



Smart Grid Cybersecurity 2020

IT OT Convergence Adressed with
A Virtual IT OT Security Organization and
An Integrated Security Event Monitoring

VIRTUAL CONFERENCE, 7 OCTOBER 2020



Fra, 30. November 2016

About BKW.

The **BKW** Group is a Berne based international energy and infrastructure services company employing about 10,000 people and generating a revenue of about CHF 3 billion.

Its company network and extensive expertise allow it to offer its customers a full range of overall solutions. The Group plans, builds and operates infrastructure to produce **Energy** and to distribute it through its **Power Grid** to businesses, households and the public sector, and it offers digital business models for renewable energies.

In addition, the BKW Group portfolio comprises everything from **Engineering** consultancy and planning for energy, infrastructure and environmental projects, through integrated offers in the field of **Building Solutions**, to the construction and maintenance of **Infra Services** for energy, telecommunications, transport and water networks.



BKW's Approach to Cyber Security.



In order to protect against cyber attacks, **BKW** follows the generally recognised risk-based approach of the common international frameworks (i.e. the **NIST Cybersecurity Framework**).

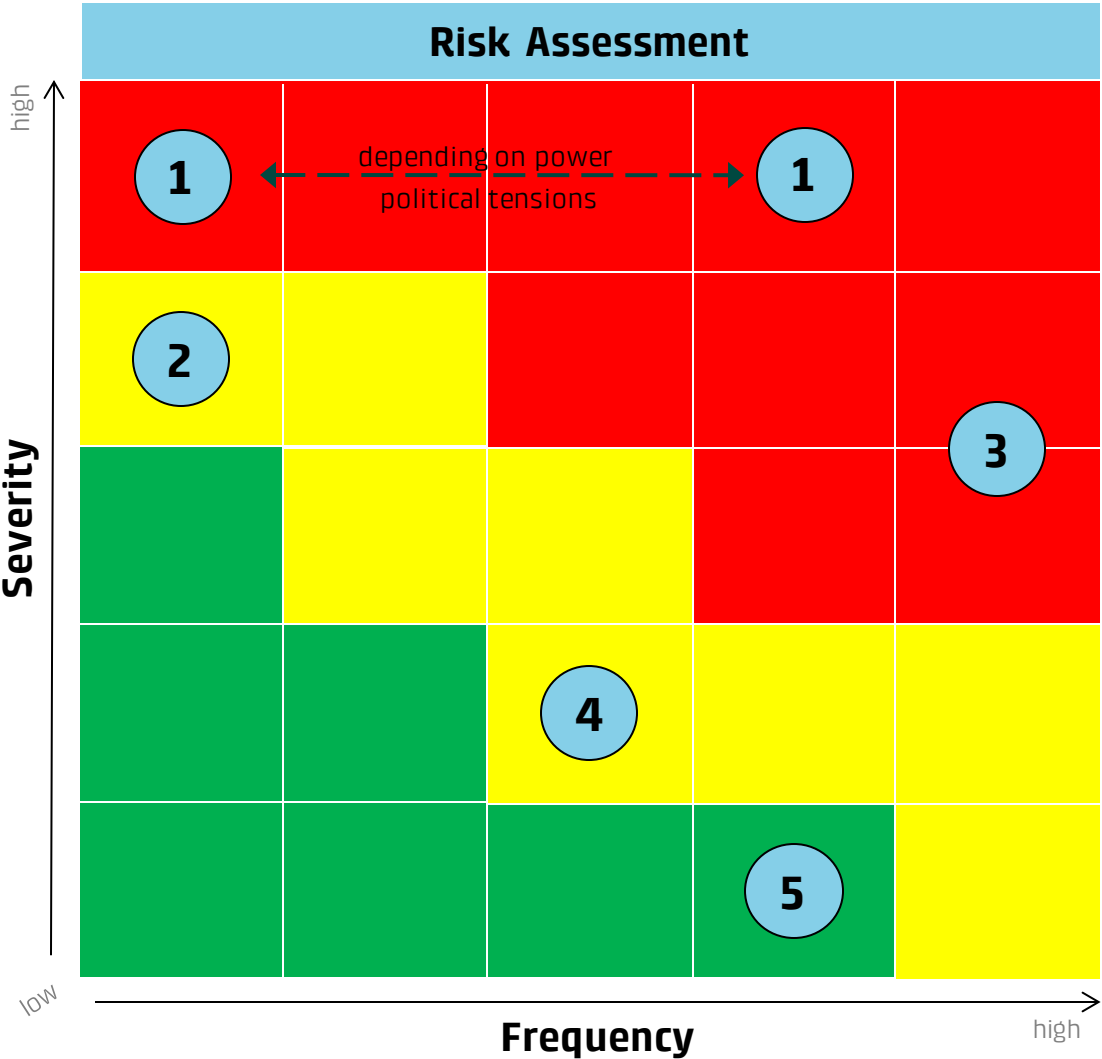
BKW integrates the protection and security of data and information into its organisation, processes, projects, systems and buildings.

To this end, it operates an Information Security Management System (**ISMS**) pursuant to **ISO/IEC 27000** and **IEC 62443**. The Corporate Policy '**Handling Data and Information Securely**' provides its base.

With its **ISMS**, BKW ensures to keep information security on the required level, while addressing deficiencies continuously any assessing it periodically.

The **CISO** proposes the Policy to the ExCom, defines the Cyber Security Strategy, runs the Cyber Security Program, releases the Guidelines and steers the Cyber Security Operations with the help of the IT/OT Security Officers.

Understand the Threat.



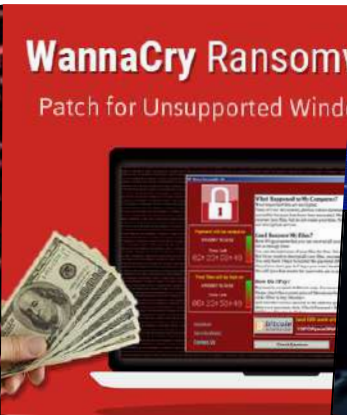
Actors	Motivation	Approach
1 Intelligence Agencies	<ul style="list-style-type: none"> Gather Information Steal intellectual property Espionage Sabotage 	<ul style="list-style-type: none"> Procure Know-how, form agents Very inconspicuous, long term approach Lots of resources allocated Very targeted, persistent approach Compromised products/supply chain
2 Terrorists	<ul style="list-style-type: none"> Fear & Panic Damage of all sorts Impose Ideology Enforce Mob Justice 	<ul style="list-style-type: none"> Buy Know-how on the black market Focus on critical infrastructures Very well organized
3 Organized Crime	<ul style="list-style-type: none"> Money Information trading (Reputational) Damage 	<ul style="list-style-type: none"> Professional offerings Spontaneously arranged campaigns Deceit, bribery and extortion
4 Activists	<ul style="list-style-type: none"> Gain attention (Reputational) Damage 	<ul style="list-style-type: none"> Highly motivated specialists Politics & Media Partially organised
5 Vandals, Hobby Hackers	<ul style="list-style-type: none"> Win fame & respect Satisfy curiosity 	<ul style="list-style-type: none"> Use of freely-available tools (darknet) Physical or logical attacks

Follow the Attack Evolution.

