



The cyber attack on Hydro

- and how our SAP system was affected

SBN 2019, SAP User Conference Norway

23 September 2019

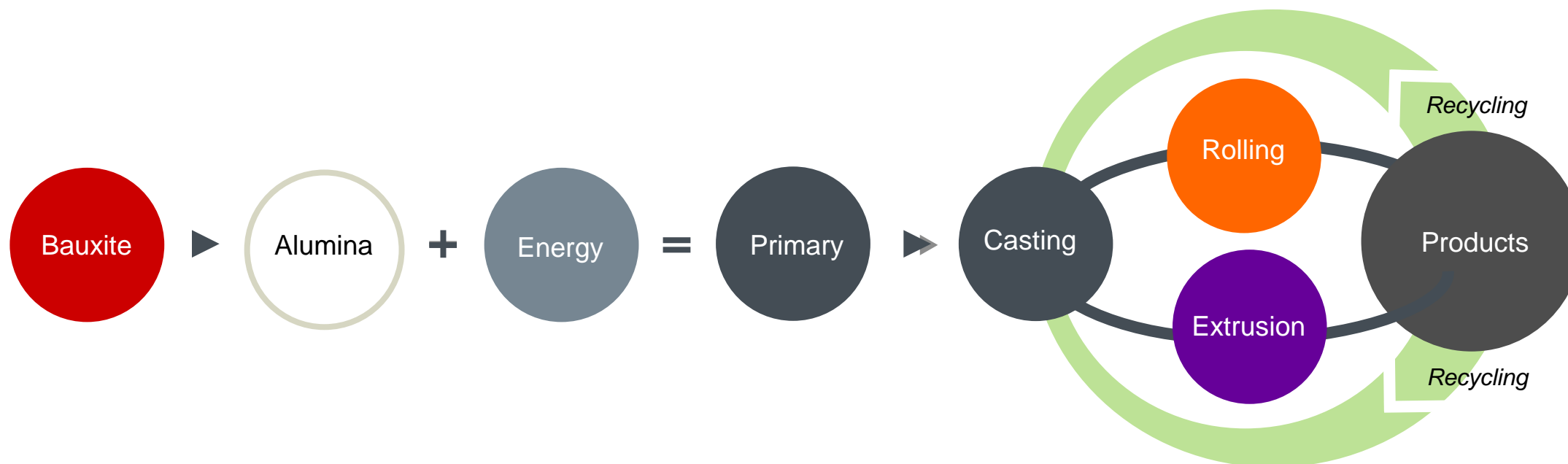
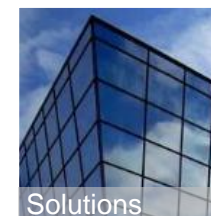
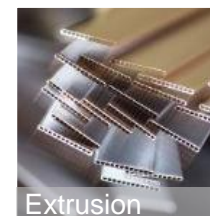
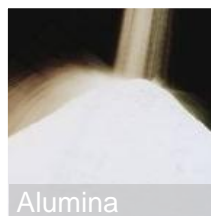
Digital Marshall & CISO, Torstein Gimnes Are

