GÉANT Security Operations Centre (SOC) Why, What, Where and Who

May 2024

SIG-NOC

GÉANT Operations Centre

Infoshare Contents

1. SOC Rationale & Timescales - **Why**
2. SOC – **What** does it do & Responsibilities
3. **Where** - does SOC fit into GEANT
4. Out of Hours Support
5. SOC – **Who** - Structure and Coverage
6. The Team and Current Work

SOC Rationale - Why

- GÉANT Board and EC led demand for enhanced cybersecurity
- World events and the rise of cyberthreats
- Protect critical infrastructure
- The increasing security related incidents that compromise the GÉANT assets
- The increasing investment in the GÉANT network as a long term asset
- The increasing complexity and breadth of the security toolset
- The restructuring of security teams within GÉANT
- NOC+SOC – Proven model already being followed by many partners
- Previous integration of Security toolset into GOC team led to suboptimal prioritisation and resourcing on both Security and Network Service issues:

SOC Timescales

- Q3 2022 - Agree Terms of Reference within GÉANT ✓
- Q3 2022 - Compile Job Descriptions ✓
- Q4 2022 - Commence recruitment ✓
- Q1 2023 - Initialisation of SOC ✓
- Q2 2023 - Meet with other NREN SOCs to compare models ✓
- Q2 2023+ - Develop and grow processes ✓
- Q3 2023+ - Training, outreach ✓
- Q1 2024 - Review SOC validity and value ✓
- Q1 2024+ - Operate ✓

SOC – What does it do – “Mission Statement”

Safeguarding the GÉANT Operational Assets by maintaining maximum possible vigilance at and within the network perimeter and acting to mitigate threats that may compromise GEANT and member assets. Supporting members’ security concerns.

What's It About

- **Operational Network Security**
- Managing/Operating Security Services
- Operational Security Support
- Maintaining Operational Security Awareness
- Protecting the GEANT backbone network
- Protecting NREN uplinks
- Expert Security Advice and Guidance to NRENs
- Fronts the GEANT CERT/CSIRT 1st Line

