Setting up a Security Operations Center/Cyber Defense Center

Darmstadt, 15th of March 2022, 6 pm.

Project Management Institute Germany

Speaker 1

LinkedIn

Website

Jutta Edith Zilian CISA, CISM, CGEIT, PMP, CAPM, Mag.

- Project Management and Information Security Consultant (since 1994)
- University degree 1994 (Magister, Leopold Franzens Universität Innsbruck)
- in IT since 1993
- Projectmanagement since 1996
- IT Security since 2004
- Information Security since 2006
- ISACA Workinggroup IT Compliance
- PMI Germany Chapter Chapter Operations (CISO) & Head of Volunteering

Project Management Institute. Germany

Speaker 2

LinkedIn

Website

Ernesto Hartmann Chief Cyber Defence Officer

- Member of the executive board and responsible for the cyber defense center
- Development of managed detect and response services
- Information Security since 2001

Agenda

- Mandate for the project (why we like to undertake this)
- Request for proposal (RfP)
  - Current market
- Considering the EBA Guideline on outsourcing arrangements
- Critical Infrastructure (KRITIS)
- Request for Proposal (RfP) and Request for Quotation (RfQ) process itself
- Setup a Security Operations Center/Cyber Defense Center (the project itself)
- Do´s, Don'ts and pitfalls

Project Management Institute. Germany

Mandate (why we like to undertake this)

- **If you are in regulated branch**
  - Financial Sector –
    - European Union (EU)
      - European Insurance and Occupational Pensions Authority (EIOPA)
        - Germany: VAIT
      - European Banking Authority EBA (Financial Sector)
        - Germany: BAIT
    - Switzerland
      - FINMA
    - Austria
      - No local regulations anymore (refer to EIOPA and EBA)
  - Critical Infrastructure (KRITIS)
- Other branches
  - Digitalization, Cybercrime

Project Management Institute. Germany

Make or buy (Outsourcing)

- If you like to setup your SOC Project alone keep in mind
  - Building up a SOC/CDC from scratch takes at minimum 2 years till it´s running smooth
  - Can your organization effort a real 7x24 onsite duty?
  - Do you have the technical knowledge on stock?
    - Keep in mind the market is empty
- If you build up a hybrid SOC/CDC
  - Your outsourcing partner has the knowledge and the staff for 7x24 operations
  - Your staff will build up the knowledge or keep it
  - It´s real partnering
- Fully managed SOC/CDC Outsourcing
  - You loose knowledge
  - Who is capable to do the triage?
  - Keep in mind – **even here you need a „retained organization“ inhouse!**

Request for proposal and quotation

- Decide if you will go for an RfP only or (preferred from my side) go for an RfP/RfQ combination directly
- What are your requirements for the location of the SOC/CDC?
  - EU/EEA/Switzerland only?
  - Outside this area –General Data Protection Regulation (GDPR) equivalent in place?
  - In case of healthcare or insurance which offers health care insurance
    - § 203 Criminal Code Germany / § 203 StGB Germany (about special professional groups, even it´s not that tight anymore as it was prior to 2018)
    - Health Insurance Portability and Accountability Act (HIPAA) USA

Request for proposal and quotation

- SOC/CDC requirements
  - Real 7x24 on site duty required? Be careful, if you need it, some provider offer a on call duty during night shift only
  - SIEM requirements
    - If you already have one, do you want to keep it?
    - Which generation SIEM is acceptable for you?
  - E D R requirements
    - If you already have one, do you want to keep it?
    - Is it a must that the provider offers this to you fully managed?
      - Is a integration of an E D R in the SOC infrastructure only, acceptable for you?
  - Do you have a vulnerability management in place?
    - Mandatory for the RfP?

Request for proposal and quotation

- SOC/CDC requirements
  - Don´t forget the **„RIGHT TO AUDIT CLAUSE“** – don´t forget to write it into ANY outsourcing agreement!
  - Due to which standard should the Outsourcing operator be certified?
    - PCI/DSS needed?
    - Are you fine with ISO 22301, ISO 27001 only?
  - SOC / CDC Staff
    - L1-L3 Level SOC Analysts needed? Or do you want to perform L3 analysis by yourself?
  - Project Scope
    - How many use cases needs to be included?
    - How many threat intelligence feeds?
    - etc. ….

