Cyber Security

Sales presentation
PAB/SGT-500/19-002, PAB/SGT-600/19-002,
PAB/SGT-700/19-002, PAB/SGT-750/19-001,
PAB/SGT-800/19-001

Headline Arial Bold 24 pt
Table of contents, option 1

Why – Cyber Security

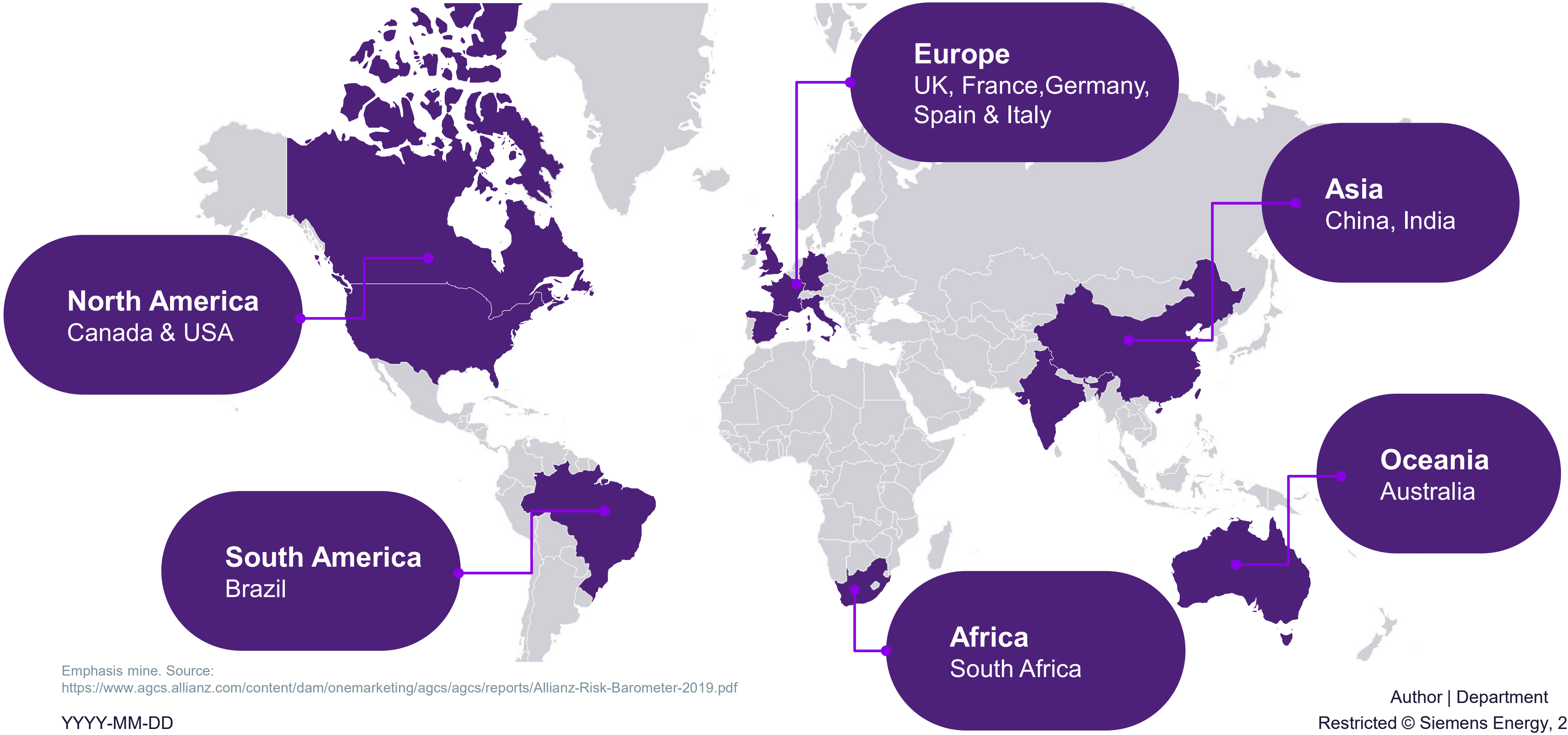
To keep the system safe…

…with our in-depth market knowledge and comprehensive set of solutions along the full value chain. We deliver clarity and focus to help you as our customer to make better decisions.

