

INDUSTRIAL AUTOMATION

ABB Ability™ Cyber Security Services

An overview of the available and upcoming cyber security services from ABB

Kees van Overveld – Global Product Manager Cyber Security Services

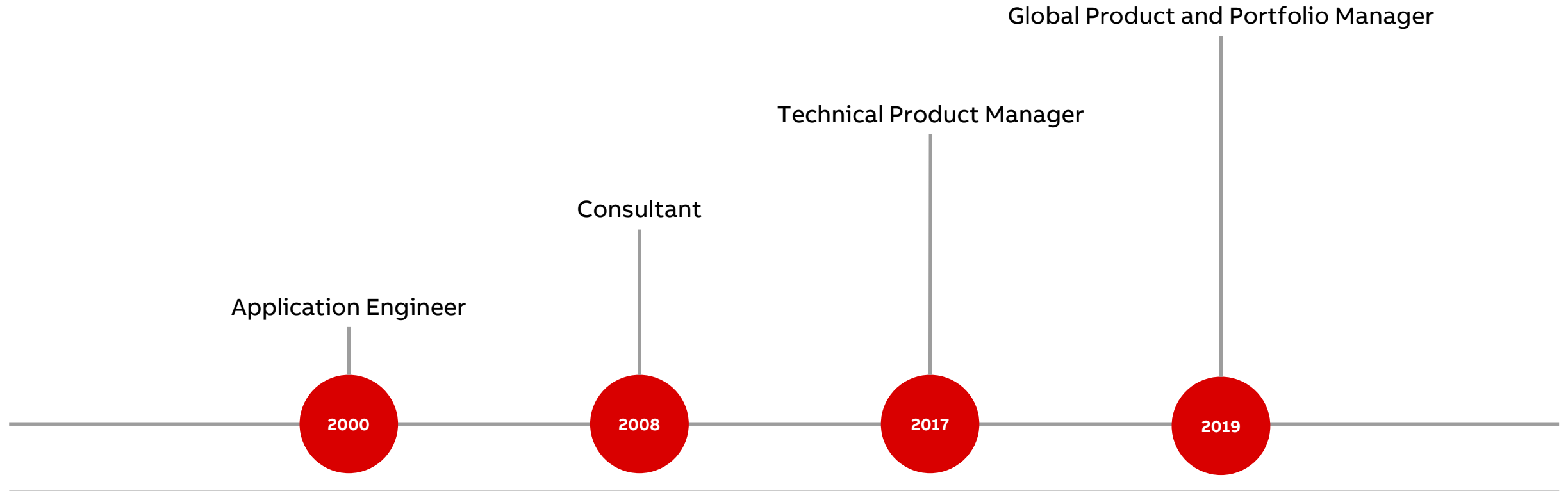




About Me

Kees van Overveld

Global Product & Portfolio Manager IA-PCP

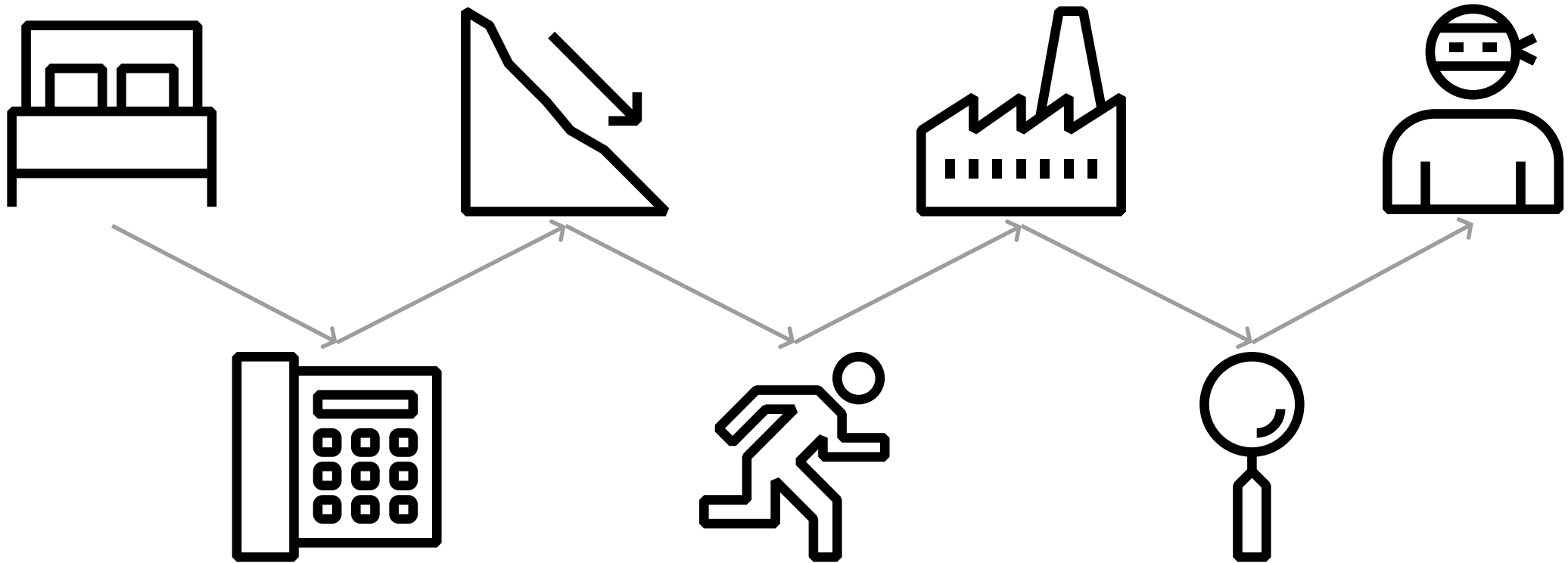




Scenario

Scenario

What?

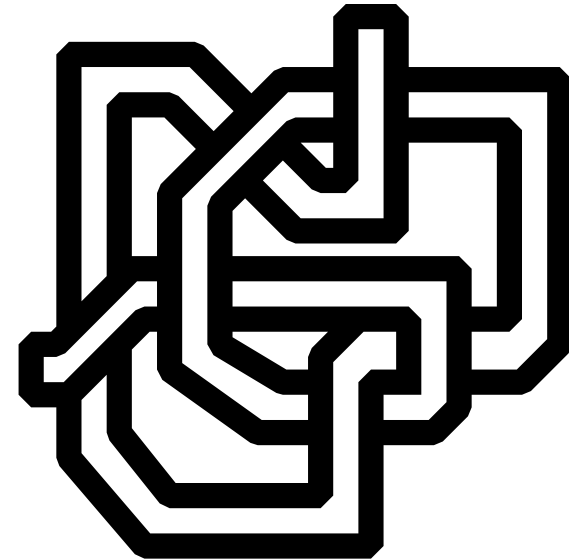


Scenario

Complicated

Analysis

- Hacker had access for several months already
 - Plenty of time for information gathering and analyzing your process
- Backups were outdated
 - Some even non-functional



Scenario

How

Analysis

- Employees did not know how to handle removable media
- Malware protection was disabled
- No patches were installed
- Back-ups were taken infrequently, incorrect and never tested
- Network connections were bypassing the firewall
- Service account was used for day-to-day work



—

It is not fiction, it is real!

The background of the entire page is a photograph of a large industrial facility, likely a hydroelectric power plant. The scene is filled with complex machinery, including large metal structures, pipes, and walkways. The lighting is a mix of bright overhead lights and softer ambient light, creating a sense of scale and industrial activity. In the top right corner, there is a small white label with the text "PTM 2".

Norsk Hydro

Hydro subject to cyber attack

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday (CET), impacting operations in several of the company's business areas.

IT-systems in most business areas are impacted and Hydro is switching to manual operations as far as possible. Hydro is working to contain and neutralize the attack, but does not yet know the full extent of the situation.

Published: March 19, 2019

Source:
<https://www.hydro.com>

Update on cyber attack April 12

During the week, Hydro has made further progress towards normalizing operations after the cyber attack, which struck Hydro on March 19.

Source:
<https://www.hydro.com/en/media/news/2019/update-on-cyber-attack-april-12/>



ASCO

De tijdelijke werkloosheid door overmacht wordt nu verlengd tot volgende week vrijdag, zegt de personeelsdirecteur en woordvoester Vicky Welvaert. Dat zou de derde week zijn dat het bedrijf stilligt.

De Zaventemse groep Asco, die gespecialiseerd is in vliegtuigonderdelen van onder andere het F-35-gevechtsvliegtuig, ligt nog langer deels lam als gevolg van de aanval met ransomware die de groep op 7 juni trof.