Request for proposal and quotation

- SOC/CDC requirements
  - Governance
    - Audit of, but not limited to:
      - KPI
      - KGI
      - SLA
      - Use Case Lifecycle
      - SOC FTE Verification
      - False negative verification
      - All data for verification must be audit proof saved
        - Chain of custody

Project Management Institute. Germany

Gartner

International

MSSP

Market Overview

Project Management Institute. Germany

High level market overview (beside Gartner)

- IBM Wroczlav, Poland (English speaking)
- Airbus Ottobrunn/Taufkirchen (German and English available)
- Fujitsu
- NTT
- CGI Northern part of Germany (German speaking)
- DXC Southern part of Germany (German speaking)
- 2 out of the Big 4 (EY, Deloitte)
- ……

Project Management Institute. Germany

Current Regulations

European Banking Authority (EBA)
https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements

https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

Bundesanstalt für Finanzdienstleistungsaufsicht (BAFIN)
https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html

Eidgenössische Finanzmarktaufsicht (FINMA)
https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2008-21-20200101.pdf?la=de

Project Management Institute. Germany

Current Regulations

Critical Infrastructure - KRITIS
https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html

https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html

Branches
https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html

https://www.bbk.bund.de/SharedDocs/Bilder/DE/Infografiken/KRITIS/Sektoren-Kuchen.jpg?__blob=normal&__ifc=large&v=6

RFP Process

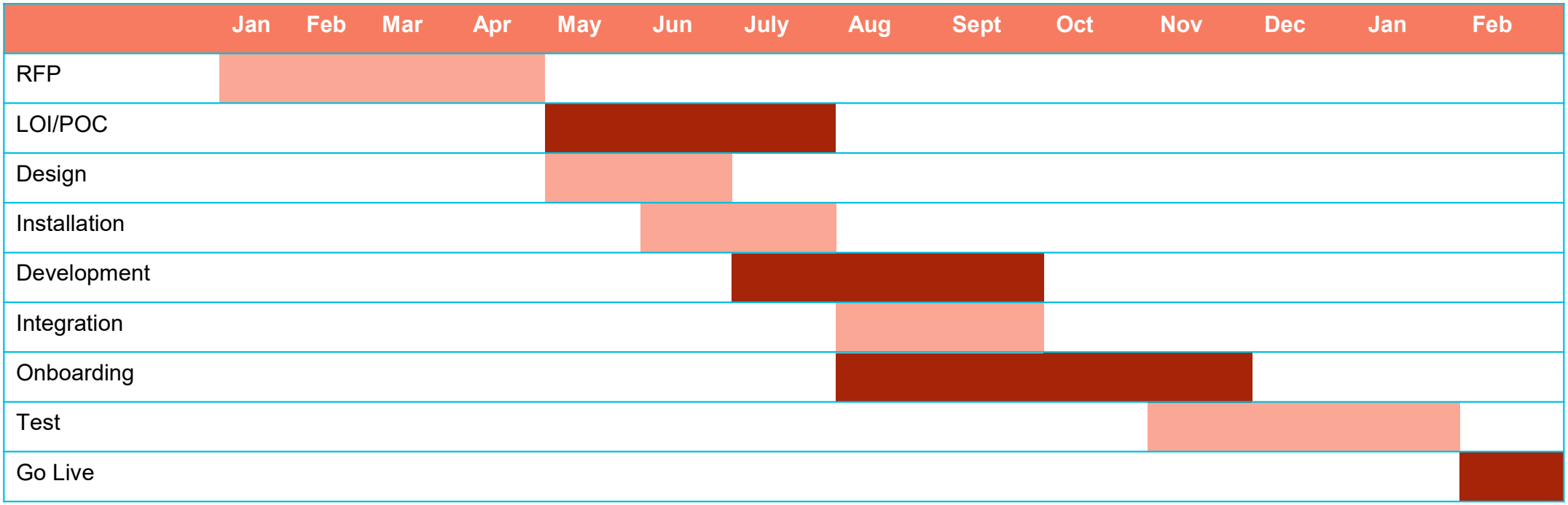
- Build a longlist
  - Ask them, if they like to have your RfP
  - Ask them to sign an NDA for the RfP
  - Send them the RfP (RfQ included)
- Provide a specific date and time till when you accept offers
- Weight the offers
  - Those with the lowest sum at the end, don´t need to be a lowest bid
    - Make them comparable
- Build a shortlist (3 up to 5 bids)

Project Management Institute. Germany

RFP Process

- Build a shortlist (3 up to 5 bids)
- Invite them to present their bids
- Conduct a workshop with the Top 3 vendors you have chosen
- Call for Best and final offer
- Chose your vendor
- Sign a letter of intent with them or conduct, if necessary, a Proof-of-concept phase first
- Run the real SOC/CDC Setup Project
- Have fun!

Project Management Institute. Germany


Jan
Feb
Mar
Apr
May
Jun
July
Aug
Sept
Oct
Nov
Dec
Jan
Feb
RFP
LOI/POC
Design
Installation
Development
Integration
Onboarding
Test
Go Live

Project Management Institute Germany

InfoGuard
SWISS CYBER SECURITY

SETTING UP A SECURITY OPERATIONS CENTER (SOC) / CYBER DEFENCE CENTER (CDC)

Ernesto Hartmann, Chief Cyber Defence Officer, InfoGuard AG

Cybersecurity Glossary
https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

SANS Institute Security Glossary

https://www.sans.org/security-resources/glossary-of-terms/