Principal Architect Security, Georg Bell

Hydro 2019: world-leading in the aluminium value chain



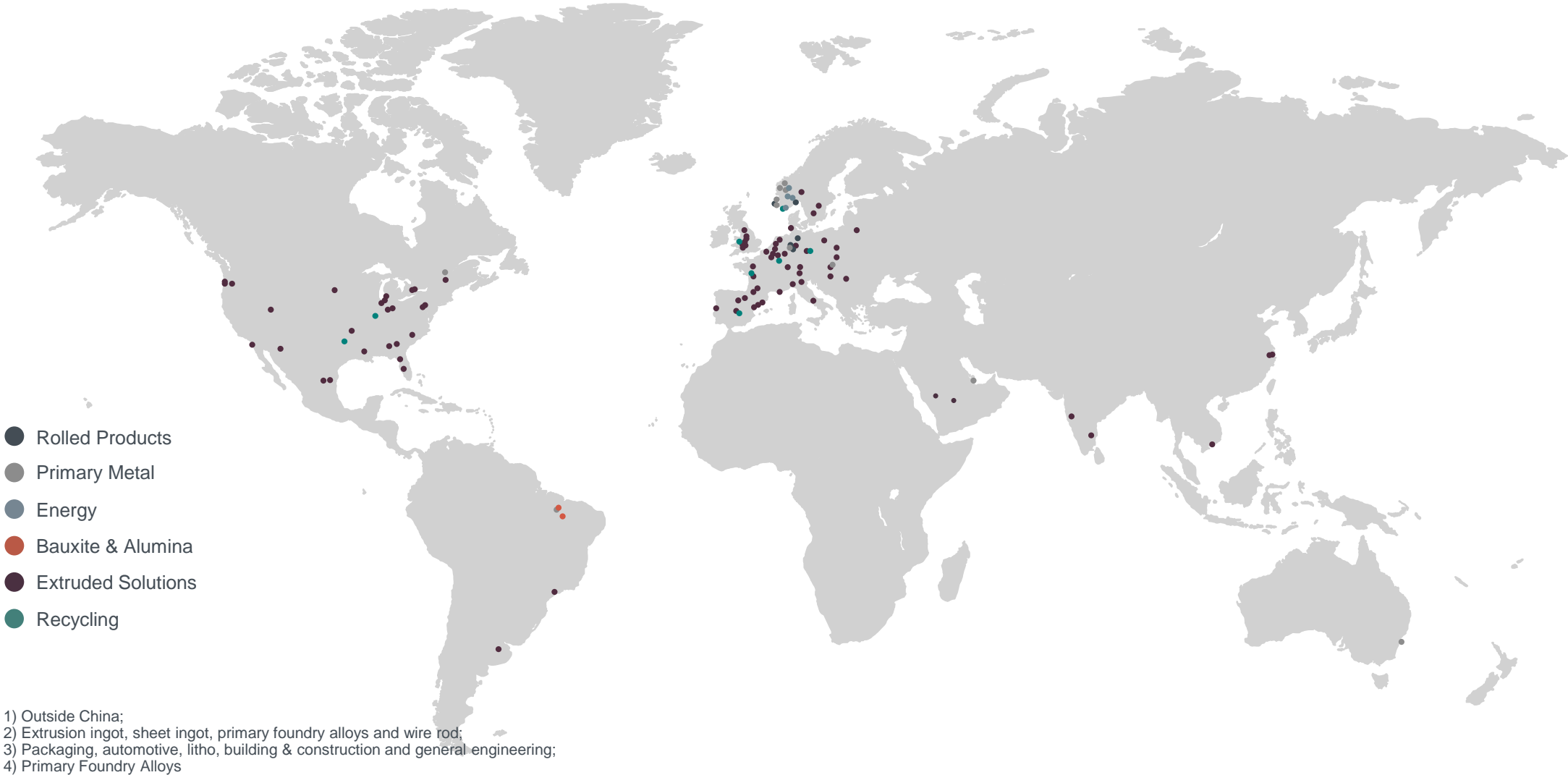
35 000 employees in 120 plants in 40 countries, 30 000 customers on all continents



