IT-S NOW

Accenture Security

Cyber Security for Industry

IT-S NOW

Cyber Security for industrials

What cyber security poses to companies operating in the IoT/OT area? And what are limitations of current methodologies?

Introduction

Threat Landscape

IOT/OT Challanges

IOT/OT Industrie insights/status

Security Projects for IOT/OT

Near Future challanges

>

Presentors

IT-S NOW

Wolfgang Mödritsch

AT

Application Security

Stefan Pfeiffer

AT

Cyber Resilience

Sybil Moser

AT

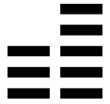
Data and AI Security

>

Answers of the most common economic questions

IT-S NOW

FINANCIAL SERVICES



Banking
Insurance

PRODUCTS

Life sciences
Retail
Manufacturing / Auto

HEALTH & PUBLIC SERVICE

Health
Government

RESOURCES

Energy
Utilities

COMMUNICATIONS MEDIA & TECH

Media
Communications
Software & platforms
Aerospace & defense

PAIN POINTS

- Cyber risk management
- Anti-money laundering
- Know Your Customer
- Crypto-currency
- Blockchain

- Retail fraud
- Connected car
- Safety

- Digital health
- Patient data protection
- Digital citizen
- eBorders
- Cyber intelligence

- Industrial Control Systems Security & Analytics
- Securing Critical infrastructure
- Safety

- Secure product development
- Intellectual Property theft

We help our clients to solve their biggest security challenges & PREPARE FOR THE FUTURE

IT-S NOW

PREPARE FOR THE REAL CYBER WAR

» Enterprises are targeted by more and more sophisticated **Cyber attacks** from **highly professional adversaries**.

» We help our clients to **prevent**, **detect**, **response** and **recover** from Cyber Attacks to secure the value of their business.

ENABLE YOUR SECURE DIGITAL TRANSFORMATION

» **Trust is the foundation** of digital business.

» Therefore, we take care that customers can rely on **secure Digital Identities** and a **secure digital user experience**.

SECURE YOUR JOURNEY INTO THE NEW (CLOUD, AI, ROBOTICS)

» Our clients are on their way into **new technologies.**

» We support them on their journey by **covering potential security risks** in their transformation.

RUN YOUR SECURITY ORGANIZATION EFFICIENTLY & COMPLIANT

» Security spend and **operational costs** are increasing over the last years. To find the **right talent** in the market is becoming more and more a challenge.

» We know how to **focus security investments** most efficiently and to **optimize security operations** compliant.

PROTECT & MANAGE YOUR DATA

» Data is the new Oil and clients want to **maximize** their **value** out of their data.

» We know how to **manage and use Data in a secure way** and in the context of **actual regulations.**

Cyber Security for industrials

What cyber security poses to companies operating in the IoT/OT area? And what are limitations of current methodologies?

Introduction

Threat Landscape

IOT/OT Challanges

IOT/OT Industrie insights/status

Security Projects for IOT/OT

Near Future challanges

>

Development of Threat Actors

IT-S NOW

Chronology of Threat Actors

Cyber Threat Actors	Motivation
Script kiddies	Profit/Satisfaction
Nation States	Geopolitical
Hacktivists	Ideological
Terrorist Groups	Ideological violence
Insider Threats	Discontent
Cyber criminals	Profit
Hacking as a Service (HaaS)	Profit
AI Assisted Hacking	all above