NotPetya



WannaCry



Emotet, Trickbot, RYUK



Side Channel Exploit



NEWS
New 'CacheOut' attack targets Intel processors, with a fix arriving soon
Intel rates CacheOut as "medium" severity RDP



BlackEnergy, KillDisk

KIM ZETTER SECURITY 03.03.16 7:00 AM
INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

CrashOverride/Industroyer

INFOSECURITY MAGAZINE HOME » NEWS » UKRAINE POWER OUTAGE CONFIRMED AS CYBER ATTACK
12 Jan 2017 News

Ukraine Power Outage Confirmed as Cyber Attack

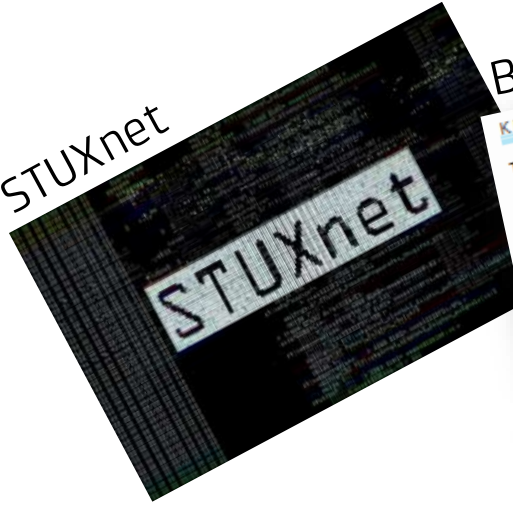
Triton



Triton: hackers take out safety systems in 'watershed' attack on energy plant
Sophisticated malware halts operations at power station in unprecedented attack











STUXnet



Understand the Cyber Kill Chain in IT and OT.



IT = Information Technology
OT = Operational Technology

<p>S o c i a l M e d i a</p> <p>IT</p> <p>OT</p>	       	<p>Start</p> <p>Reconnaissance</p> <p>Weaponization</p> <p>Delivery</p> <p>Exploitation</p> <p>Installation</p> <p>Command & Control</p> <p>Actions on Objectives</p>	<p>BKW may be identified as a target for its funds and critical infrastructure.</p> <p>Intruder researches target and attempts to identify vulnerabilities in it.</p> <p>Intruder creates remote access malware weapon tailored to vulnerabilities.</p> <p>Initial Access: (Spear) Phishing, USB Sticks, CEO-Fraud, Social Engineering, Malware Downloads, Fake Password Change, Watering Hole</p> <p>Malware code triggers, escalates privileges and takes action on target to exploit vulnerability.</p> <p>Malware installs access point (e.g. "backdoor") usable by intruder's command & control networks.</p> <p>Malware enables intruder to have persistent access to target network.</p> <p>Intruder takes action, such as data exfiltration, destruction, or encryption.</p>
--	---	---	--

Attacks Usually Start in IT ...



Delivery



Exploitation



Installation



Command & Control



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise		Scheduled Task		Binary Padding		Network Sniffing		Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Launchctl Local Job Scheduling		Access Token Manipulation Bypass User Account Control		Account Manipulation Bash History	Account Discovery Application Window Discovery	AppleScript Application Deployment Software	Automated Collection Clipboard Data	Communication Through Removable Media	Data Compressed Data Encrypted	Data Encrypted for Impact Defacement
External Remote Services	LSASS Driver		Extra Window Memory Injection		Brute Force			Data from Information Repositories	Connection Proxy	Data Transfer Size Limits	Disk Content Wipe
Hardware Additions	Trap		Process Injection		Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Data from Local System	Custom Command and Control Protocol	Exfiltration Over Other Network Medium	Disk Structure Wipe
Replication Through Removable Media	AppleScript CMSTP		DLL Search Order Hijacking Image File Execution Options Injection		Credentials in Files Credentials in Registry	Domain Trust Discovery	Exploitation of Remote Services Logon Scripts	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Endpoint Denial of Service Firmware Corruption
Spearphishing Attachment	Command-Line Interface		Plist Modification Valid Accounts		Exploitation for Credential Access	File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Custom Cryptographic Protocol	Exfiltration Over Command and Control Channel	Inhibit System Recovery
Spearphishing Link	Compiled HTML File				Forced Authentication	Network Service Scanning	Pass the Hash	Data from Removable Media	Data Encoding Data Obfuscation	Exfiltration Over Alternative Protocol	Network Denial of Service Resource Hijacking
Spearphishing v. Service	Control Panel Items	Accessibility Features		BITS Jobs	Hooking	Network Share Discovery	Pass the Ticket	Data Staged	Data Obfuscation	Exfiltration Over Alternative Protocol	Resource Hijacking
Supply Chain Compromise	Dynamic Data Exchange	AppCert DLLs		Clear Command History	Input Capture	Password Policy Discovery	Remote Desktop Protocol	Mail Collection	Domain Fronting	Exfiltration Over Physical Medium	Runtime Data Manipulation
Trusted Relationship	Execution through API	Appinit DLLs		CMSTP	Input Prompt	Peripheral Device Discovery	Remote File Copy	Input Capture	Domain Generation Algorithms	Exfiltration Over Physical Medium	Service Stop
Valid Accounts	Execution through Module Load	Application Shimming Dylib Hijacking		Code Signing	Input Prompt	Permission Groups Discovery	Remote Services	Man in the Browser		Scheduled Transfer	Stored Data Manipulation
		File System Permissions Weakness		Compiled HTML File	Kerberoasting	Process Discovery	Replication Through Removable Media	Screen Capture	Failback Channels		Transmitted Data Manipulation
	Exploitation for Client Execution	Hooking		Component Firmware	LLMNR/NBNS Poisoning and Relay	Query Registry	Shared Webroot	Video Capture	Multiband Communication		
	Graphical User Interface	Launch Daemon		Component Object Model Hijacking		Remote System Discovery	SSH Hijacking		Multi-hop Proxy		
	Install/Uninstall	New Service		Control Panel Items	Password Filter DLL	Security Software Discovery	Taint Shared Content		Multi-layer Encryption		
	Mshta	Path Interception		DCShadow	Private Keys	System Information Discovery	Third-party Software		Multi-Stage Channels		
	PowerShell	Port Monitors		Deobfuscate/Decode Files or Information	Security Memory	System Network Configuration Discovery	Windows Admin Shares		Port Knocking		
	Regsvcs/Regasm	Service Registry Permissions Weakness		Disabling Security Tools	Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management		Remote Access Tools		
	Regsvr32	Setup and Setgid		DLL Side-Loading		System Network Configuration Discovery			Remote File Copy		
	Rundll32	Startup Items		Execution Guardrails		System Network Configuration Discovery			Standard Application Layer Protocol		
	Scripting	Web Shell				System Network Configuration Discovery			Standard Cryptographic Protocol		
	Service Execution	bash_profile and .bashrc	Exploitation for Privilege Escalation			System On-Disk Discovery			Standard Non-Application Layer Protocol		
	Signed Binary Proxy Execution	Account Manipulation Authentication Package	SID-History Injection	File Deletion		System Service Discovery			Uncommonly Used Port		
	Signed Script Proxy Execution	BITS Jobs Bootkit	Sudo Sudo Caching	File Permissions Modification		System Time Discovery			Web Service		
	Source	Browser Extensions				Virtualization/Sandbox Evasion					
	Space after Filename	Change Default File Association		File System Logical Offsets							
	Third-party Software			Gatekeeper Bypass							
	Trusted Developer Utilities	Component Firmware		Group Policy Modification							
				Hidden Files and Directories							

Example: Backdoor.Oldrea aka Havex is a Remote Access Trojan (RAT)