Source:

<https://www.tijd.be/ondernemen/luchtvaart/asco-ligt-al-derde-week-stil-na-cyberaanval/10138910.html>

NETHERLANDS



10 MOST-ATTACKED COUNTRY

OAS	15458
ODS	8238
MAV	549
WAV	13243
IDS	98139
VUL	526
KAS	383414
BAD	1

Detections discovered since 00:00 GMT

[More details](#)

Share data







DEMO ON

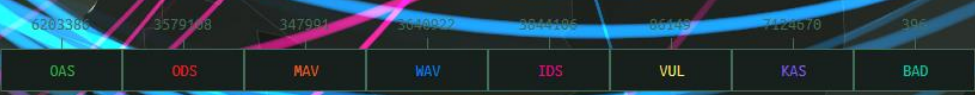


ABB has services to help protect your assets

ABB Ability™ Cyber Security Services

Portfolio aligns with NIST Cyber Security Framework

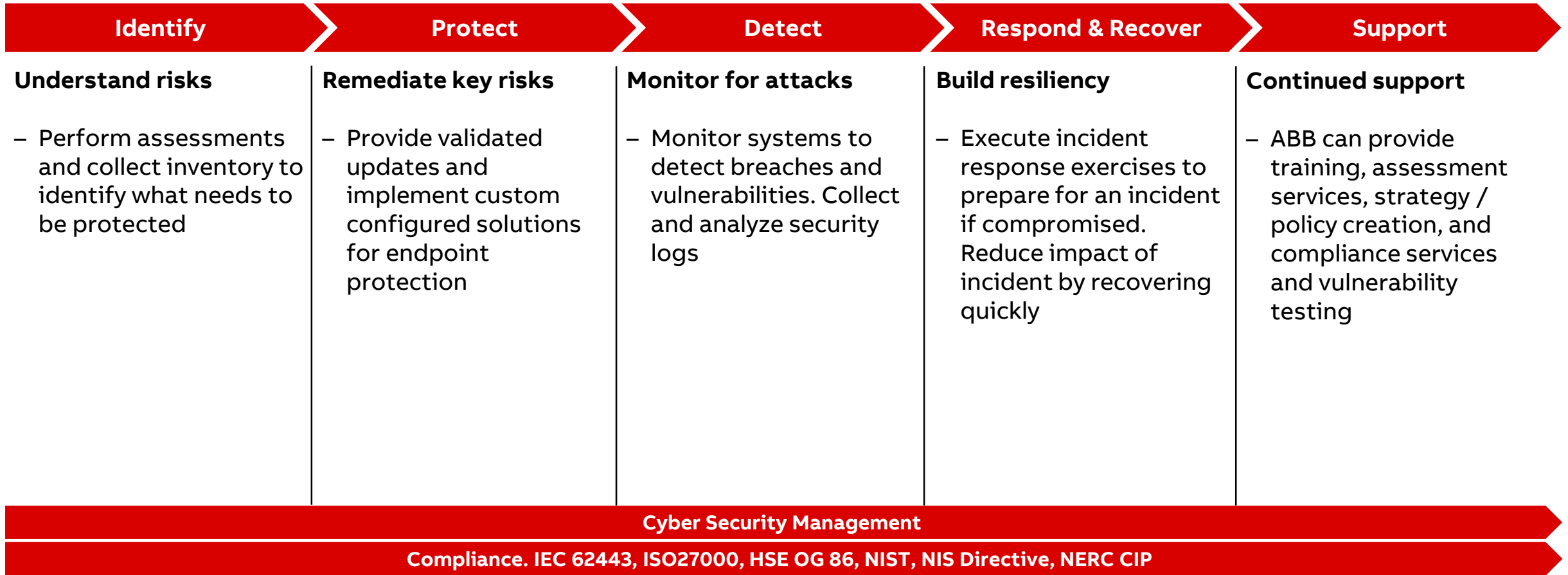


ABB Ability™ Cyber Security Services

Portfolio aligns with NIST Cyber Security Framework

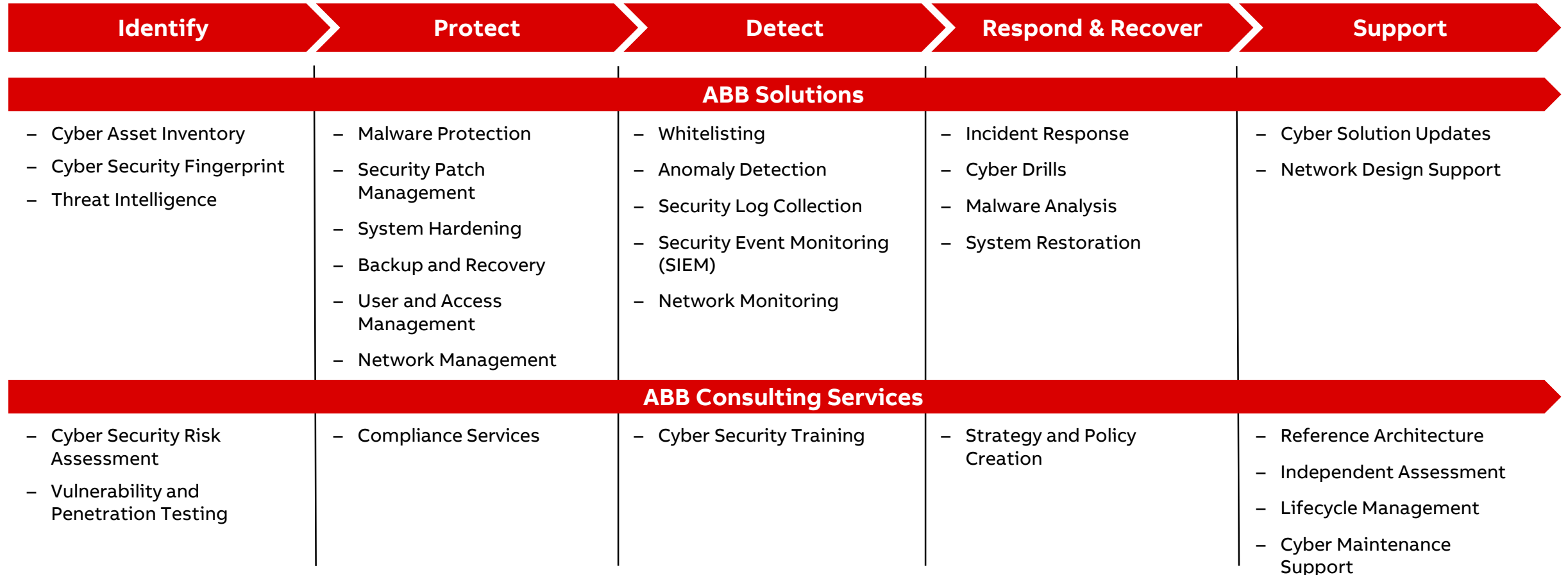


ABB Ability™ Cyber Security Asset Inventory

Would have detected the unknown devices

Key functions

- Passive probing of the network
 - Using SPAN/MIRROR
 - New devices which communicate will be automatically detected
- Results enhanced with information from active probing