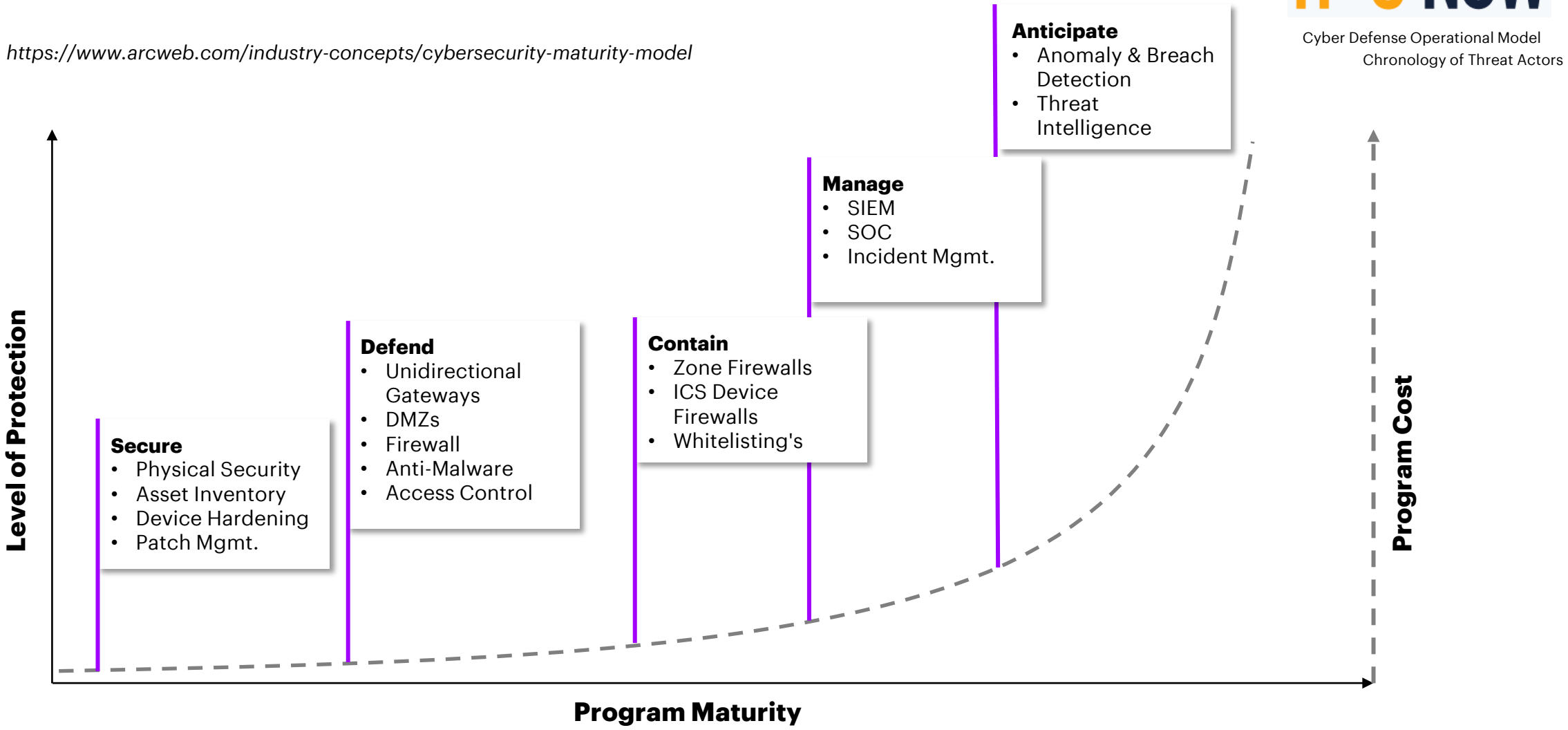
>

Cybersecurity Maturity Model

IT-S NOW

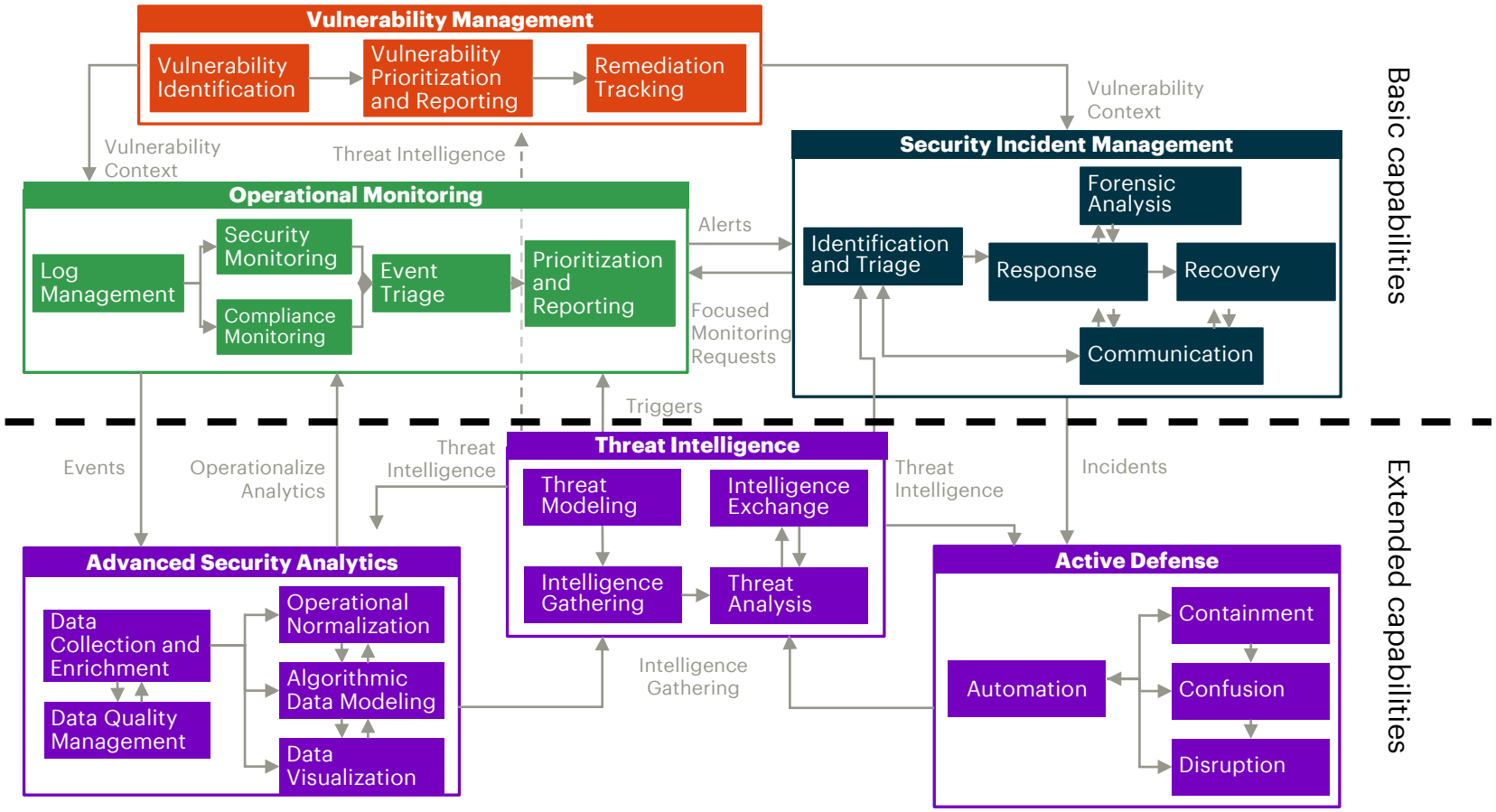
Cyber Defense Operational Model
Chronology of Threat Actors

https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model



Example Cyber Defense Setup

Cyber defense operating model



MITRE Att&ck

IT-S NOW

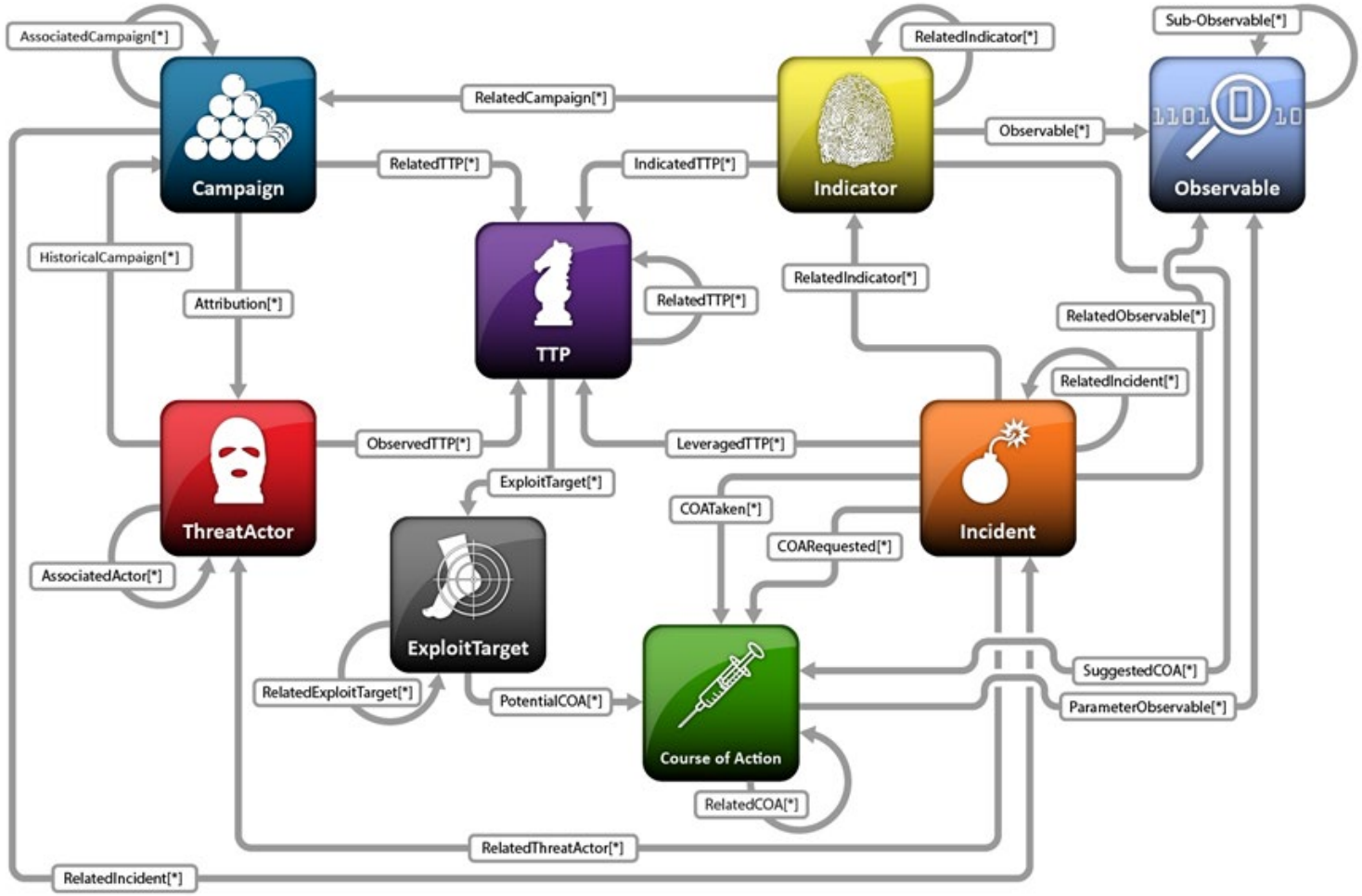
How we apply a framework to an attack?