Our mission is in strengthening your Cyber Defenses, we navigate you through the complex relationship between your information technology (IT) and operational technology (OT) environments.

With increasing growth in technological and digital innovations come great challenges on information security and data protection.

Top Cyber Incidents/Business interruption around the world



North America
Canada & USA

South America
Brazil

Europe
UK, France,Germany,
Spain & Italy

Africa
South Africa

Asia
China, India

Oceania
Australia

Emphasis mine. Source:
https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf

Why – Cyber Security

IT

Information system used for business communication

- Traditional focus for cyber investment
- Systems replaces every 3 – 5 years
- Known assets/well understood
- Attackers steal data
- Tolerance for failover or delay

OT

Operational systems used at the plant level to produce and transport energy

Automation hardware

Power Meters

DCS / HMI screens

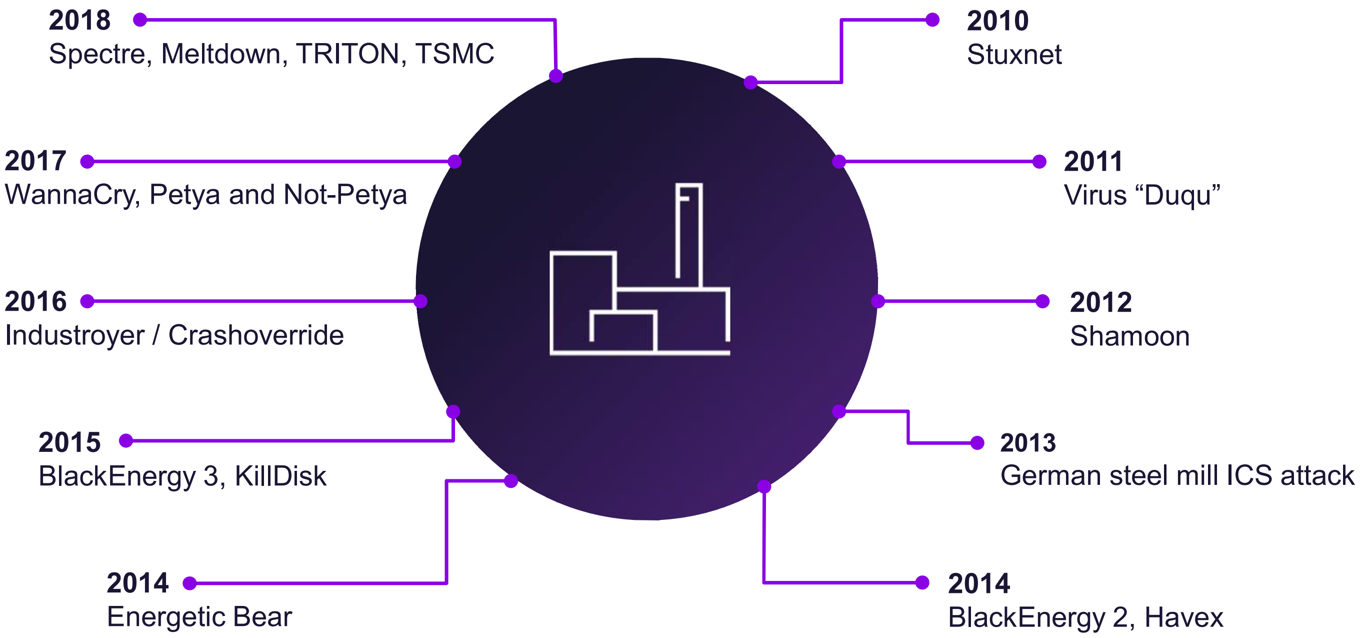
Field Devices

- Often ignored – lower cyber maturity
- Legacy systems last 20-30 Years
- Many unknown assets/not well understood
- Attackers disrupt/destroy/delay power supply
- Uptime is critical