A truly global aluminium company



More than 150 production sites along the entire value chain



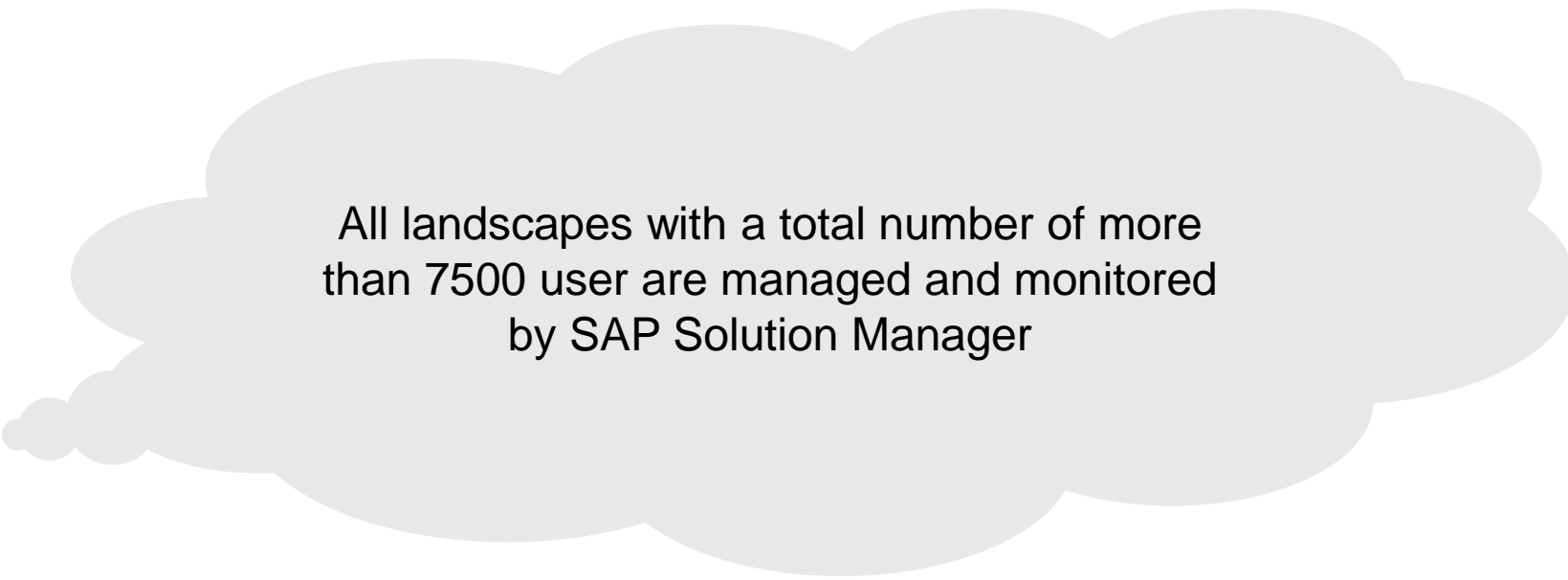
01

Hydro's SAP security
status prior to the
cyber attack

Hydro's SAP footprint

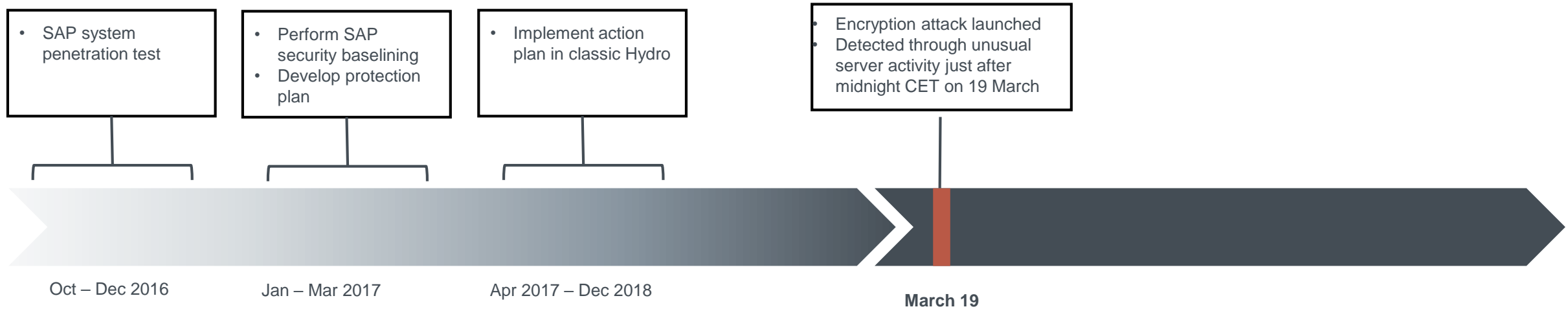


- 5 ERP landscapes
- 1 BW4/HANA landscape
- 1 HCM landscape covering Germany
- 1 GRC landscape (not productive yet)
- 2 PI/PO landscapes

A large, light gray thought bubble with a small tail pointing towards the list of landscapes.

All landscapes with a total number of more than 7500 user are managed and monitored by SAP Solution Manager

SAP Security improvement journey 2016 – 2018



01

Cyber attack impact on SAP environment

Cyber attack impact on SAP environment

Direct technical impact on SAP environment

- No direct impact (infection) of SAP instances
- Some impact on support systems like e.g. jump server

Indirect technical impact on SAP environment

- DNS resolution issues for some user / sites
- Communication issues due to network restrictions

Questions raised by management:

Have been our SAP systems or it's data be targeted by the attack?