Attacks Usually Start in IT ... and Continue in OT



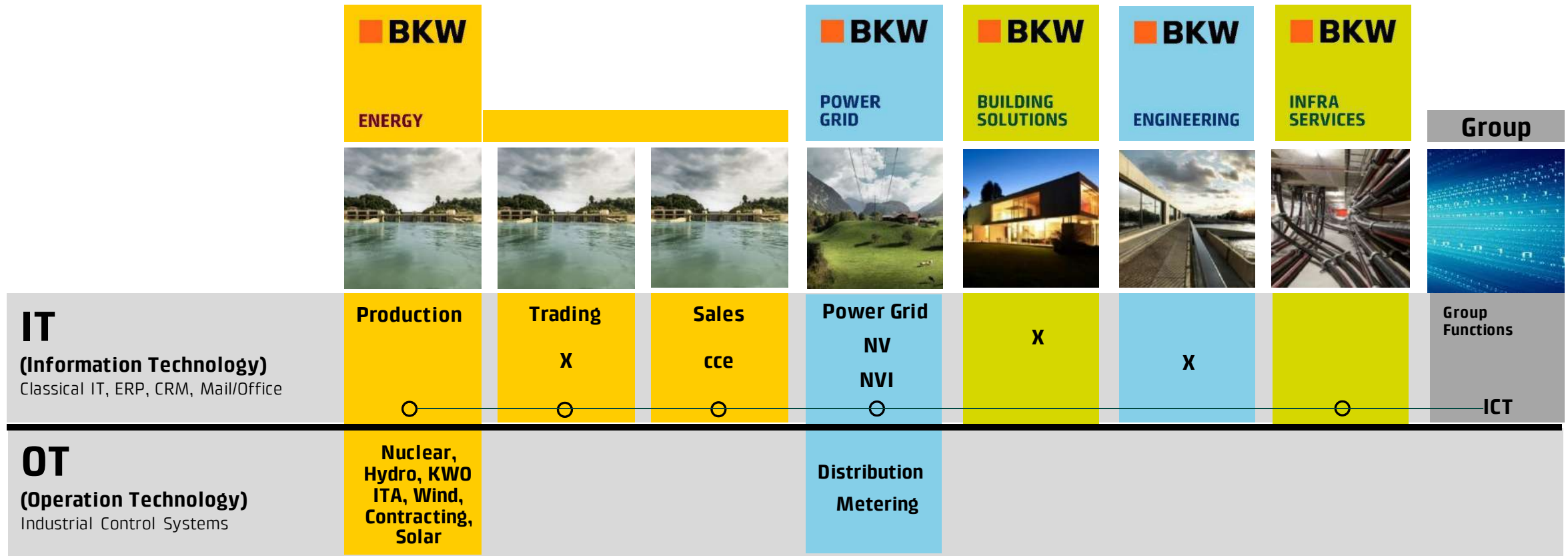
Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Example: Backdoor.Oldrea aka Havex is a Remote Access Trojan (RAT)

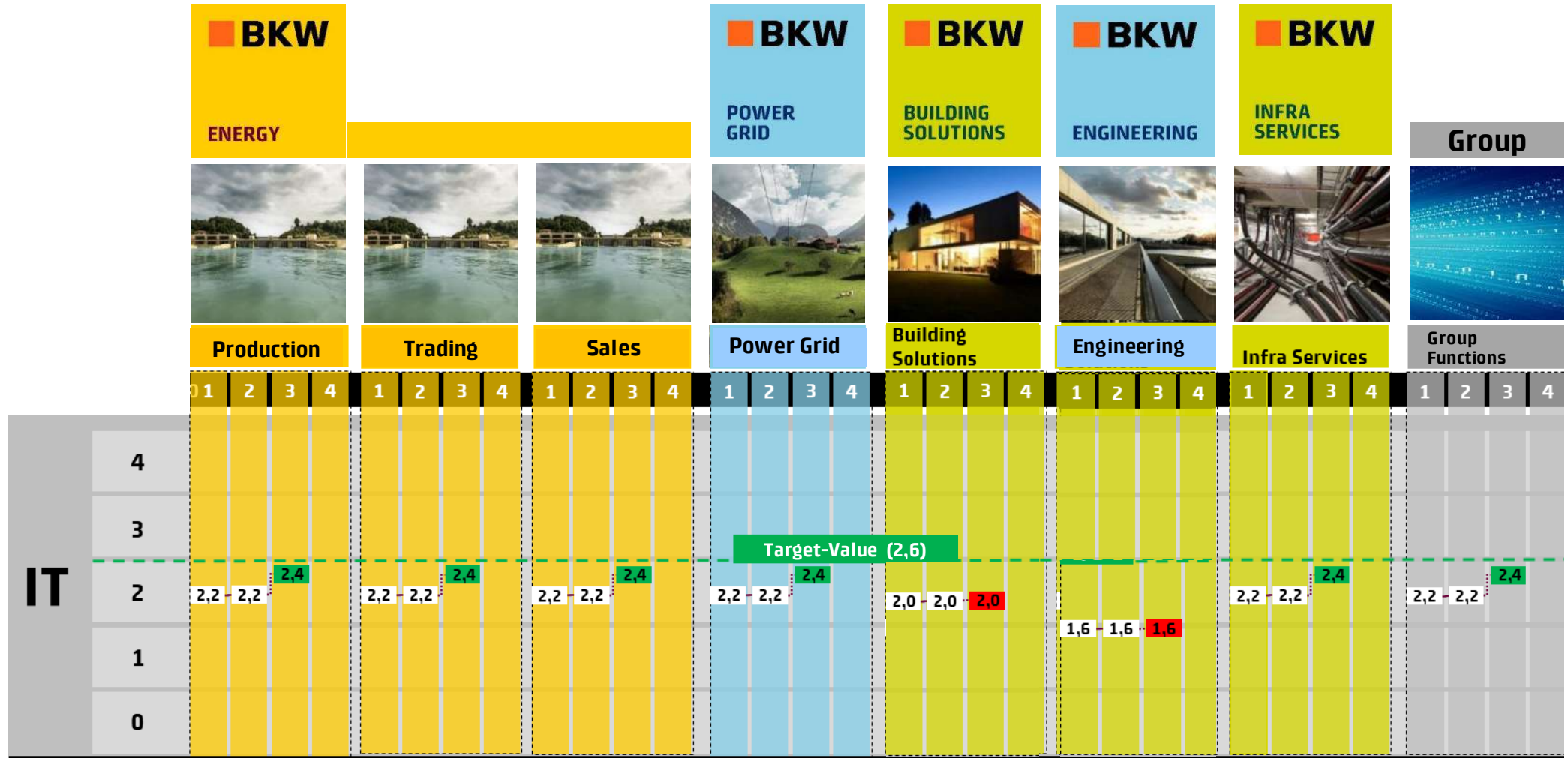
Finding

A successful attack is only a matter of time and resources invested by the adversary

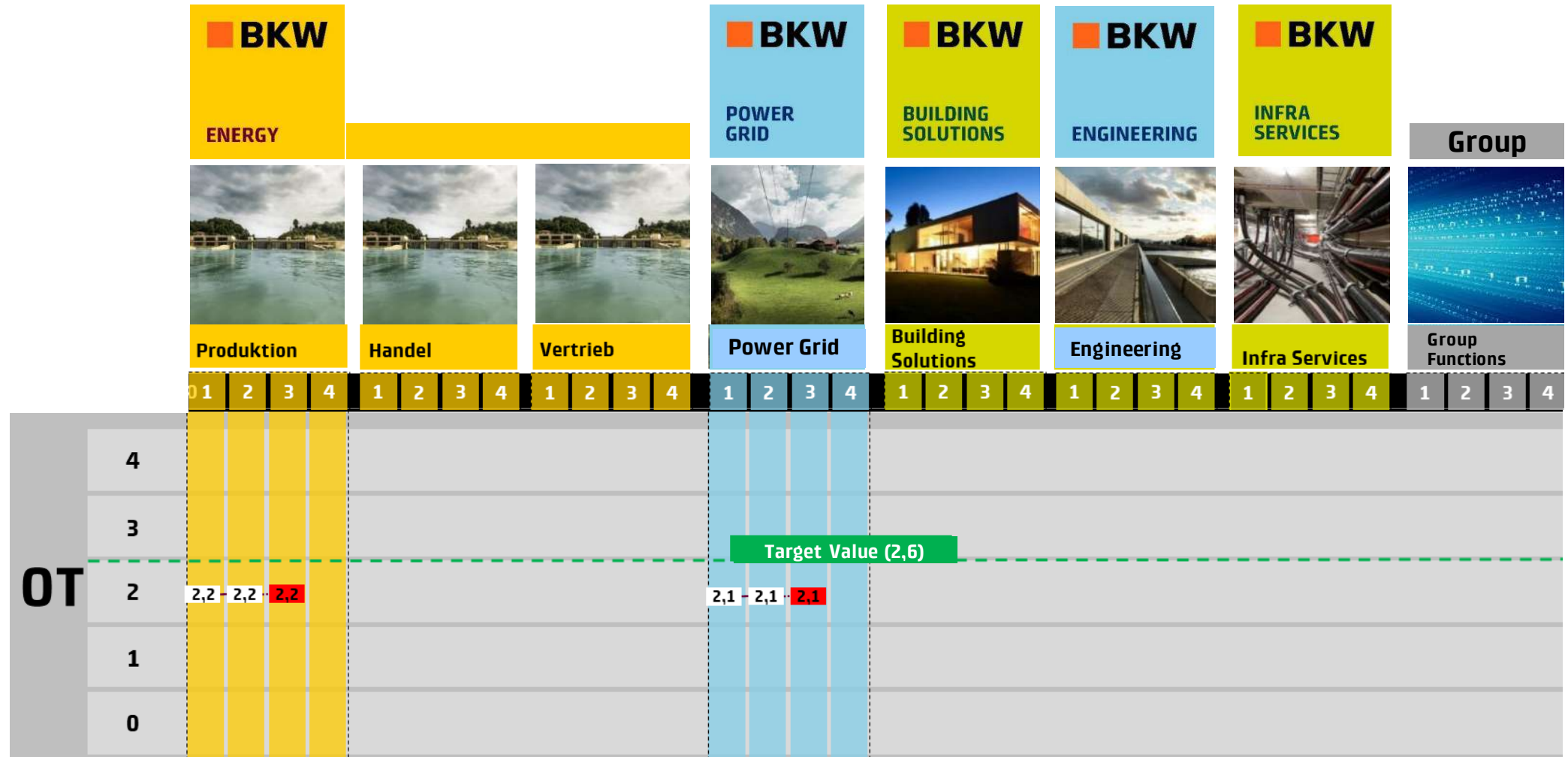
Identify All Your IT and OT Organisations.