Area of Siemens Energy Deep Expertise

Why – Cyber Security

Cyber Security attacks on industrial systems (2010-2018, selection)



2010
Stuxnet

2011
Virus “Duqu”

2012
Shamoon

2013
German steel mill ICS attack

2014
BlackEnergy 2, Havex

2014
Energetic Bear

2015
BlackEnergy 3, KillDisk

2016
Industroyer / Crashoverride

2017
WannaCry, Petya and Not-Petya

2018
Spectre, Meltdown, TRITON, TSMC

Source: SANS, Hackmageddon, Reuters, NY Times, sans.org, Trend Micro, FireEye

Disrupting, delaying, or destroying the supply of energy is a big incentive

There are a variety of attackers

- Examples: Nation States, Organized Crime, Terrorist, Hacktivists

Attacks have grown in frequency and Intensity

- Examples: Ransomware, Insider Threat, Phishing Attacks, Malware, zero day

Why – Cyber Security,
Because Cyber Attacks can have costly impacts on operations

National Cyber Security Centre
a part of GCHQ

£17 M

May 2018 saw the introduction of the Networks and Information Systems (NIS) Directive. If Organizations do not comply they can face a fine for every cyber incident.

$1-2 M/day

Economic impact of buying energy to replace production Capabilities

Richmond Times Dispatch
http://www.richmond.com/business/nuclear-plant-outagescostly/article_da2b7cbe-b2ef-567ca28d-694459d0b726.html

$38-88M

Average annual spend on unplanned downtime

GE – The Impact of Digital on Unplanned Downtime. October 2016.
https://www.geoilandgas.com/sites/geog.dev.local/files/ge_offshore_study_paper.pdf

225,000

Customers without power due to Black Energy attack, 2015

E-ISAC Analysis:
https://ics.sans.org/media/EISAC_SANS_Ukraine_DUC_5.pdf

$300 M

Cost of NotPetya ransomware ICS attack to single industrial company in 2017

CNBC
https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattackcould-cost-300-million.html

What – Cyber Security Solutions

Your IACS (Industrial Automation and Control Systems)

Equipment is subject to Cyber Security risks which can be addressed with the latest solutions. Potential hazards, security risks and defense measures are constantly changing, so it is important to always keep an overview of the current state to manage the potential risk of an unwanted operational impact.

Our solution is to implement the Cyber Security Essential package consisting of six elements for minimizing Cyber Security risks over time.

A risk assessment should be executed in close collaboration With you as a customer for optimal results based on IEC62443 and NERC

What – Cyber Security Solutions, focus on developing three key areas

Assess and Plan

- What do I need to protect?
- What are my threats?
- Where are my vulnerabilities and weaknesses?
- How do I create a cyber roadmap?