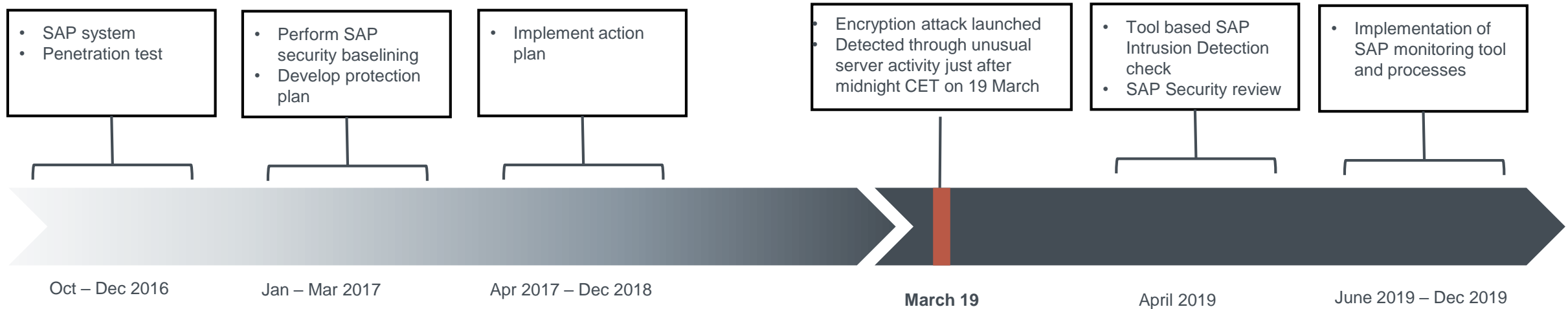
Are we well enough prepared to recognize such attacks in the future?

High level answer to the questions raised by management

- Has our SAP systems or it's data be the target of the attack?
 - Forensic investigation has shown no suspicious activities by user or by the system itself
 - Tool based review of SAP log files
 - Manual investigation of unclear monitoring events
 - Review of relevant master data by business
- Is Hydro well enough prepared to react on future attacks?

- **Real time monitoring of SAP systems is required**
- **Align processes with SOC Team**
- **Alert handling procedures must be defined**