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration
51 items	27 items	49 items	18 items	17 items	17 items	25 items	13 items	9 items
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration
Accessibility Features T1015	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Network Shared Drive	Exfiltration Over Command and Control Channel
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Permission Groups Discovery	Pass the Ticket	InstallUtil	Data from Removable Media	Exfiltration Over Other Network Medium
Browser Extensions	Dylib Hijacking	Deobfuscate/Decode Files or Information	Hooking	Process Discovery	Remote Desktop Protocol	Launchctl	Data Staged	Exfiltration Over Physical Medium
Change Default File Association	Exploitation of Vulnerability	Disabling Security Tools	Input Capture	Query Registry	Remote File Copy	Local Job Scheduling	Email Collection	Scheduled Transfer
Component Firmware	Extra Window Memory Injection	DLL Search Order Hijacking	Input Prompt	Remote System Discovery	Remote Services	LSASS Driver	Input Capture	
Component Object Model Hijacking	File System Permissions Weakness	DLL Side-Loading	Keychain	Security Software Discovery	Replication Through Removable Media	Mshta	Man in the Browser	
Create Account	Hooking	Exploitation of Vulnerability	LLMNR/NBT-NS Poisoning	System Information Discovery	Shared Webroot	PowerShell	Screen Capture	
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Network Sniffing	System Network Configuration Discovery	SSH Hijacking	Regsvcs/Regasm	Video Capture	
Dylib Hijacking	Launch Daemon	File Deletion	Password Filter DLL	System Network Connections Discovery	Taint Shared Content	Regsvr32		
External Remote Services	New Service	File System Logical Offsets	Private Keys	System Owner/User Discovery	Third-party Software	Rundll32		
File System Permissions Weakness	Path Interception	Gatekeeper Bypass	Replication Through Removable Media		Windows Admin Shares	Scheduled Task		
Hidden Files and Directories	Plist Modification	Hidden Files and Directories	Securityd Memory		Windows Remote Management	Scripting		
Hooking	Port Monitors	Hidden Users	Two-Factor Authentication Interception			Service Execution		
Hypervisor		Hidden Window				Source		
Image File Execution Options Injection		HISTCONTROL				Space after Filename		
		Image File Execution Options				Third-party Software		

Finding the Connection

IT-S NOW

Artifact to Cyber Attack: Forensics



Security Challenges

IT-S NOW

With a spotlight on IoT/OT

Insight into Systems with no perfect solution

Planning/Rollout against never change a running system

Security implementation with high costs

CI**A** with a focus on Availability

Cyber Security for industrials

What cyber security poses to companies operating in the IoT/OT area? And what are limitations of current methodologies?