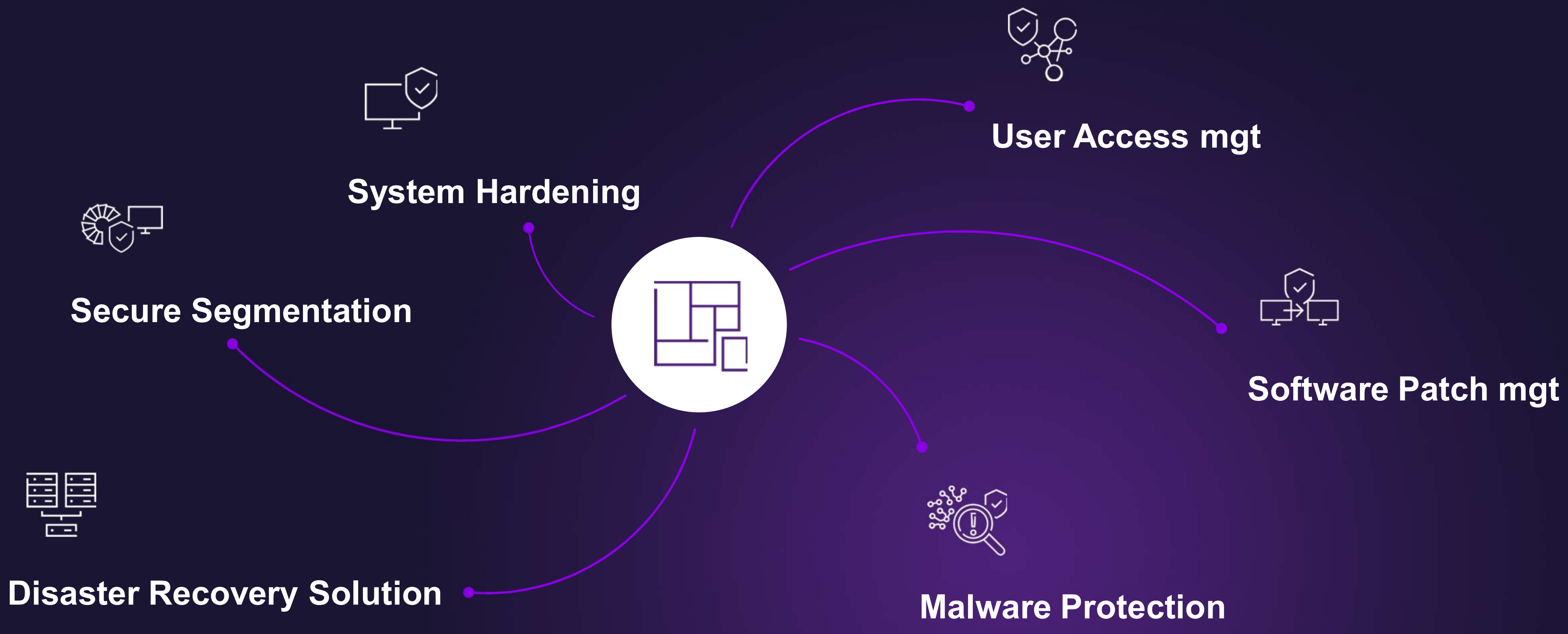
Protect

- What protection do I put in place (at every level)?
- What cyber capabilities do I need to have?
- How do I test my cyber protections?

Detect and Respond

- How do I know I have been breached?
- How do I know when new vulnerabilities are announced?
- How do I best respond to an attack?
- How do I make sure it doesn’t happen again?

How – To apply Cyber Security with our Essential package



User Access mgt

System Hardening

Secure Segmentation

Software Patch mgt

Malware Protection

Disaster Recovery Solution

System Hardening is the process of limiting potential weaknesses that make systems vulnerable to Cyber Attacks