SAP Security improvement journey



01

SAP security monitoring tool implementation

Key risks to be mitigated by the SAP Security monitoring tool

- Application level monitoring

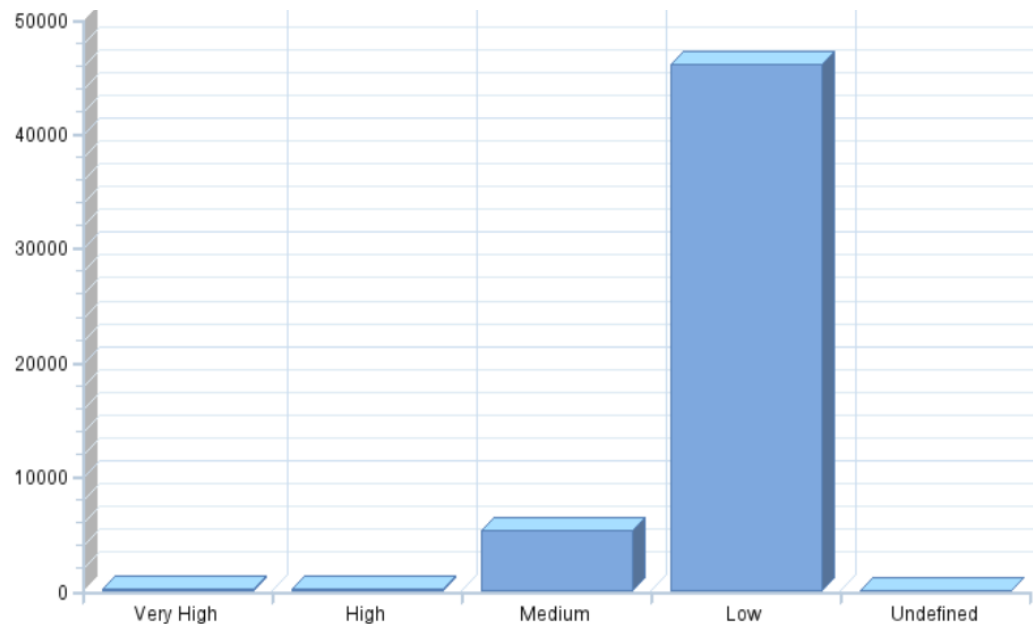


- **Manage and minimize the attack surface**
 - Perform a baselining first to get an overview of the risks
 - Fix issues based on priorities
- **Get alerted on potential hacking attack**
 - Consider process to handle planned maintenance activities
 - Apply filter to avoid false alarms
- **Manage vulnerable code**
 - Define the baseline and fix issues based on priorities
 - Keep the code base clean by adjusted development process and QA process
- **Follow up critical access to business functionality and data**

Key tasks during a security tool implementation

Events by severity

Severity	Total count
Very High	3
High	31
Medium	5.127
Low	45.885
Undefined	0



- **Requirements to avoid false alarms**

- Define who is allowed to perform critical activities on the system
 - SAP Basis activities like changing RFC connections
 - SAP authorization activities like role and user maintenance
 - Critical RFC calls which are allowed for defined communication partners

- **Align system maintenance process with security monitoring process**

- Avoid false alarms during agreed maintenance processes
- Review performed maintenance activities

- **Enable organisation to react asap on Very high alerts**

- Routing of alerts classified as very high to central SOC team
- Define and maintain contact matrix for all systems

- **ABAP code related vulnerabilities**

- Define what is important to fix asap
- Define what is important to avoid in the future
- Review development process and related QA

Key learnings

- SAP security is a journey, especially if systems have a long lasting legacy
 - Consider a penetration test to facilitate a kick start
 - Security baselining and a risk analysis based on penetration test and SAP Secure Operations Map
 - A monitoring tool implementation requires a good understanding of the security baseline
 - To be successful, roles and responsibilities must be clarified during the implementation of the monitoring tool and it's related processes

SAP Secure Operations Map

Security Compliance	Security Governance	Audit	Cloud Security	Emergency Concept
Secure Operation	Users and Authorizations	Authentication and Single Sign-On	Support Security	Security Review and Monitoring
Secure Setup	Secure Configuration	Communication Security	Data Security	
Secure Code	Security Maintenance of SAP Code		Custom Code Security	
Infrastructure Security	Network Security	Operating System and Database Security	Frontend Security	

01

Background material & additional reading

SAP penetration test 2016

- Implemented risk mitigation

- **Network**

- New network security concept

- **SAP system setup**

- One instance per virtual machine (VM)
- Maintain SAP gateway access control lists (reginfo / secinfo)
- Define default values for security related parameter
- Remove weak password hash codes from systems