Introduction

Threat Landscape

IOT/OT Challanges

IOT/OT Industrie
insights/status

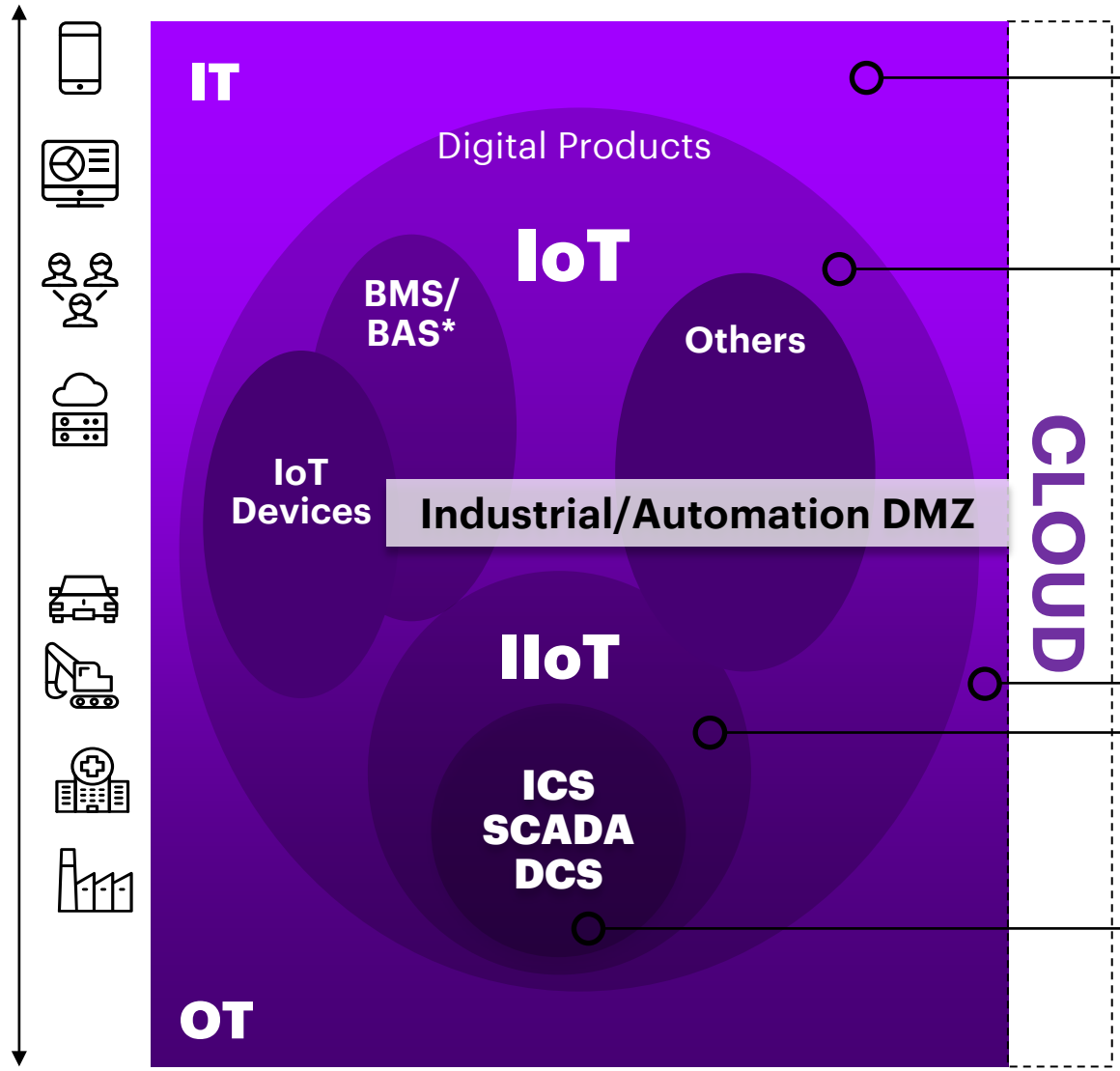
Security Projects for IOT/OT

Near Future challanges

>

Defining the new IT | OT | IIoT Technology Ecosystem

IT-S NOW



Information Technology

Covers the spectrum of technologies for information processing in the enterprise, including software, hardware, communications, and services.

Internet Of Things (IOT)

The network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. (Gartner definition)

Operational Technology (OT)

Hardware and software that detects or causes a change of state, through the direct monitoring and/or control of physical devices, processes and events in the enterprise. (Gartner definition)

Industrial Internet Of Things (IIOT)

Internet-connected systems used to monitor and control physical processes or events; refers to industrial automation of all types.

Industrial Control Systems (ICS)

Systems used to monitor and control physical processes or events; includes Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), Building Management Systems, etc.

* Building Management Systems (BMS, BMCS) or Building Automation Systems

KEY DIFFERENCES BETWEEN IT AND OT

IT-S NOW

WE UNDERSTAND THE SPECIFIC CHALLENGES OF OT-SECURITY, AND THE DIFFERENT OPERATIONAL REQUIREMENTS WHICH IMPACT OT SYSTEMS' ABILITY TO RESPOND AND ADAPT TO THREATS

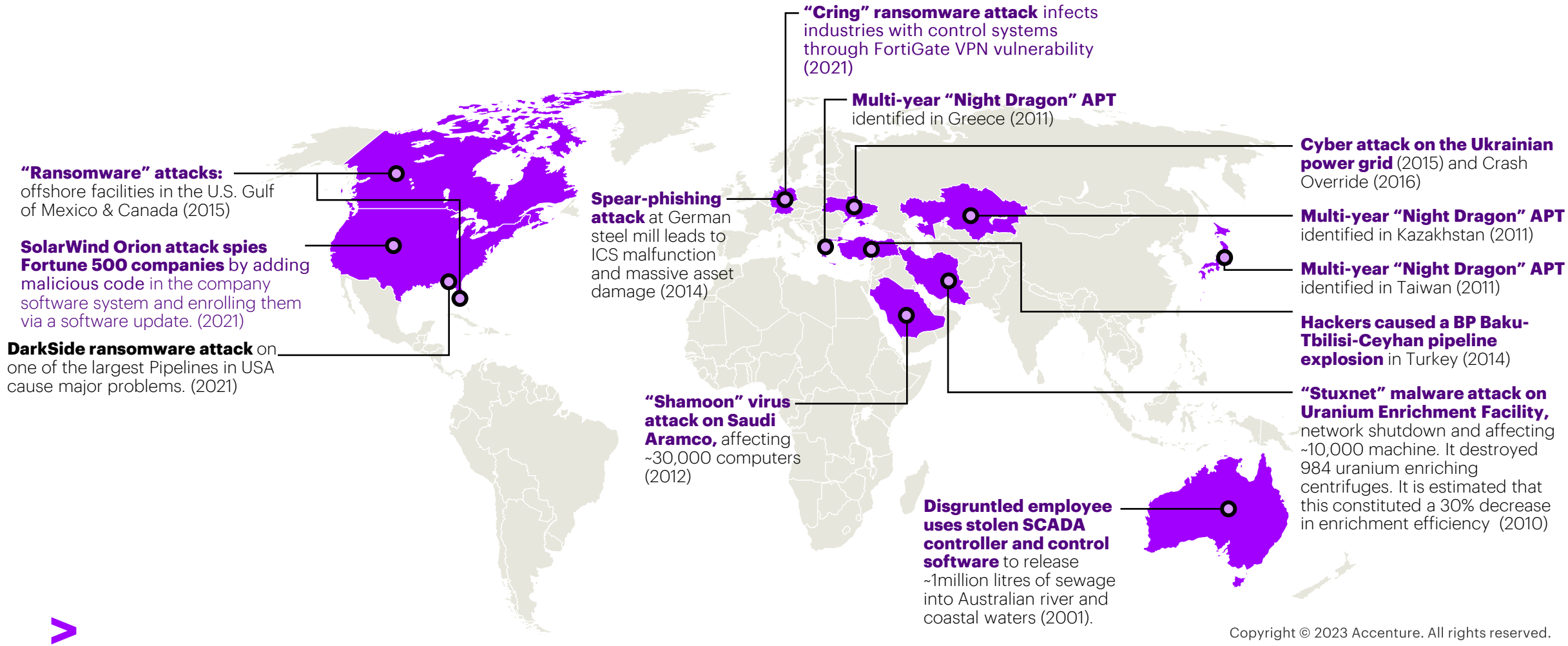
OT		IT
Limited data capacity and computing power	⟷	High data capacity and computing power
Safety Operations is critical	⟷	Few safety critical operations
High availability & integrity are vital with less stringent confidentiality requirements	⟷	Confidentiality & integrity are vital while availability is important
Critical operation and systems at edge of network with human operators at the center	⟷	Critical operation and systems at center of network, Human users at edge
Long life resulting in legacy, unsupported infrastructure	⟷	Continuous equipment upgrade with short life cycles
Essential equipment and operations remotely deployed at edge of network	⟷	Essential equipment and operations concentrated at center of network
Slow response to threats – rapid patching might be impossible due to outages	⟷	Rapid response to threats, patching and reboots acceptable