System Hardening

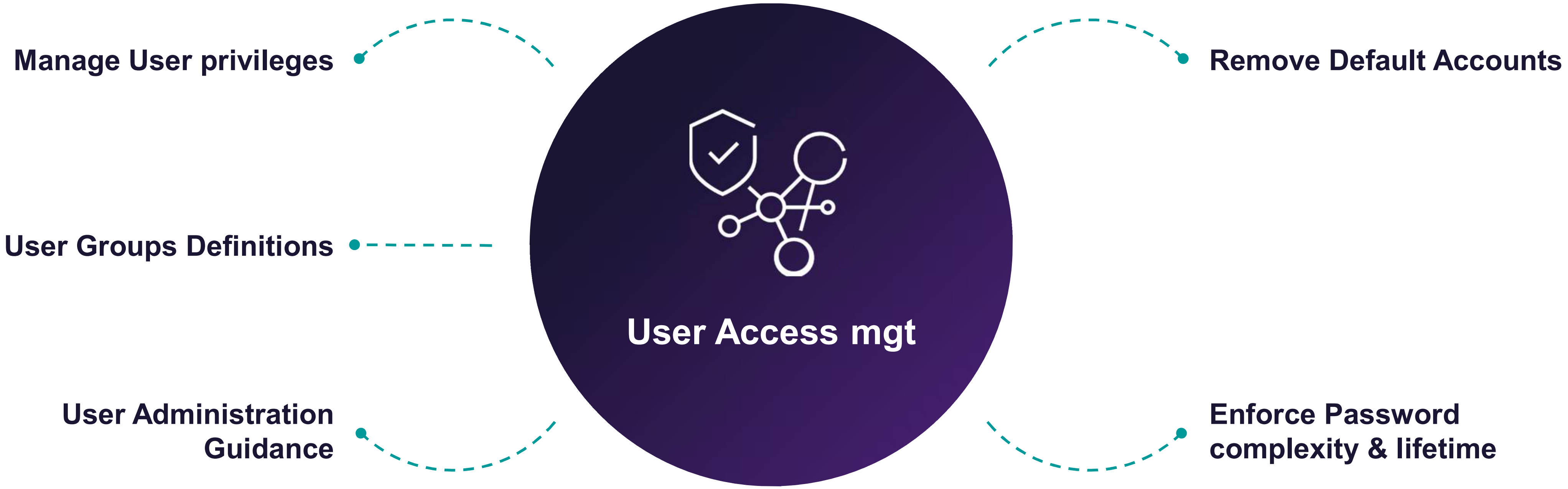
Remove / Disable
Unneeded Services

Set BIOS Password &
Disable CD/DVD/USB
as Bootable Devices

Remove Unneeded
Software / Programs

Disable / Close
Unused Ports
(Network & USB)

User access management describes the basic definitions, principles, processes & guidance to minimize Cyber Attacks



Manage User privileges

User Groups Definitions

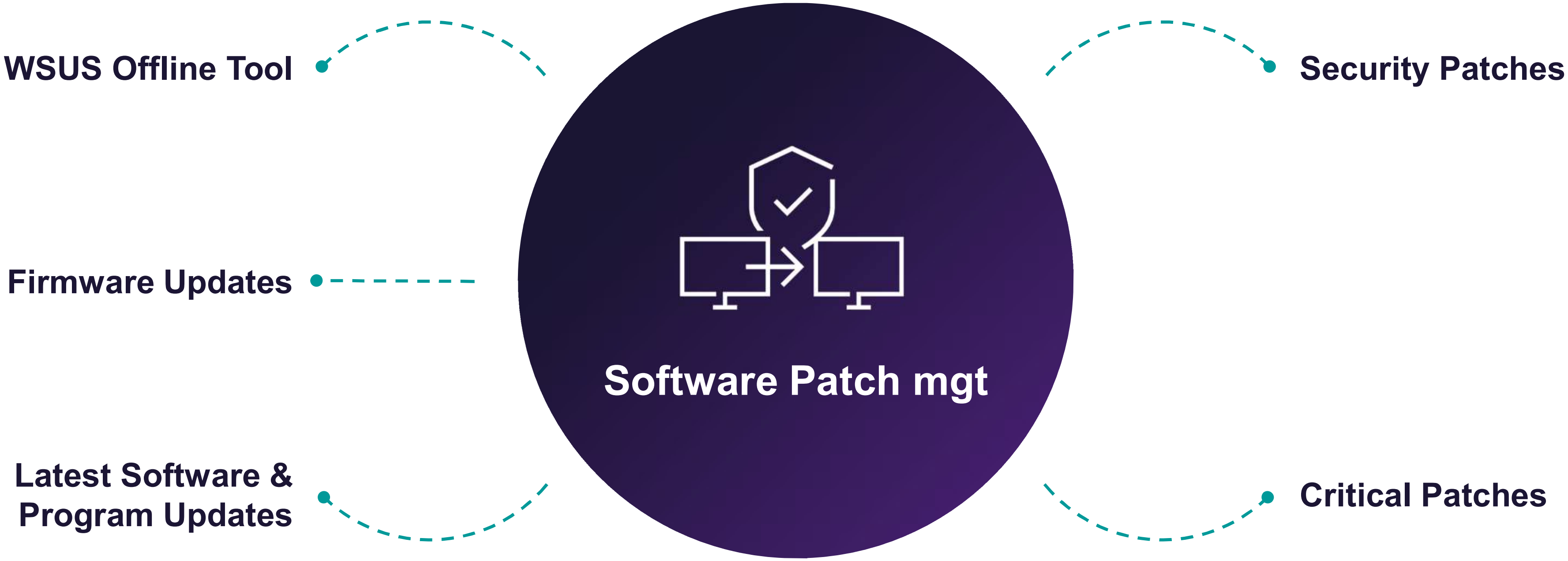
User Administration Guidance

User Access mgt

Remove Default Accounts

Enforce Password complexity & lifetime

Software Patch management aligns with Siemens Energy to update the IACS with Security & Critical Patches to minimize Cyber Attacks



