmätning

Incidentstatistik

Sårbarhetsstatistik

Krisövningar

För frågor och uppföljning kring dessa presentationer så får ni höra av er till oss.