SECURITY CONCERNS ⟵ **SAFETY** — **AVAILABILITY** — **INTEGRITY** — **CONFIDENTIALITY** ⟶

IOT/IIOT Security is challanged

IT-S NOW

The increasing number of cyber attacks against ICS and critical infrastructure has demonstrated to the industry a few years ago, that it already represents a real risk to client businesses



The Industry on a page
What makes Industrial so special

- **HETEROGENEITY** – auto suppliers, heavy construction, freight & logistics …. and the diversity of industries they serve.
- **GLOBAL X GLOBAL** – sell and operate from everywhere…China, Germany, US, Japan, Mexico … Global x Global = Complex Supply Chains.
- **ENGINEERING** – strong product culture, hardware heritage, R&D drives innovation…
- **CONSERVATIVE** – 82% of the C-suite are homegrown (1) , last major industry shift was really the industrial revolution in the mid 19th c.
- **DISRUPTION IN SIGHT** – at the mist of the 4th industrial revolution powered by Digital… Susceptibility to Future Disruption = HIGH.
- **ECONOMIC UNCERTAINTY** – facing a downturn (could even go as far as saying a recession) even before the Covid 19 pandemic came about.
- **THIN MARGINS** – from low single digit in automotive to low double digit in pure machine equipment ….Investment capacity low, need to get it right the first time.

Note : Homegrown meaning has been in the company more than 20 years

IT-S NOW

Cyber Security for industrials

What cyber security poses to companies operating in the IoT/OT area? And what are limitations of current methodologies?

60

Introduction

Threat Landscape

IOT/OT Challanges

IOT/OT Industrie insights/status

Security Projects for IOT/OT

Near Future challanges

>

The new IT organization needs to implement key IT | OT | IoT security functions

IT-S NOW

IN ALL INDUSTRIES THE DIGITALIZATION REQUIRES INCREASING CONNECTIVITY, MAKING THE VULNERABILITY OF IOT ELEMENTS MUCH MORE EASILY EXPLOITABLE. SAFETY CONCERNS ENFORCE SECURITY MEASURES

Protect business and brand

Customer Demand

- Customers requesting from suppliers placing equipment into their productive environment to „prove“ their security – see also compliance
- Customers are requesting to be informed on important vulnerabilities
  (Driver: „log4j“ issue)

Integrity, Safety and Brand

- Security ensures to be seen as a trustworthy partner with **minimal business risk**
- Protects the **confidentiality and integrity** of information critical its **brand name**
- Meets operating requirements to protect **health & safety, people, and environment**

Compliance & Brand

Various Industries are driven by emerging security standards:

- Critical Infrastructure: NIS, Suppliers: NIS2
- Production: IEC 62443
- Automotive: UNregNo155
- Compliance to **legislation,** (e.g., GDPR,) is a must to protect against **risks and liabilities**

By safeguarding assets

Data

Corporate information that **support the enterprise, records interactions, and operations**

..which enables..

Applications

Programs and software designed to **enable specific business purposes and tasks** required by end users

..connected by..

Network & Services

Provide and enable enterprise **connectivity, communication, and operations**

..interacting with..

Physical Infrastructure

Computer systems, industrial machinery (OT[1]), or other end user devices that **enable functionality**

..thereby protecting..

People

health & safety elements that are influenced by functionality of IT and especially OT[1]

Against emerging risks and threats

External drivers

Growing Critical Infrastructure, Application and Data Threats increases risk exposure due to connectivity, open protocols and likelihood of insider threats

Legal & Regulatory Compliance Requirements like UNregNo155, GDPR and nation sanctions add complexity to compliance and assurance processes

IT OT

IT Security: Cybersecurity focusing on organizational assets (i.e., computers, networks and data)

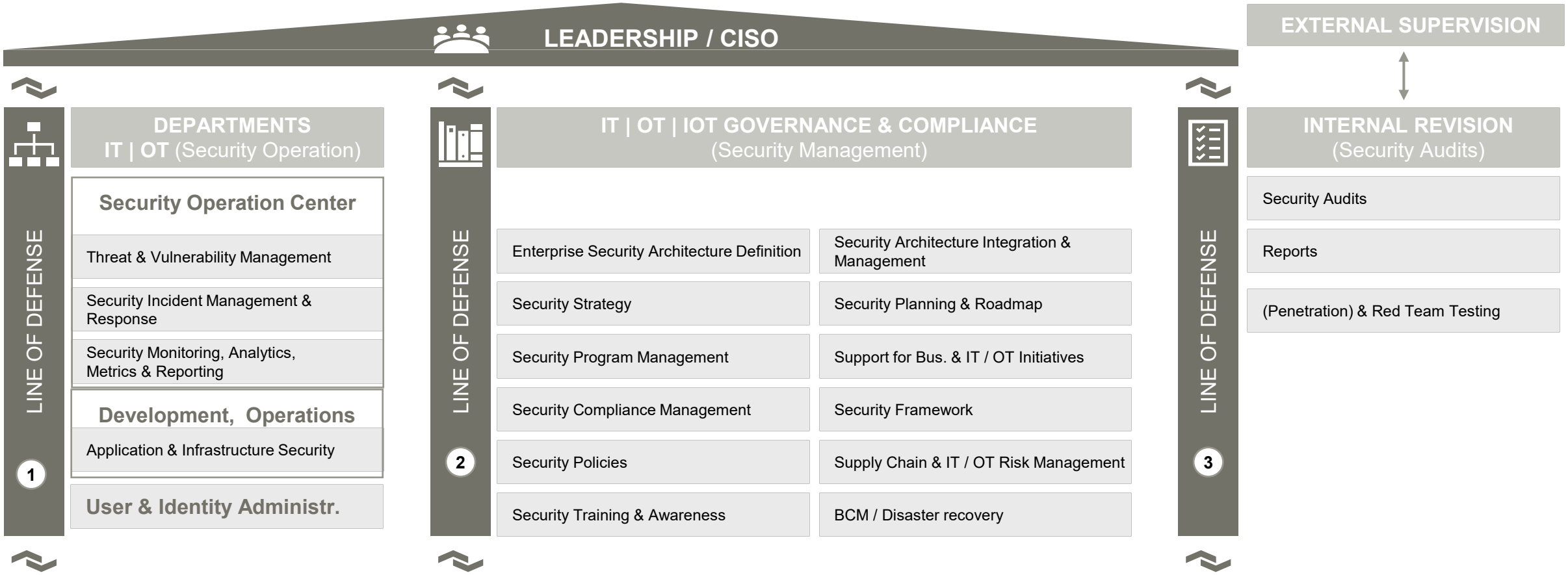
OT Security: Cybersecurity focusing on monitoring threats to physical devices (i.e., machinery) to protect the essential core business

Internal drivers

Convergence of IT and OT[1] on assets introduces complexity in the landscape leading to increasing threats, vulnerabilities, and attack vectors

A shift to Agile Product Teams & DevOps opens new risks as part of the new Agile way of working by Business and IT

Implement key security functions for Security Strategy, Governance and Compliance in IT | OT | IoT



IT | OT | IoT Security Transformation with a vision, small steps and in close cooperation of IT and OT departments

IT-S NOW

The security maturity level was determined with the help of a security assessment.