Assess their Cybersecurity Maturity Yearly.



Assess their Cybersecurity Maturity Yearly.

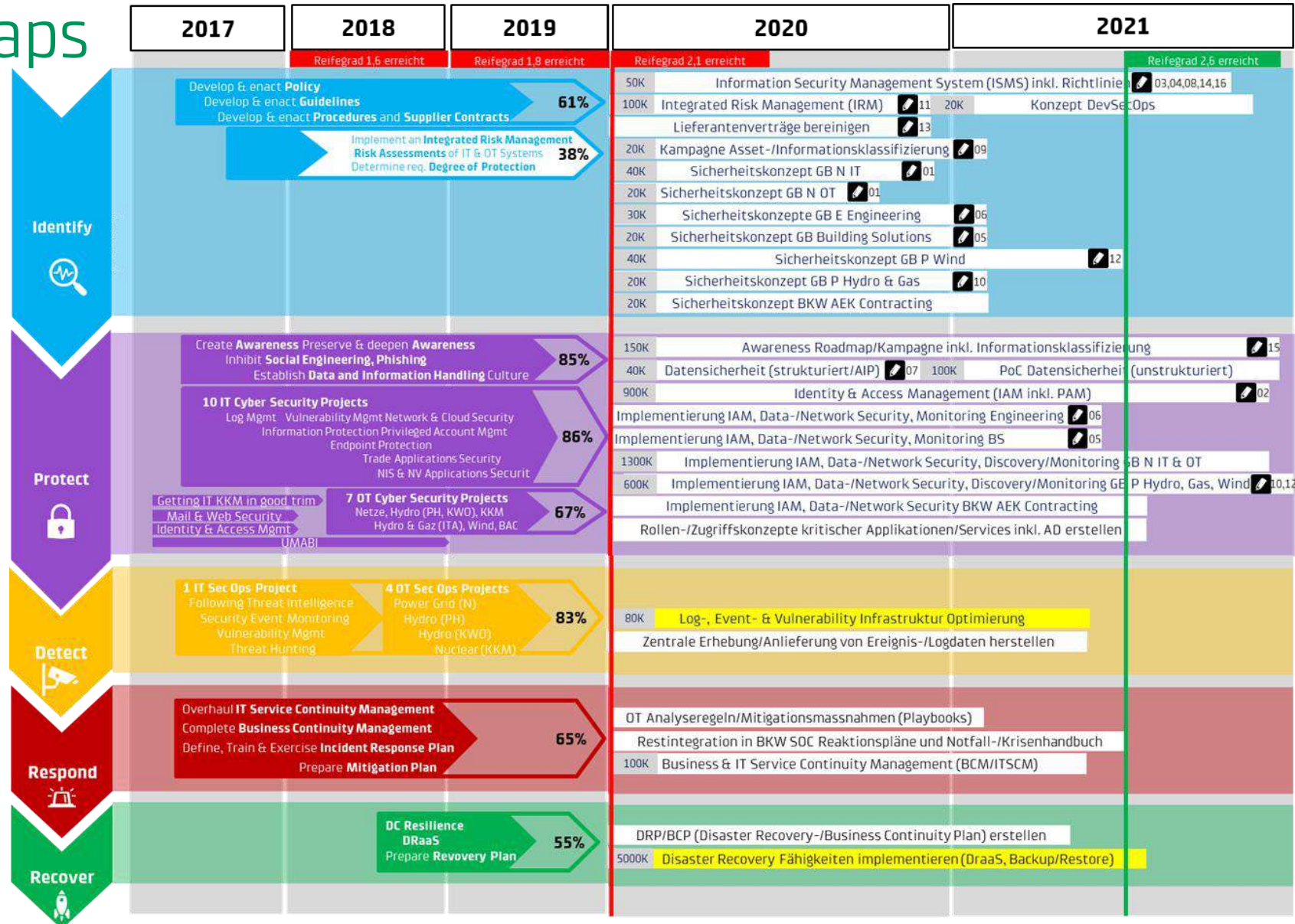


Close the Gaps. Define the Measures to Reach the Objectives

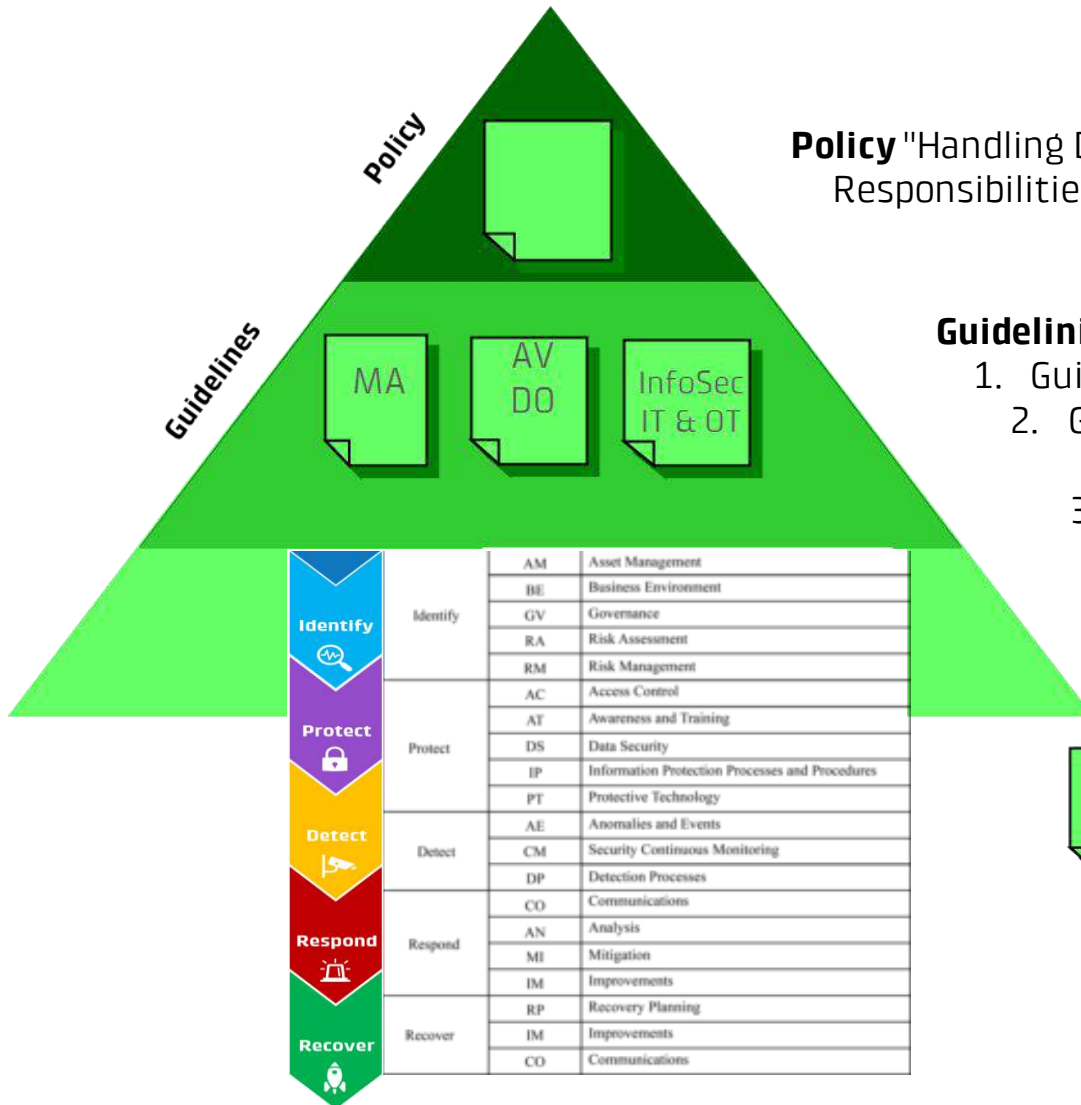
	Actual	Principle Measures to reach Target	Target
 <p>Identify</p>	2,2	<ul style="list-style-type: none"> Fully establish Information Security Management System (ISMS) Run Asset / Information Classification Campaign Create Security Concepts detailing Measures to be implemented 	2,6
 <p>Protect</p>	2,3	<ul style="list-style-type: none"> Create continued Awareness Roadmap / Run Data Culture Campaign Implement Information Security & Data Protection (for structured & unstructured data) Renew Identity & Access Management (incl. Privileged Account/Access Management) Finish Implementation of Protective Measures for IT & OT in Power Grid Finish Implementation of Protective Measures for IT & OT in Production 	2,6
 <p>Detect</p>	2,0	<ul style="list-style-type: none"> Create Security Operation Guideline, Train OSIs/OSSs accordingly Optimize Log-, Event- & Vulnerability Infrastructure Optimize Surveillance (Dashboards, KPIs, Reports) 	2,6
 <p>Respond</p>	2,1	<ul style="list-style-type: none"> Create Reaction Plans (Emergency / Crisis Handbook) Create Specific Analysis Guidance & Prepare Mitigation Measures (Playbooks) Establish Business & IT Service Continuity Management (BCM/ITSCM) 	2,6
 <p>Recover</p>	2,0	<ul style="list-style-type: none"> Create Business Continuity Plans Establish and Improve Recovery Capabilities (DRaaS, Backup/Restore) 	2,6

Complete the Cyber Security Program.

Close the Gaps



Establish the Governance.



Policy "Handling Data and Information Safely"

Responsibilities & Principles for the whole BKW Group

-> aimed at all Employees, specially to BU-Leaders and GMs

