
SWAMID
Swedish Academic Identity Federation

SWAMID

Konsultation om förändring av SWAMID:s incidenthanteringsrutiner

2021-03-04

SUNET

Hur fungerar konsultationen

- SWAMID Operations skickar ut förslaget på SAML-admins
  - Skedde 19 februari
- Alla som använder SWAMID har möjlighet att kommentera och diskutera förslaget fram till 31 mars
  - SWAMID Operations anordnar ett zoommöte för kortpresentation och diskussion
- SWAMID Operations sammanställer resultatet av konsultationen och samråder med SUNET CERT om ev. ändringar
- Om ändringarna är små skickar SWAMID Operations uppdaterat förslag till SWAMID Board of Trustees för beslut

SWAMID

Bakgrund

- SWAMID genomgår just nu en fullständig policyöversyn med modernisering och tydlighet som fokus
- Under förra året uppdaterades SWAMID:s policy samt tillitsnivåer och i år är det incidenthanteringsrutinerna och teknikprofilerna
- Nuvarande incidenthanteringsrutiner infördes 2012 efter en säkerhetsincident inom federationen
- SWAMID behöver modernisera och harmonisera våra incidenthanteringsrutiner med andra federationer som vi samverkar med genom t.ex. interfederationen eduGAIN

SWAMID

Incidenthantering inom eduGAIN

- I eduGAIN finns sedan ett par år tillbaka en särskild funktion för att hantera säkerhetsincidenter, eduGAIN Security Team
- Teamet består av personer som är uthyrda till eduGAIN, på delar av sin arbetstid, för att hantera säkerhetsfrågor
- Under 2020 skrevs inom ramen för eduGAIN Security Team och arbetsgruppen för SIRTFI inom REFEDS incidenthanteringsrutiner för eduGAIN i eduGAIN Security Incident Response Handbook (eduGAIN SIR) och dessa är f.n. på väg att införas i eduGAIN

Förslag till nya incidenthanteringsrutiner

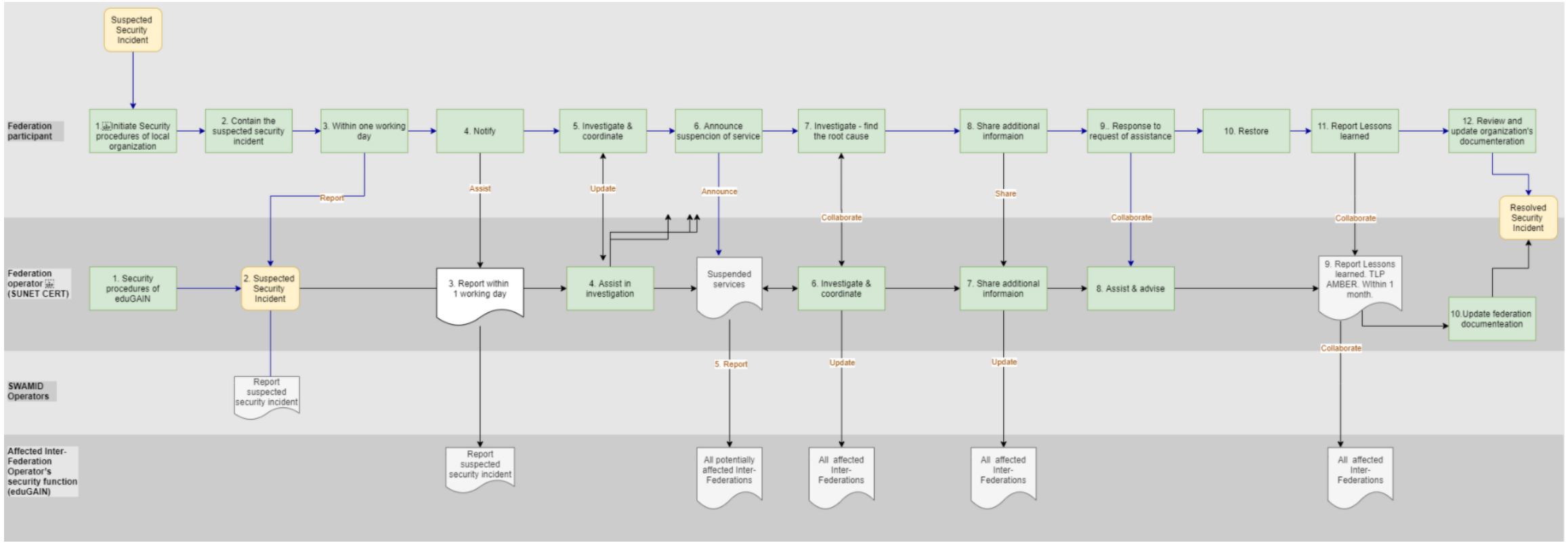
- SWAMID Operations har i samråd med SUNET CERT tagit fram ett nytt förslag på incidenthanteringsrutiner inom SWAMID
- De nya rutinerna bygger på eduGAIN SIR men är anpassade efter hur SWAMID är uppbyggt och fungerar
- Precis som i nuvarande rutiner är SUNET CERT säkerhetskontakt för säkerhetsincidenter inom SWAMID

SWAMID

Förslaget i korthet

- Incidenthanteringsrutinerna har två nivåer och dessa ska samverka
  - Federationsdeltagare – Identitetsutgivare och tjänster
  - Identitetsfederationen – SUNET CERT och SWAMID Operations
- Incidentrutinerna avser följande områden efter upptäckt
  - Informera
  - Begränsa
  - Undersöka
  - Åtgärda

Förslaget i en bild



SWAMID

Förslagets relation till REFEDS SIRTFI

- Inom SWAMID krävs inte att REFEDS SIRTFI används men det rekommenderas för både identitetsutfärdare och tjänster
  - För mer information om SIRTFI se https://refeds.org/sirtfi
- Förslaget uppfyller i princip avsnitt 2.2 Incident Response [IR] i SIRTFI förutom i två punkter
  - Krav i punkt [IR1] om säkerhetskontakt – kommer att hanteras i uppdaterad teknikprofil
  - Krav i punkt [IR2] om användarnas integritet – uppfylls av gällande dataskyddslagstiftning
- För de som idag inte uppfyller REFEDS SIRTFI finns för SUNET CERT ett ansvar att informationsdelning genomförs enligt SIRTFI

SWAMID

Dags för frågor och diskussion

- Vi kommer inte att gå igenom förslaget i detalj utan endast dyka ner där frågor och funderingar finns

- Ordet är fritt…

SUNET