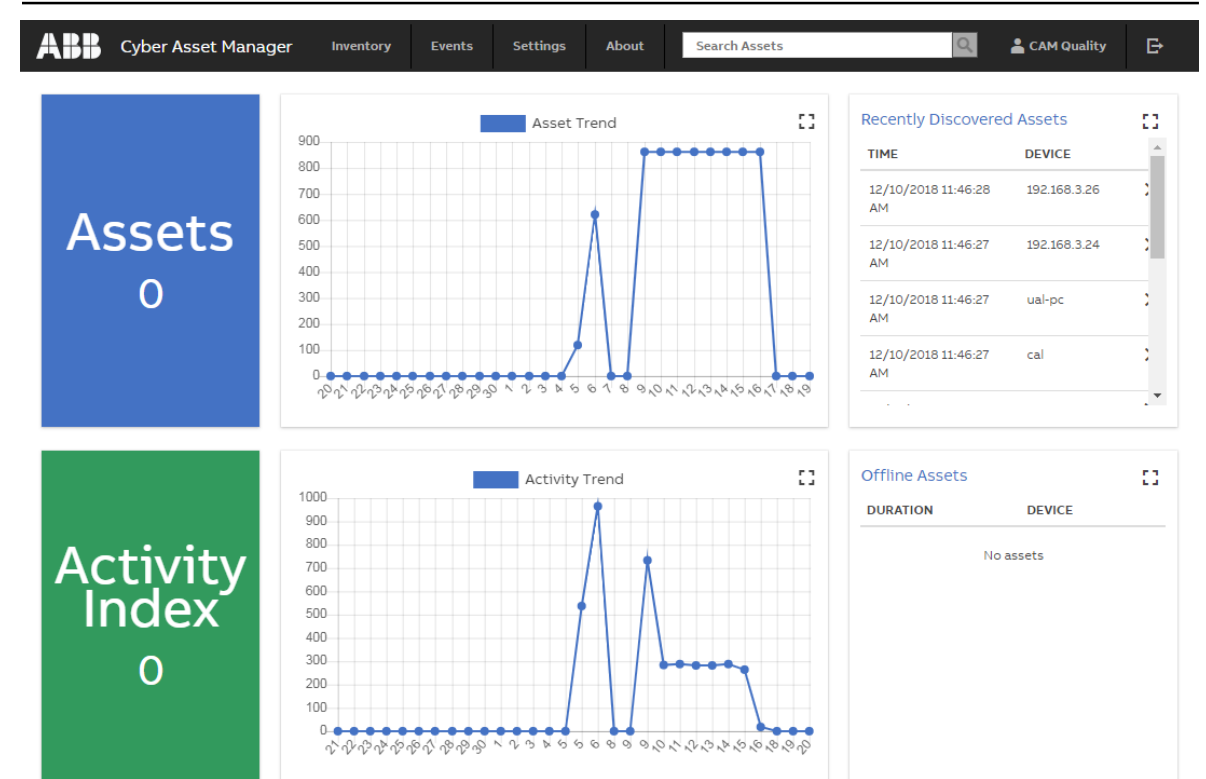


ABB Ability™ Cyber Security Fingerprint

Would have detected the inactive malware protection, missing updates and more

Key functions

- Data collector & analysis towards KPIs
- Fingerprint following the MCS Fingerprint philosophy
- also available in Service App on Laptop

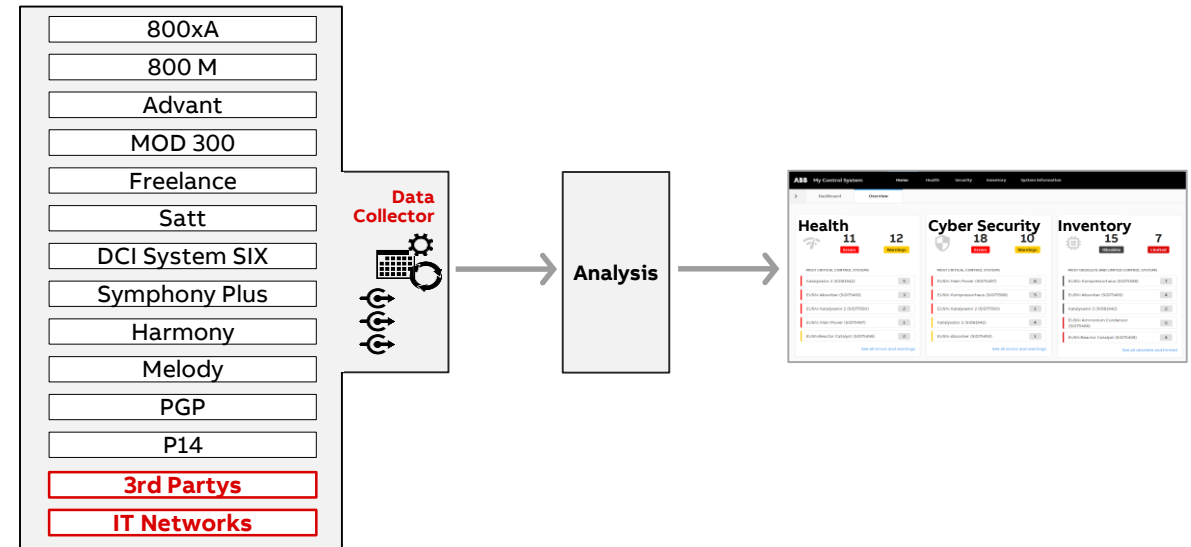


ABB Ability™ Cyber Security Endpoint Protection

Would have detected the malware

Key functions

- Traditional Anti Virus
 - Still a “must have”
 - Current support for McAfee VirusScan Enterprise and Symantec EndPoint Protection
- Whitelisting
 - SE46 is EOS and EOL end of 2019
 - Validating McAfee Application Control as replacement*
- 3rd Party EPP Validation-as-a-Service**
 - New technologies for EPP change the market
 - Growing variety of suppliers and solutions
 - A validation service for 3rd party software allows to support customer requests, which are not covered out of the box