Guidelines to address specific Target Audiences

1. Guideline "Information Security for Employees"
2. Guideline "Information Security for Business Functions" (defining e.g. Application Responsibles & Data Owners)
3. Guideline "Information Security for IT and OT"

Standard Operating Procedures

Generic, independent of Products / Releases

Technical Operating Procedures

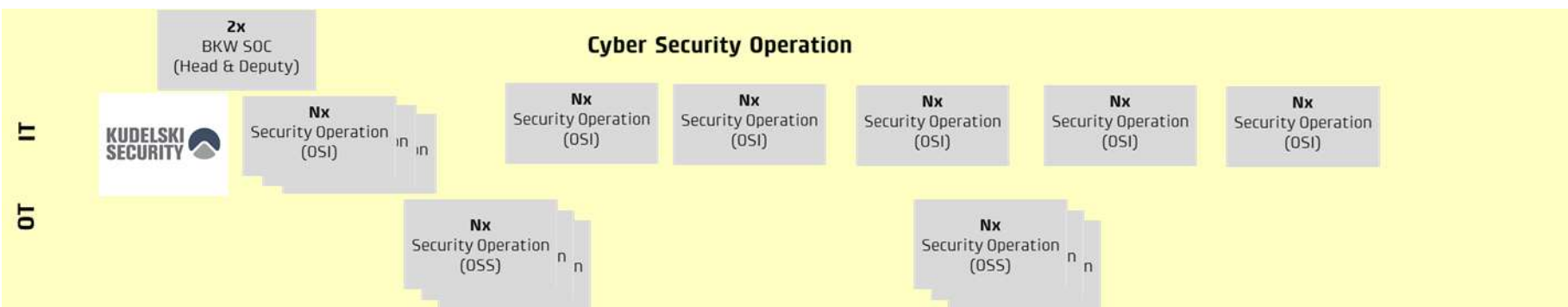
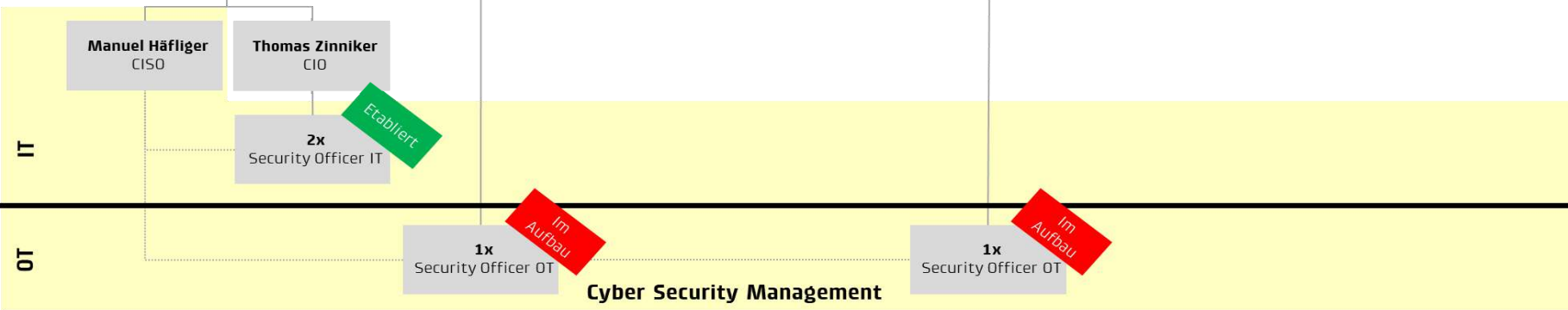
Product- / Release-dependent Instructions

Supplier and Third Party Operators Contracts

"Appendix Information Security"

Identify	AM	Asset Management
	BE	Business Environment
	GV	Governance
	RA	Risk Assessment
	RM	Risk Management
Protect	AC	Access Control
	AT	Awareness and Training
	DS	Data Security
	IP	Information Protection Processes and Procedures
	PT	Protective Technology
Detect	AE	Anomalies and Events
	CM	Security Continuous Monitoring
	DP	Detection Processes
Respond	CO	Communications
	AN	Analysis
	MI	Mitigation
	IM	Improvements
Recover	RP	Recovery Planning
	IM	Improvements
	CO	Communications

Assign the Responsibilities to A Virtual IT OT Security Organization



First Line of Defence

- 1 Line Management down from the ExCom is responsible to have Cyber Security Projects executed and Operations ensured according to the Policy released by the ExCom.
- 2 The Head ICT provides the Resources (Contract, Finance, Personnel) for the operational Lead of the BKW SOC. The Head of the BKW SOC leads the MSSP and the virtual SOC (consisting of the OSIs and OSSs) operationally.
- 3 The Department & Team Leaders in IT and OT and the Application Responsibles (AR) and Data Owners (DO) in the Business Functions ensure the daily SecOps by assigning and enabling **Operational Security Engineers IT (OSI)** and **Operational Security Engineers SCADA (OSS)**.