Malware protection is a type of program that actively prevent malicious software from infecting the IACS to Cyber Attacks

End Point Protection - Malicious Code

Malware Protection

Antivirus Definitions

Disaster Recovery Solution is to have tried-and-tested backup, restore software processes in case of any upcoming disaster

Disaster Recovery Solution

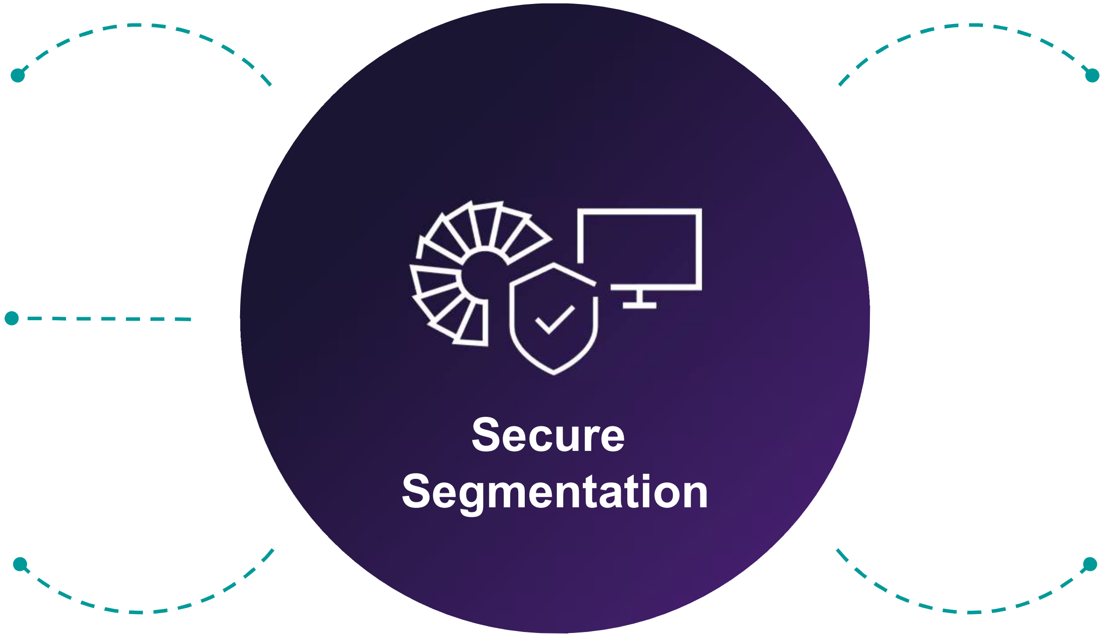
Create Backups of IACS

Test & Verification of Backups

Backup Policy

Security Storage of the Backups

Secure segmentation is to limit potential weaknesses in layers of network communication to Cyber Attacks