Critical points were addressed with immediate measures

At the beginning, a vision of IT security was defined together with the customer and pursued across all projects

Fast and sustainable results were achieved with co-creation and agile methods

Cyber Security for industrials

What cyber security poses to companies operating in the IoT/OT area? And what are limitations of current methodologies?

Introduction

Threat Landscape

IOT/OT Challanges

IOT/OT Industrie insights/status

Security Projects for IOT/OT

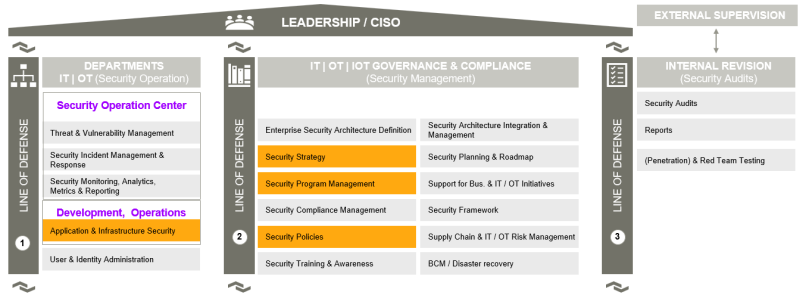
Near Future challanges

>

Project Example: Governance and Application Security (Product) for OT Application Development

IT-S NOW

International company producing machines for Food, Pharma, Chemical and other special industries



Product Development

SW is everywhere

- As SW is part of every machinery nowadays, creating secure sofware even in the area of production is becoming relevat.
- Up to now, basically the only security measuer was physical access protection.

Challanges

Distributed Development

- SW development is distributed in Organisational pillars, countries, locations
- No working overall security governance structure: Organization, Policies, Knowledge, et.
- Wide range of project size: From 7h to years programs

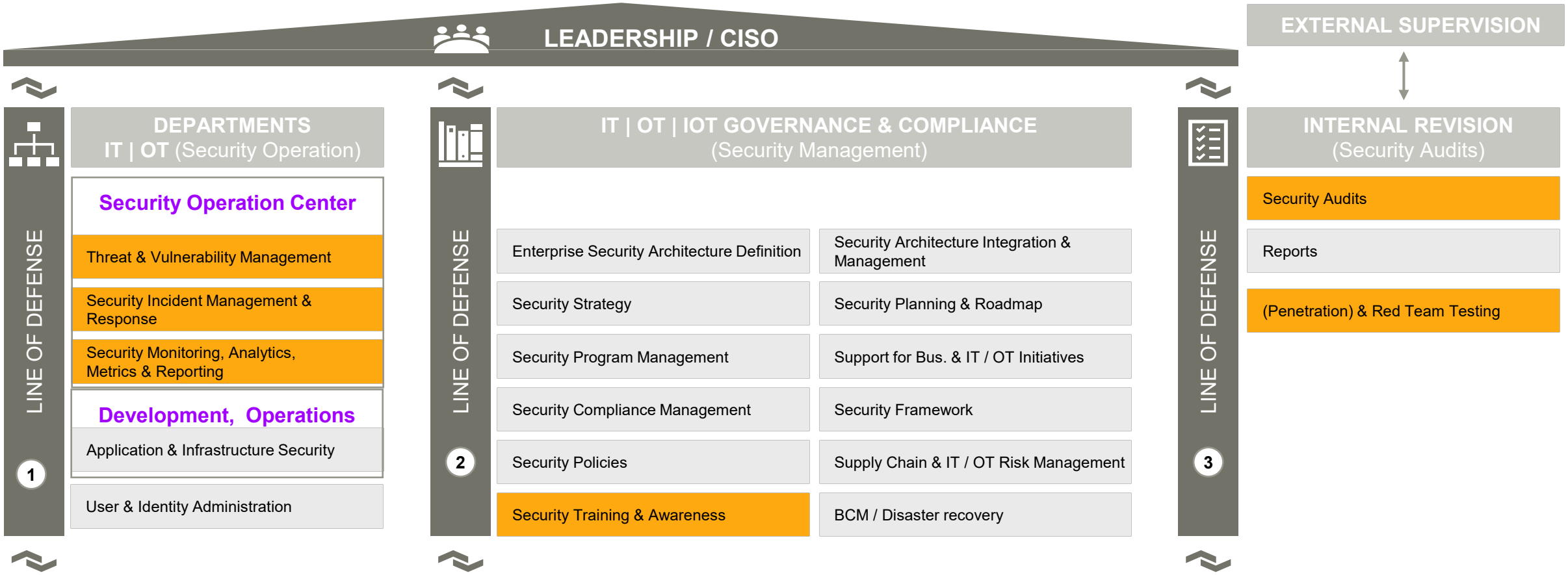
The project

Working with limited ressources

- Governance – No security culture in product development
- Onboarding of new staff very slow.
- Work in parallel to daily project work
- Resulting in long project durations (Years)