Second Line of Defence

- 4 The CISO proposes the Policy to the ExCom, defines the Cyber Security Strategy, runs the Cyber Security Program, releases the Guidelines and steers Cyber Security Operations with the IT/OT Security Officers (2nd Line of Defence).
- 5 The IT/OT Security Officers steer the secure Use of the Applications and Infrastructure in IT & OT by applying the Guidelines. They advise Projects & Operations, in particular the OSIs/OSSs and approve the Procedures (2nd Line of Defence).

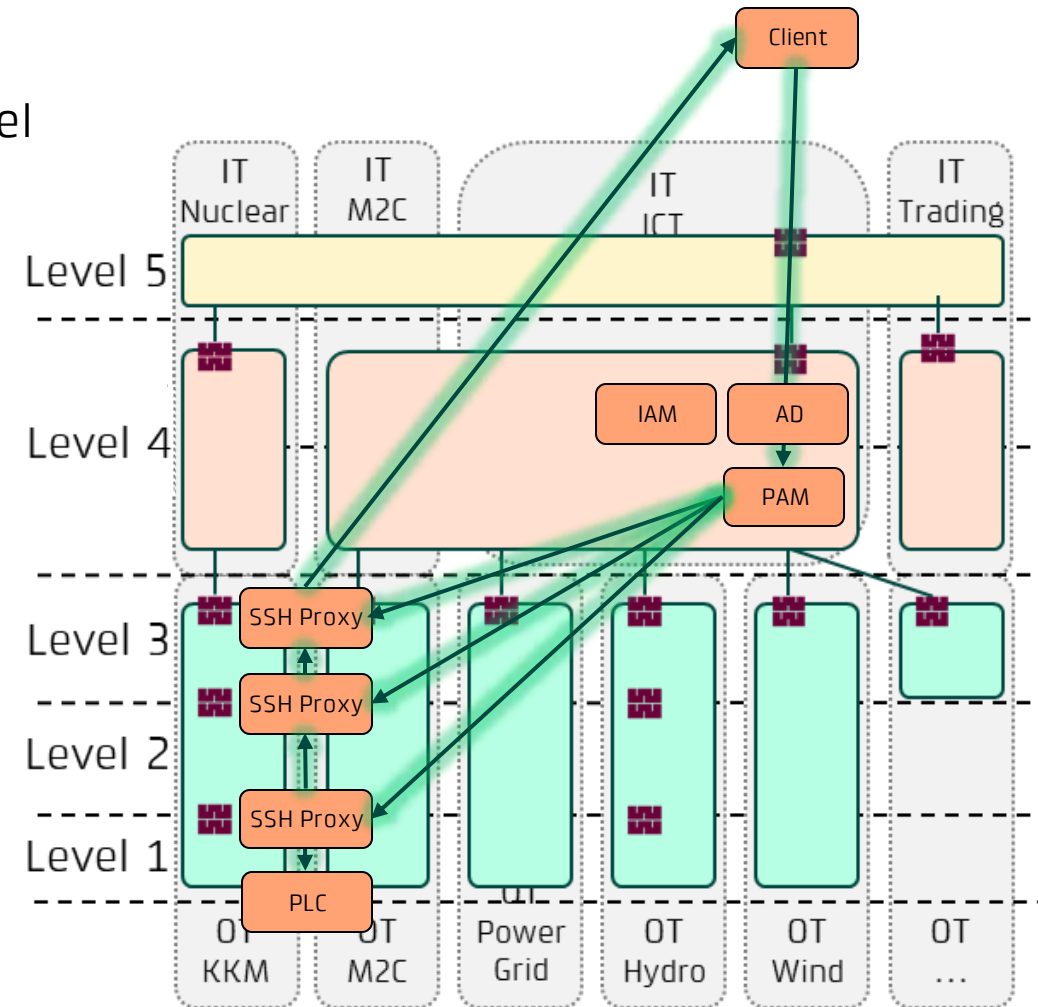
Third Line of Defence

- 6 Internal and External Audit exercise the oversight over the Execution of the Cyber Security Program and Cyber Security Operations (3rd Line of Defence).

Build Defence in Depth, Manage Authentication, Impose Secure Access.

- ① Assign Systems to correct Level
- ② Build Firewalls according to the determined Protection Level
- ③ Grant (Remote) Privileged Access with PAM depending on Time & Location incl. 2FA & Session Recording

Level 5	Enterprise (FW, WAN, BYOD, Partners)
Level 4	Office (Endpoints, Servers, DBs, Apps)
Level 3	Operation & Control (AV, MDM, DNS/DHCP)
Level 2	Area Control (SCADA, HMI)
Level 1	Basic Control (PLC, RTU)



Manage Vulnerabilities and Patches.

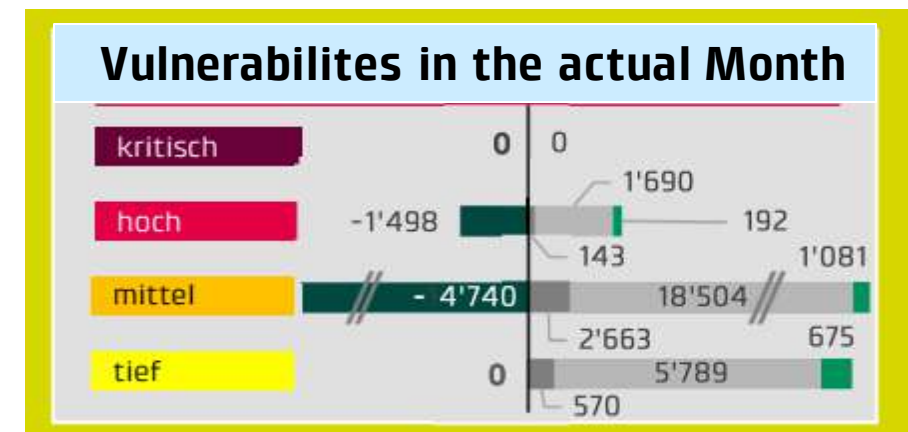
Impose a strict Guideline, have all Teams apply it with self-responsibility

Criticality	CVSS	Time Window	MaxTTPatch
1 - Critical	9.0 - 10.0	7 x 24 h	48 h (Test Community) 96 (Full Deployment)
2 - High	7.0 - 8.9	5 x 10 h	Max. 1 Monat
3 - Medium	4.0 - 6.9	5 x 10 h	Next minor release, max. 1 Quartal
4 - Low	0.1 - 3.9	5 x 10 h	Next major release, max. 1 Jahr