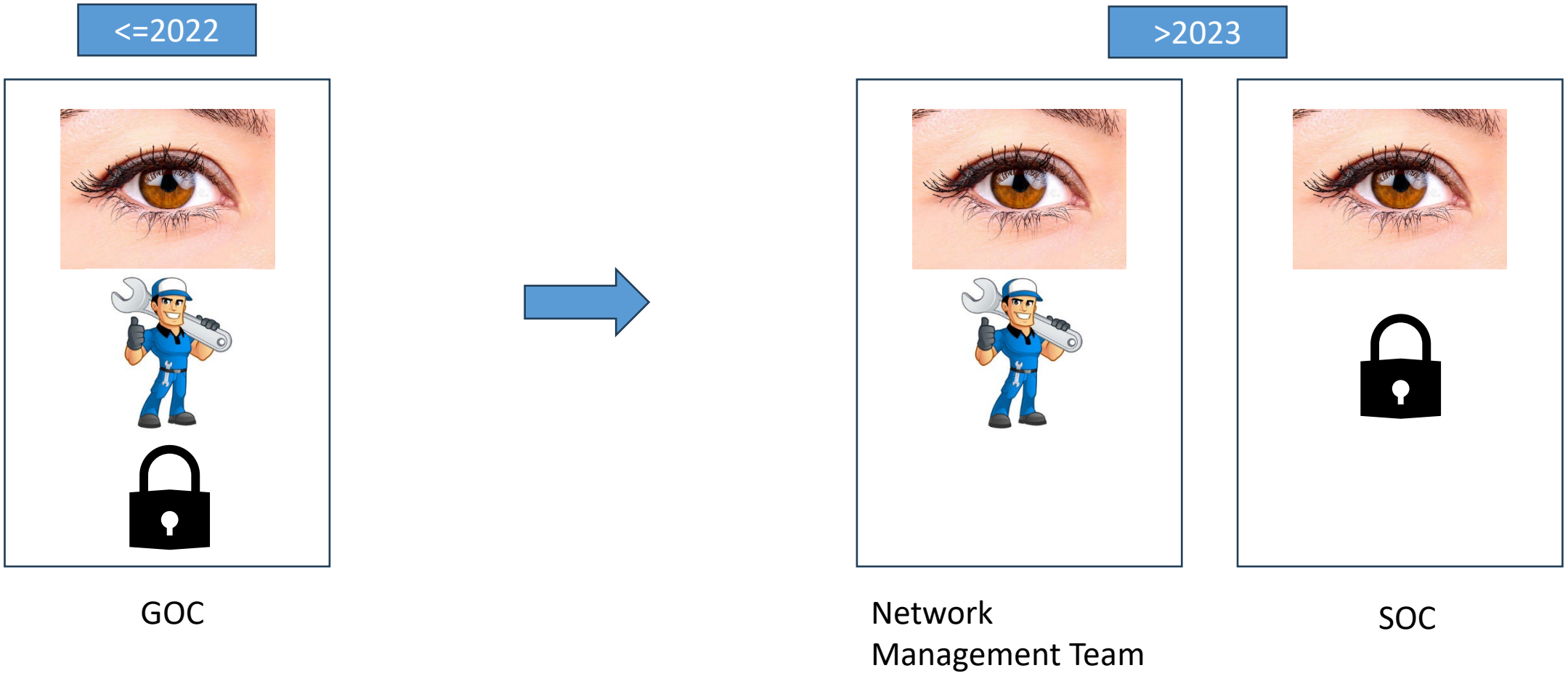
Some Responsibilities

- GEANT Security Services
  - DDoS Cleansing and Alerting Service
  - Firewall-on-Demand
  - Vulnerability Scanning Service (coming soon)
  - Trusted Certificate Service (coming TBC)
- Toolset
  - Manages **RPKI routing security application** and monitors for required actions
  - Anomaly Detection System – DataCentre
  - Scanning of internal assets (scanning as a service coming soon)
- BAU.
  - ACL design and composition recommendations
  - **Vendor Security Bulletin evaluation** and actions arising – in line with developed company security processes
  - Monitoring network operating systems for vulnerabilities, works with NetEng to agree actions
  - Protocol guidance, i.e. SSH versions etc
  - Ensure current best practice standards are followed for control and data planes, for example changes to RPKI routing security standards
  - SPLUNK rules for network equipment are maintained and monitored to ensure maximum security
  - Vulnerability monitoring where applicable
  - Threat Intelligence, receives and processes data from: Shadowserver
  - Qrator RADAR - Global Internet Routing anomalies
  - Periodic penetration testing of the network layer components for access and protocol vulnerabilities
  - Maintain company certifications and representations, i.e. FIRST, Trusted Introducer, GEANT CERT

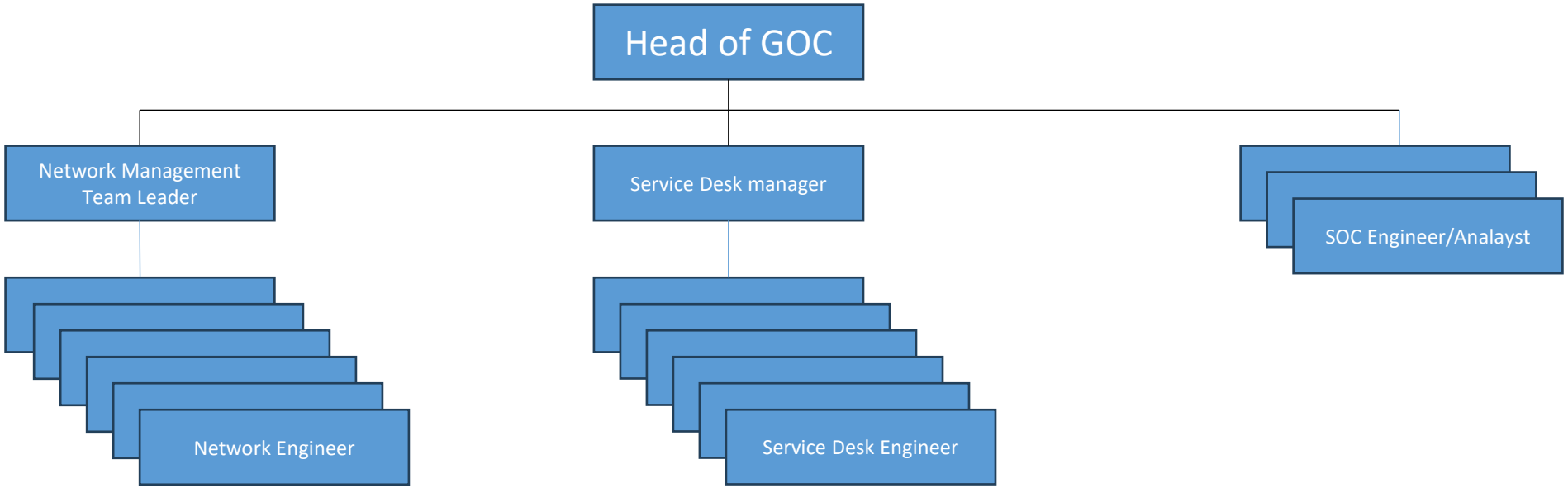
Out Of Scope for SOC

- Desktop computers and desktop applications
- Tools and Applications in general except where agreed i.e. TNMS/Intermapper
- Security Product Design
- Server Farms
- Server(+Virtual) hardware and Operating Systems
- Project software applications and COTS applications (That are not primarily operated by the GOC)
- Corporate office security except where agreed