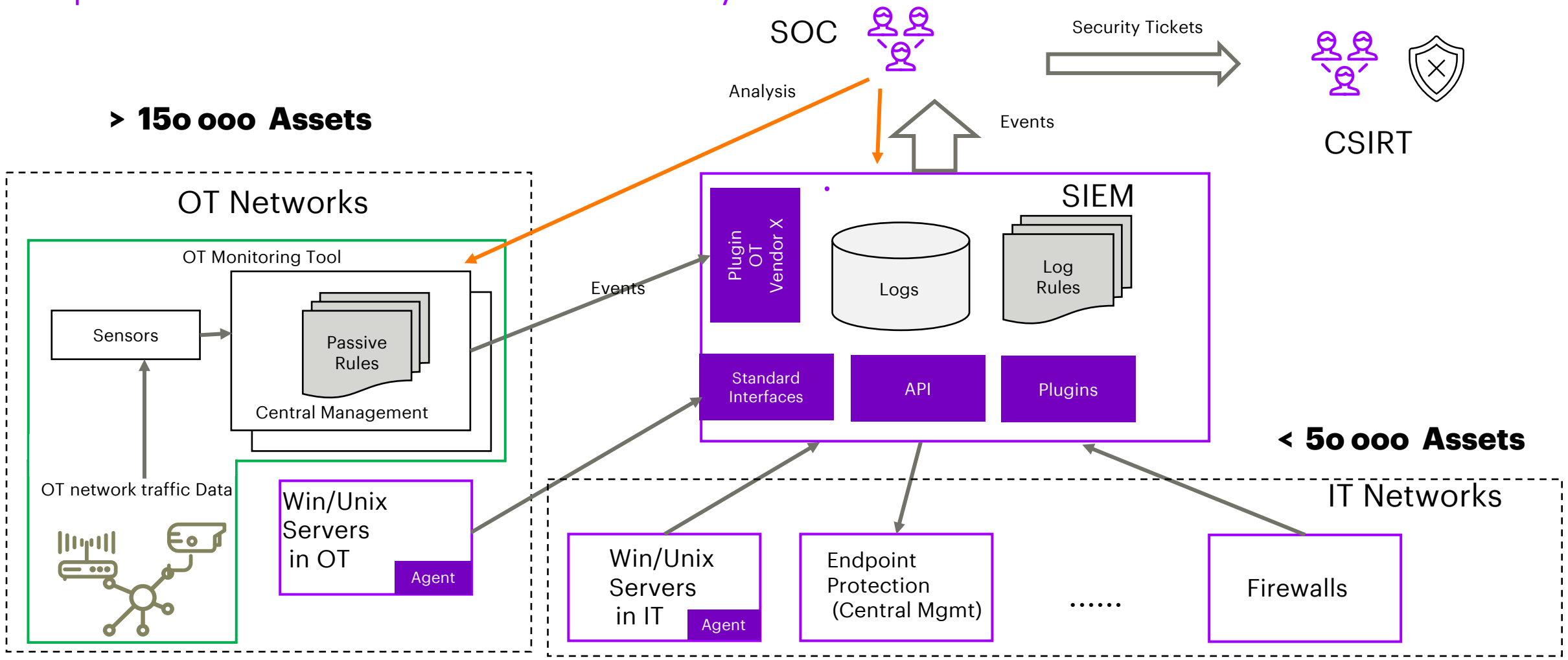
>

Implement key security functions for Security Strategy, Governance and Compliance in IT | OT | IoT



IT und OT Monitoring – large Infrastructures

A unique view on both IT and OT Infrastructure is key



Cyber Security for industrials

What cyber security poses to companies operating in the IoT/OT area? And what are limitations of current methodologies?

Introduction

Threat Landscape

IOT/OT Challenges

IOT/OT Industrie insights/status

Security Projects for IOT/OT

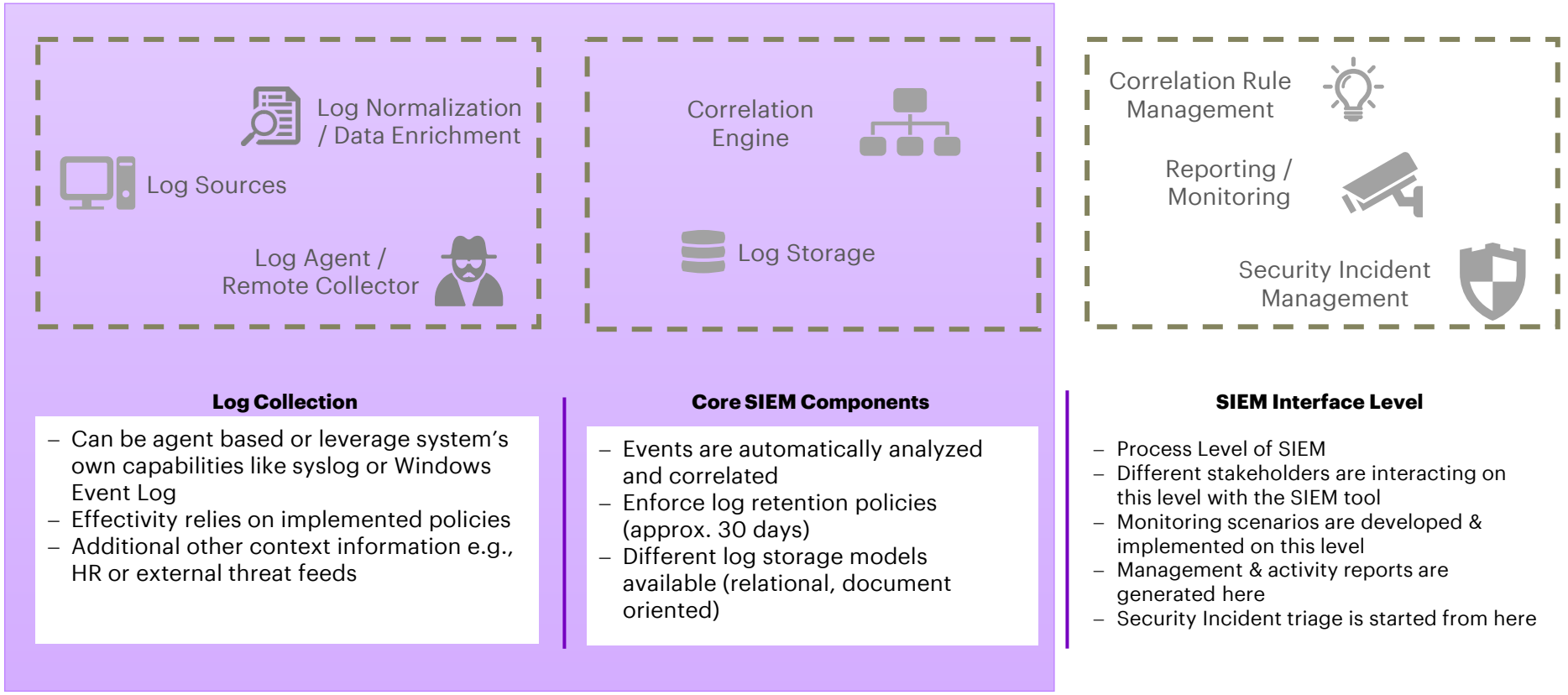
Near Future challenges

>

High Level Deployment Architecture

IT-S NOW

SIEM Basic Architecture



Log Collection

- Can be agent based or leverage system's own capabilities like syslog or Windows Event Log
- Effectivity relies on implemented policies
- Additional other context information e.g., HR or external threat feeds