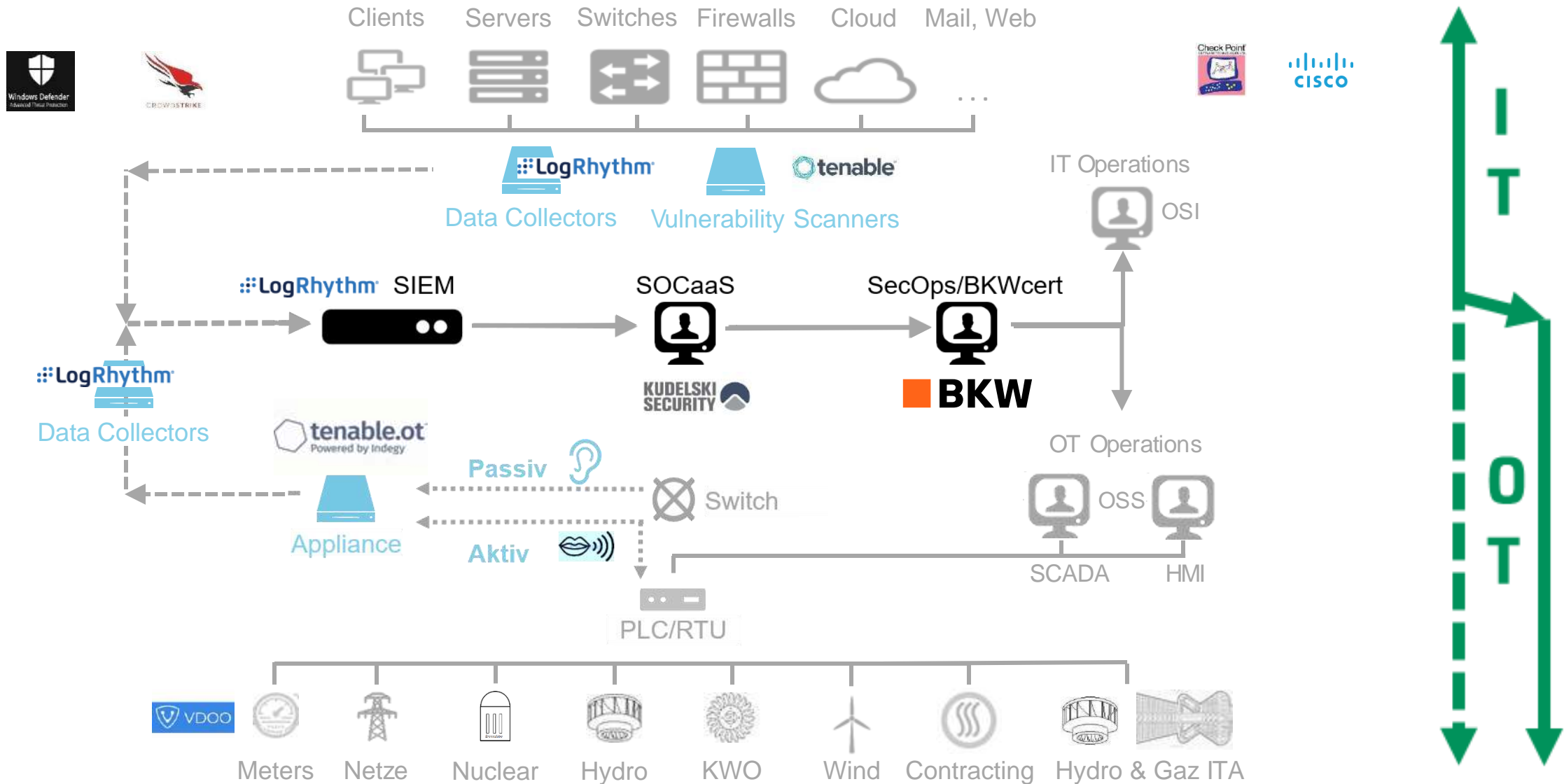
Rule of Thumb:

Deduct 2 Points, if not directly Internet facing

Report to all Management Levels



Ensure An Integrated Security Event Monitoring.



Establish A Regular Reporting.

BKW Cyber Security Bericht Juni 2020

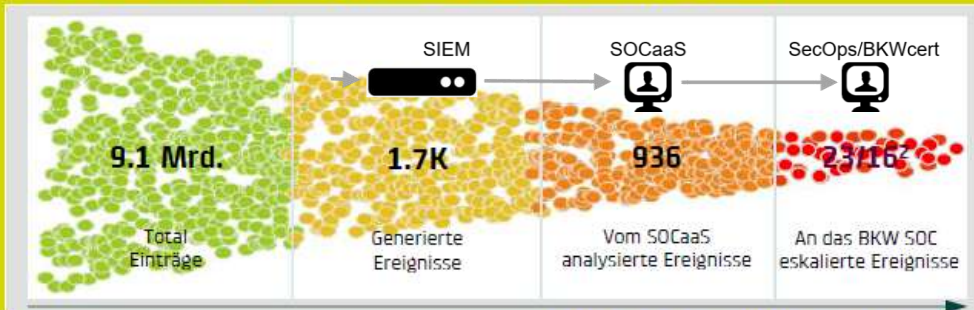


Aktuelle Cyber Security Bedrohungen (Quelle: MELANI et altera)

Publiziert	Name	Vermutl. Ursprung	Kategorie	BKW betroffen	nicht betroffen
9. Juni	Industrial Control Systems von Honda infiziert	Organisierte Kriminalität	Ransomware		X
12. Juni	Weltweit eingesetzte VPN-Produkte angegriffen	Staatliche Akteure	Advanced Persistent Threats	X ¹	

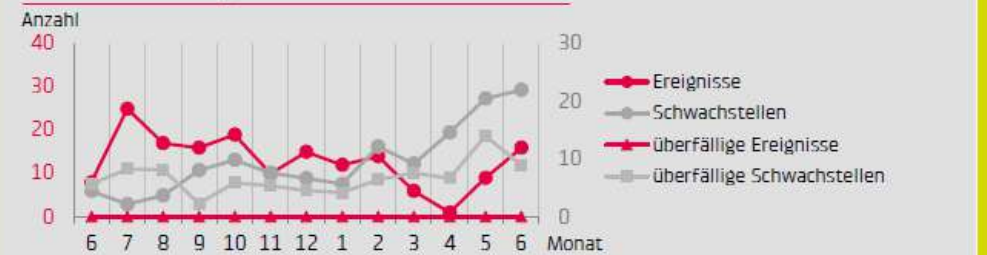
¹ rechtzeitig gepatched

Ereignisübersicht BKW (Quelle: Kudelski Security SOCaas)



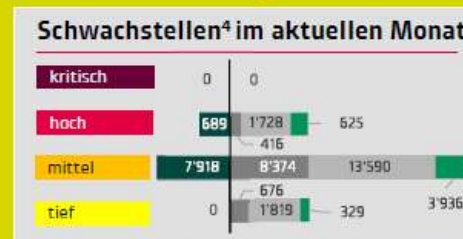
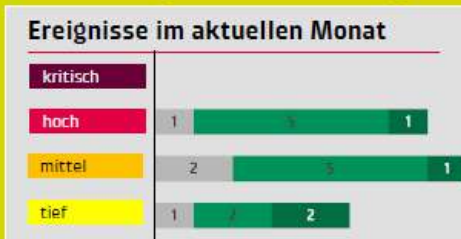
² Total gemeldete / Real zu bearbeitende Ereignisse

Anzahl neue Ereignisse & Schwachstellen³ YTD



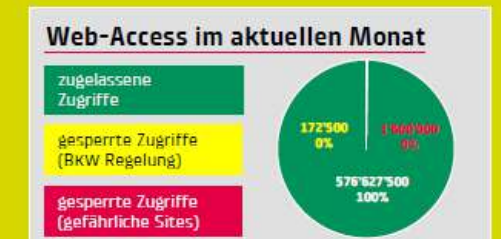
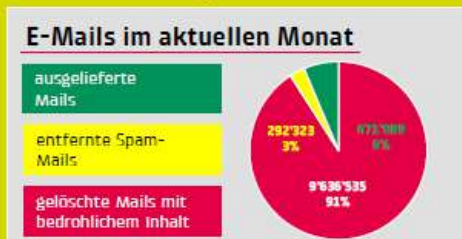
³ Schwachstellen: Schwachstelle * Anzahl Instanzen in 1000

Bearbeitungsfortschritt Ereignisse und Schwachstellen (Quelle: BKW SOC, Kudelski Security)