Split out existing Security Work from within GOC

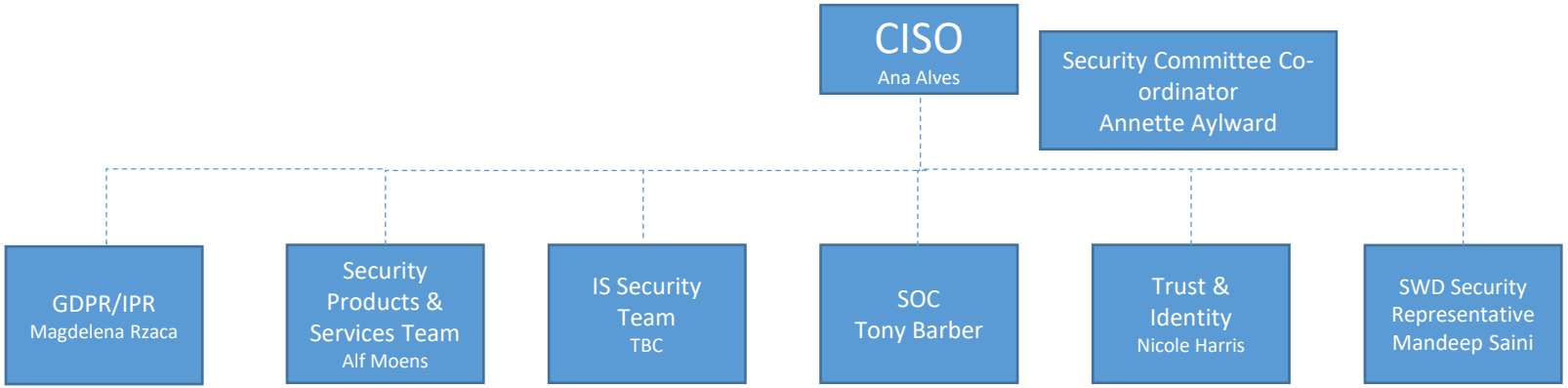


GEANT Operations Centre (GOC) Team Structure **2023 ->**



* Number of boxes is indicative only and does not represent number of staff

Where does SOC fit into GEANT Security 'Blanket'



1.GDPR issues
2.IPR

1.High Level Strategy
2.Product Design
3.GNT Project Security Coordination

1.Desktop & Web Services security
2.Patch Management
3.Corporate Security Management
4.Secure operation of end user devices

1.Operate Security Services
2.Protect the GNT Network Assets
3.Support Members

1.Develop and Deliver access solutions
2.Support identity federations
3.eduroam/eduGAIN/eduteams/InAcademia/MyAcademicID

1.Ensure good security practices are considered
2.Followup vulnerabilities requiring development & mitigation

Dotted line reporting to CISO. Not line management

SOC Coverage - Out of Hours Support

- Operates within GOC
- ~0830-1700 Monday to Friday
  - Best effort outside of hours –currently
- 24x7 cover (from SOC staff) not possible with available resources
  - Some repeatable tasks such as basic DDoS mitigation managed by NM engineers oncall out of hours

CERT – Computer Emergency Response Team

- CERT is an externally advertised concept – GEANT CERT, CSIRT etc

  = cross team expert group
- SOC & SD are CERT first line
  - CERT 2nd line are other internal experts

Who are the GEANT SOC Team

- Laurentiu Sandu-Bufi
- Ryan Richford
- Mohammad Hussain Faqeri
- 3-month Undergraduate intern summer of 23 and 24

Laurentiu Sandu-Bufi

- DNSSEC Deployment
- Hardening GEANT authoritative DNS

Mohammad Hussain Faqeri

- Kentik alerting system
- Creating parent polices
- Defining threshold
- Notification channel

Ryan Richford

- ADS
- DDoS Cleansing & Alerting
- Scanning (Nessus, IVRE & Outpost)

Questions