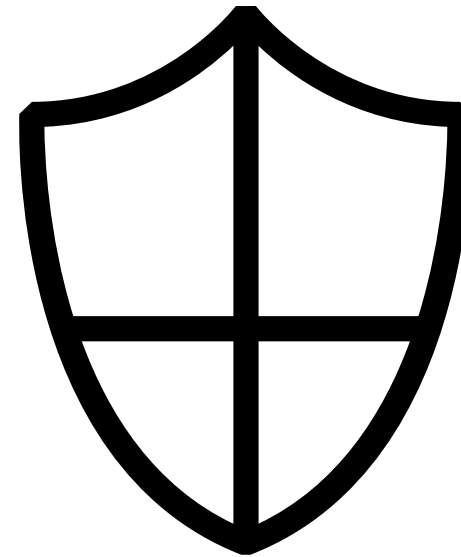


ABB Ability™ Cyber Security Updates

Would have prevented using known weaknesses in the system

Key functions

- Online deployment
 - Via local WSUS
 - Via Service Station*
- Offline deployment**
 - Via import to a local WSUS
 - Via import to the Service Station*

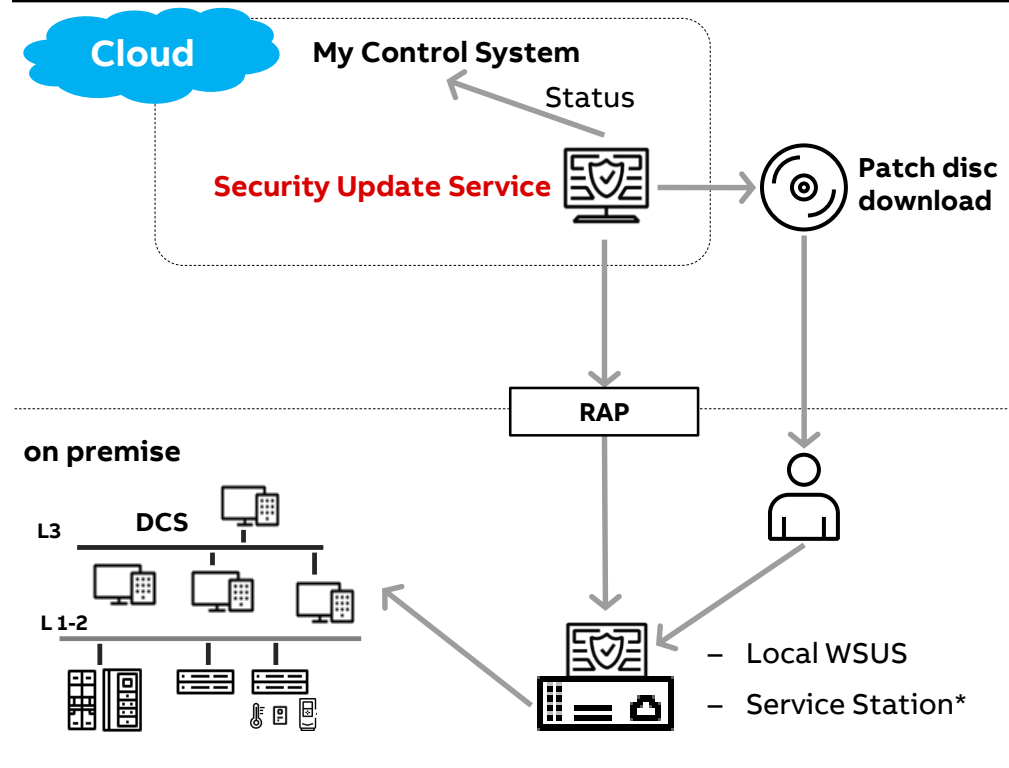
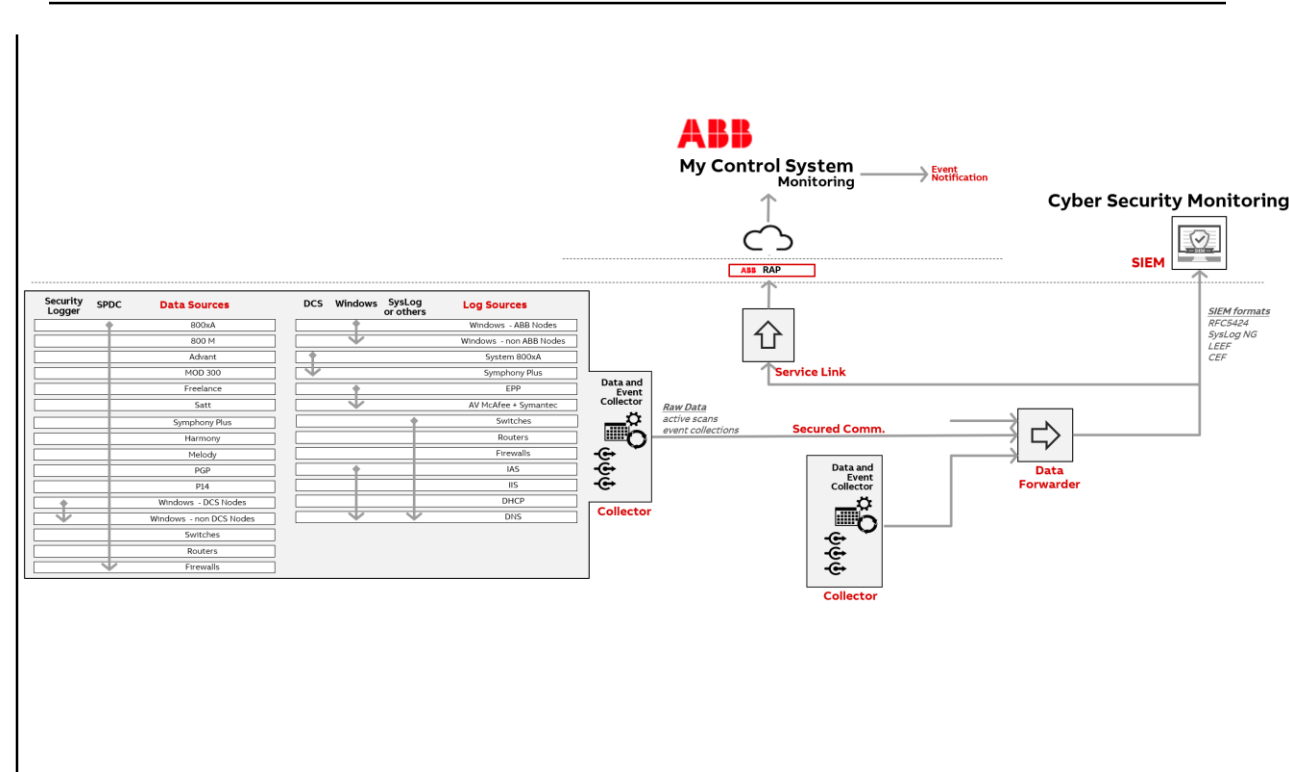