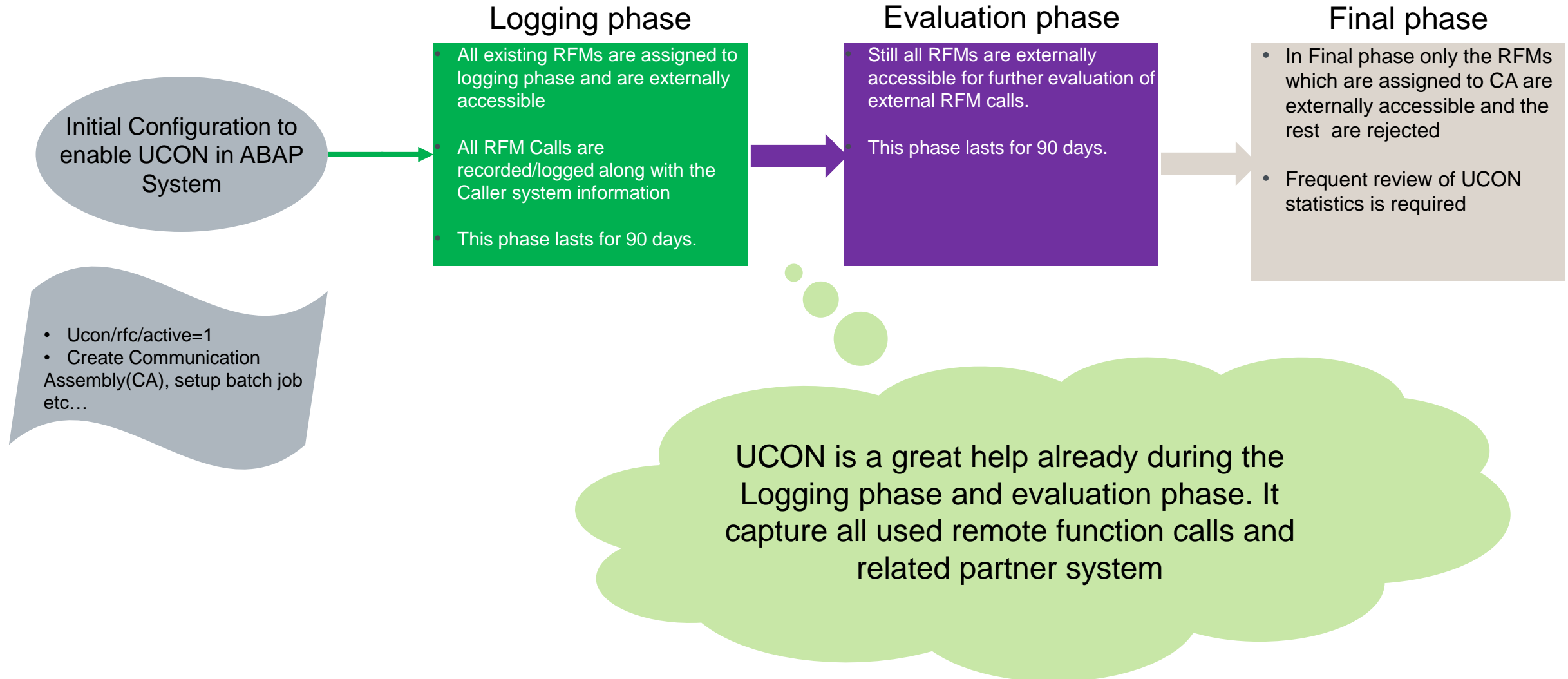
- **Setup of SAP interfaces**

- Reset password of interface user to enforce strong passwords
- Remove critical authorizations from interface roles
- Implement UCON (SAP Unified communication)

- **Additional measures**

- Check and adjust SAP Security Audit Log retention time
 - 400 days for productive system
 - 100 days for non productive systems
- Monthly OS patching
- Monthly implementation of SAP security notes
- Implement SAP Security monitoring processes
 - SAP Solution Manager Configuration validation
 - SAP Security Business process Monitoring

UCON in a Nut Shell



Relevant links

SAP Secure Operations Map

https://support.sap.com/content/dam/support/en_us/library/ssp/offerings-and-programs/support-services/sap-security-optimization-services-portfolio/SAP_Secure_Operations_Map.pdf

SAP Security baseline template

https://support.sap.com/content/dam/support/en_us/library/ssp/offerings-and-programs/support-services/sap-security-optimization-services-portfolio/Security_Baseline_Template.zip

Securing remote function calls

<https://launchpad.support.sap.com/#/notes/2008727>

Key risks to be mitigated by the SAP Security monitoring tool

- Application level monitoring – detailed view

- **Manage and minimize the attack surface**
 - Monitor SAP system parameter changes
 - Monitor changes of interfaces connections
 - Monitor system / application server restart
- **Get alerted on potential hacking attack**
 - Monitor unsuccessful logins for end user and interfaces to identify potential hacking attacks
 - Monitor unauthorized changes to roles and user
 - Monitor unclassified / unapproved function calls from outside the SAP system
 - Monitor unauthorized access to password hash codes
 - Assignment of authorization to own account
- **Monitor execution of vulnerable code**
 - Follow up the creation of vulnerable code at development system → inform developer to get it fixed
 - Follow up the execution of vulnerable code on productive system → inform development manager to follow up
- **Follow up critical access to business functionality and data**
 - Monitor manual data manipulation in production system using the developer tool called debugger
 - Monitor access to defined critical transactions from non Hydro PC
 - Monitor the download of data based on defined rules
 - Monitor deletion of lock entries (Follow up data consistency)



Hydro

We are aluminium