⁴ Schwachstellen: Schwachstelle * Anzahl Instanzen

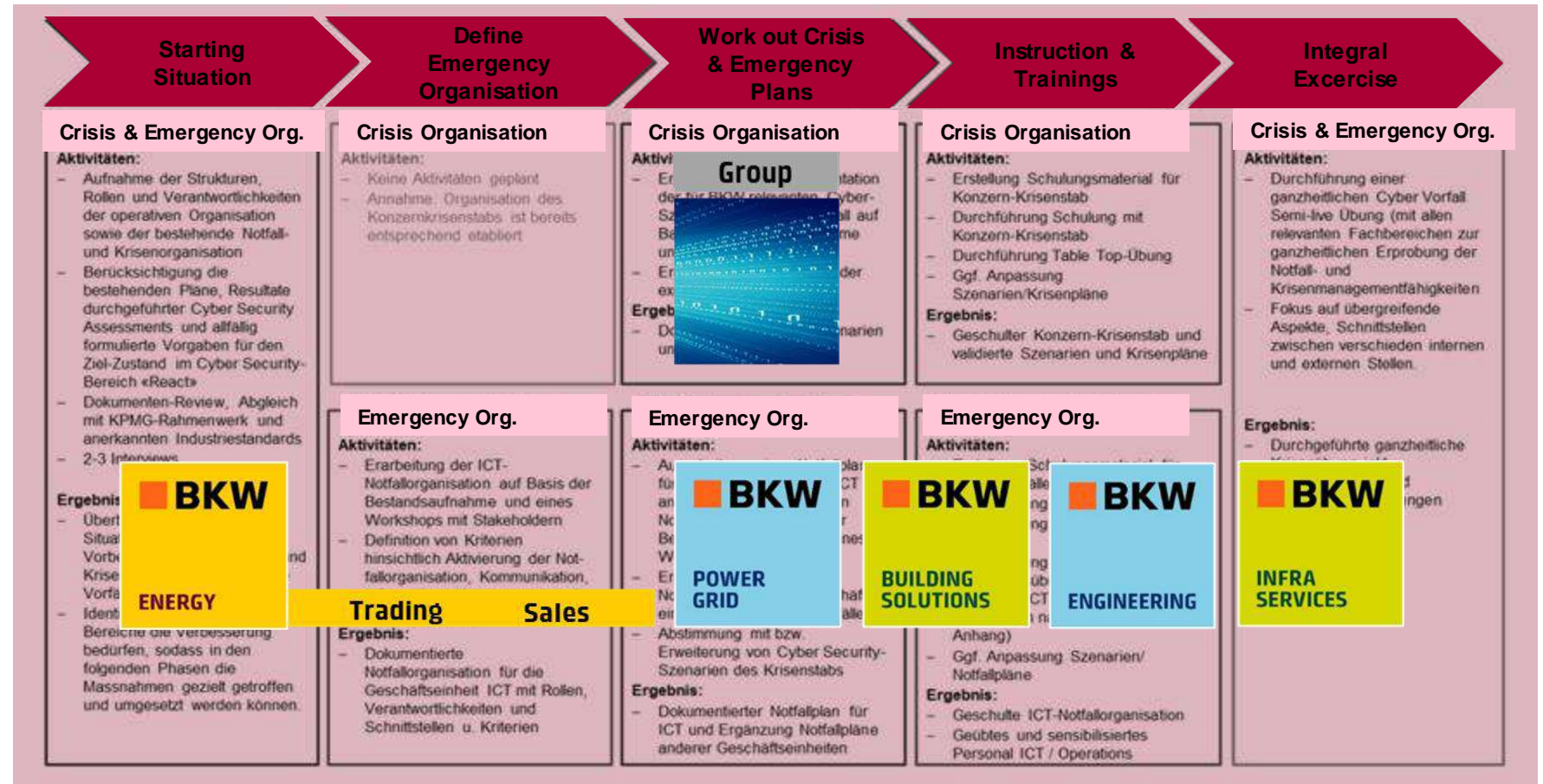
überfällig offen (älter) offen (Juni) erledigt (Juni) erledigt (älter)



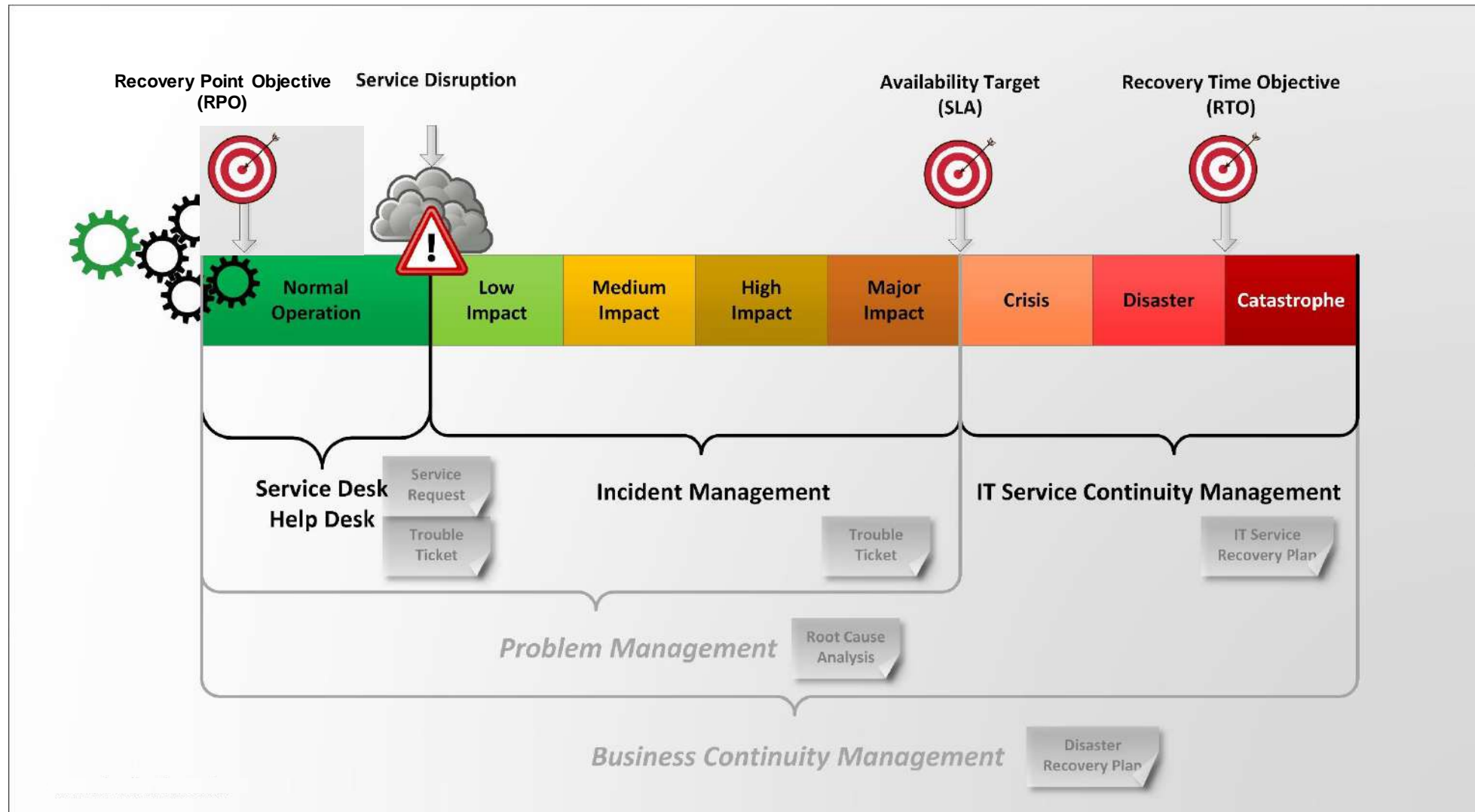
Complete the Major Incident Handling Organisations with Cybersecurity Scenarios & Exercises.

Group Crisis Manager and Group Crisis Staff

Business Unit Emergency Organisations (3 Escalation Levels)



Prepare and Exercise Recovery Plans (BCM, ITSCM)



Conclusion

Converged IT OT Cyber Security will be successful, if the effort of the adversary in relation to the expected return is too high.

Questions?



Thank you for your Attention.

Ivo Maritz
Executive Consultant, Cyber Security
ivo.maritz@bkw.ch
www.bkw.ch