ABB Ability™ Cyber Security Event Monitoring*

Collect events and forward to a SIEM solution

Key functions

- Collector and forwarder for events to various SIEM's in market
 - Supporting Syslog RFC 5424, LEEF and CEF formatting
 - Adding the SID as unique identifier to the message
- Support active ABB control systems
- Use of on-Premise MCS for
 - Preprocessing of events with correlation rules
 - Log Aggregation
 - Monitoring and reporting

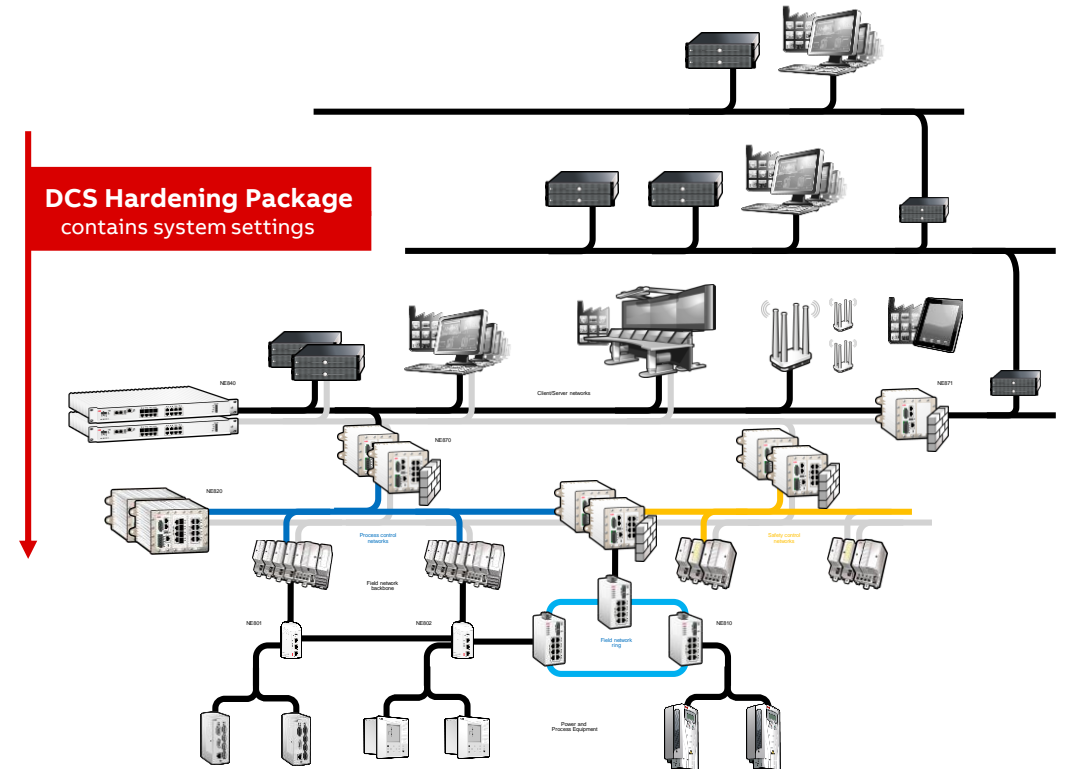


Hardening Services

Would have prevented usage of removable media

Key functions

- Standardization across Business Units/Countries
- Support New Windows Operating Systems
- Support Hybrid Control Systems
- Native Product Support
- Hardening non-Windows devices (e.g. BIOS, USB ports, switches)

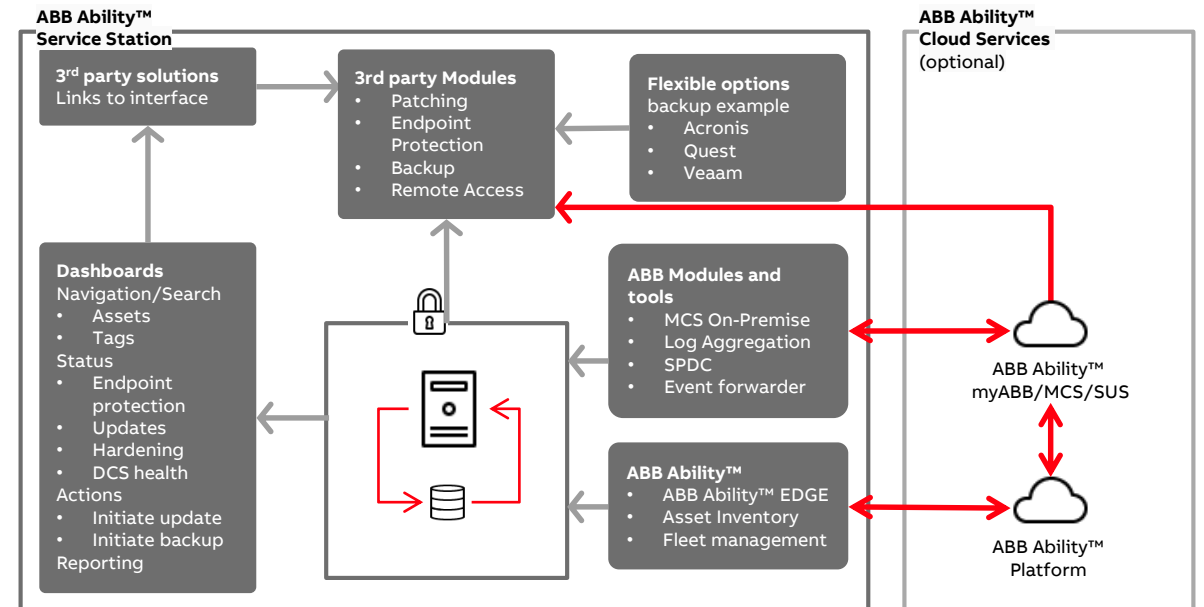


Service Station*

Combining multiple solutions into one station

Key functions

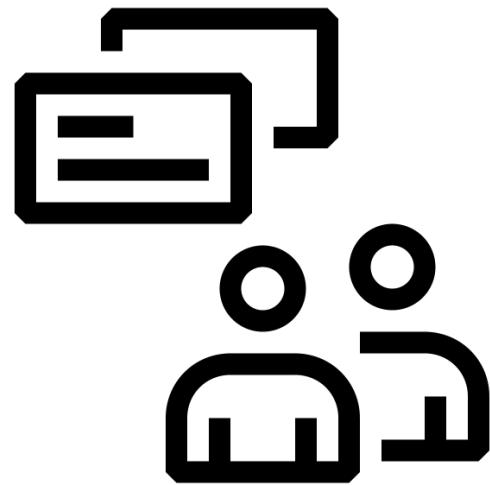
- Patching
 - Online / Offline
- Anti malware
 - Anti Virus
 - Whitelisting
- Local dashboard
- Backup & Recovery solution
- Remote Access
- Log aggregation
- SPDC
- Asset Inventory



—

Q & A

Q & A



ABB