DMZ

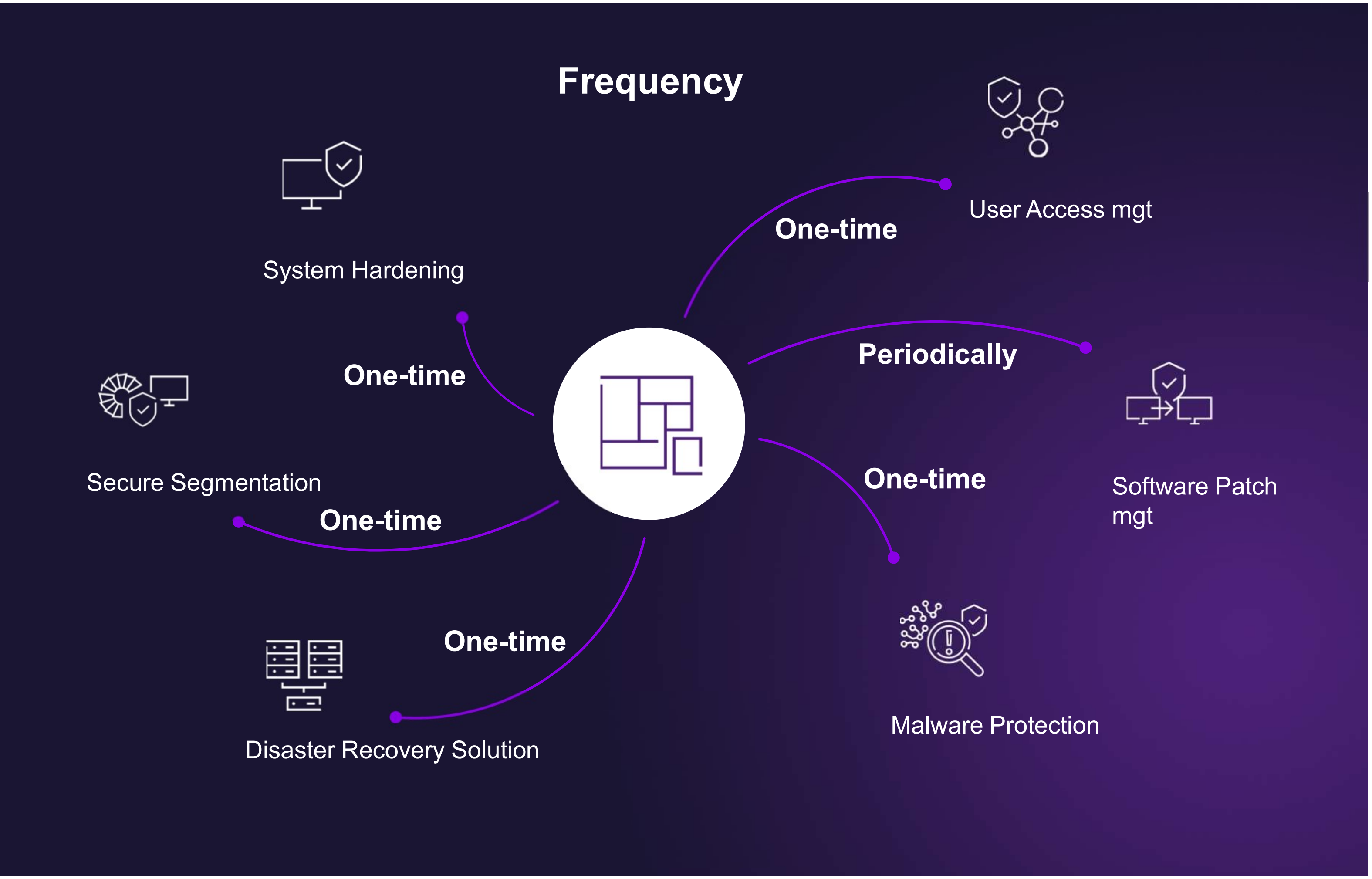
Firewalls, Data Diode

System / Function Segmentation

Machine Segmentation

Segmentation of IT & OT

How – To apply Cyber Security with our Essential package, with pre-defined package for Defense in Depth



Option:
Assessment
IEC62443/NERC -
One-time

Your Benefit

With Siemens Energy OEM knowledge, products, and comprehensive Cyber Security technology, experience, and access to diverse industry expertise your benefits are:

- An essential package to raise your IACS Cyber Security standard.
- Minimize the risk of unwanted business interruptions due to Cyber Security threats.
- Minimize security gaps.
- Increased awareness and capabilities to maintain Cyber Security level when cyber threats are changing
- Support to be compliant with legislation/standards such as IEC62443 and NERC.

Questions

Disclaimer

Subject to change and error. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Siemens Energy is a trademark licensed by Siemens AG.