Core SIEM Components

- Events are automatically analyzed and correlated
- Enforce log retention policies (approx. 30 days)
- Different log storage models available (relational, document oriented)

SIEM Interface Level

- Process Level of SIEM
- Different stakeholders are interacting on this level with the SIEM tool
- Monitoring scenarios are developed & implemented on this level
- Management & activity reports are generated here
- Security Incident triage is started from here

Security Operation Center (SOC)

IT-S NOW

SOC vs NOC

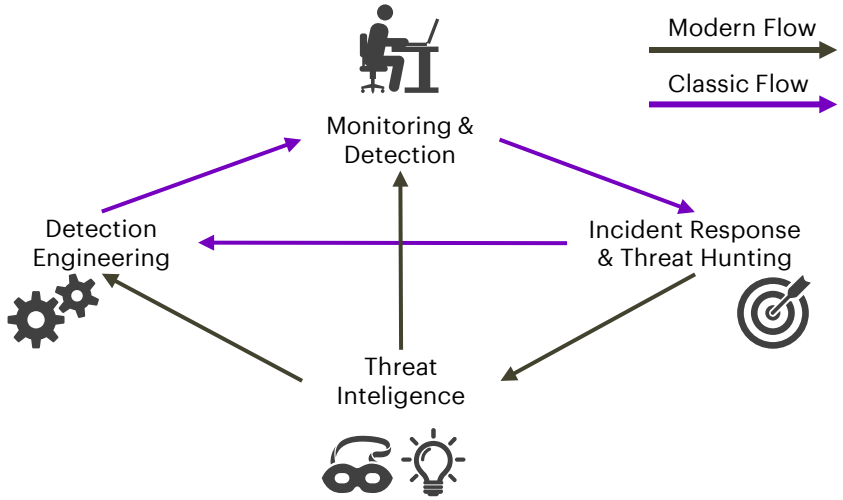
Development Assumptions for Security Operation Centers

- By 2019 50% of midsize and large companies will conduct security work out of an owned or shared security operations center.
- 2015 only 15% of security work is delivered from a security operation center
- Security operations centers (SOCs) have historically been adopted by very large organizations requiring centralized and consolidated security operations primarily for efficiency and cost reasons.
- The evolving and escalating threat environment and the shift in security defense from "Prevent" to "Detect and Respond" has prompted a renewed adoption of SOCs by a wider user base

SOC Definition

A SOC is defined as both a team, often operating in shifts around the clock, and a facility dedicated to and organized to prevent, detect, assess and respond to cyber security threats and incidents, and to fulfill and assess regulatory compliance. The term "cyber security operation center" is often used synonymously for SOC.

Functional view of a modern SOC

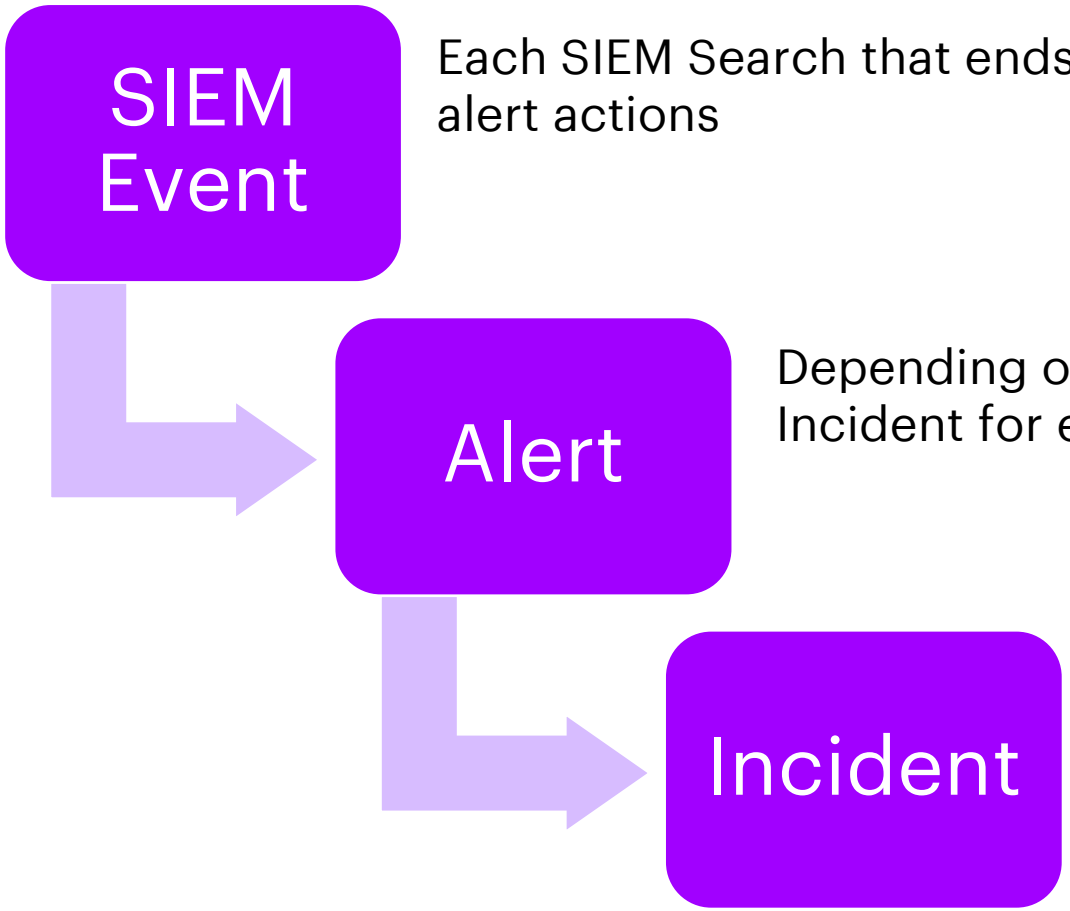


Functional Description

- Security device management and maintenance
- Threat and vulnerability management
- Security monitoring and auditing
- Cyber security incident response management
- Security compliance management

Normal UC Alert Process

Each alert will create an Incident. Every UC should have a high chance to be applied to a malicious case.



Each SIEM Search that ends with results in the given Timeframe triggers the alert actions

Depending on the alert action settings the UC creates a SNOW Incident for each result created by the CS.

All Incidents from a UC are handled by hand and in case of duplicates the Analyst must close them. **The correlation of multiple UCs is pending on the Analyst.**

IoT Challenge for SIEM

IT-S NOW

CI**A** for IoT with a capital **A**vailability

Most security relevant logs come from Management Console

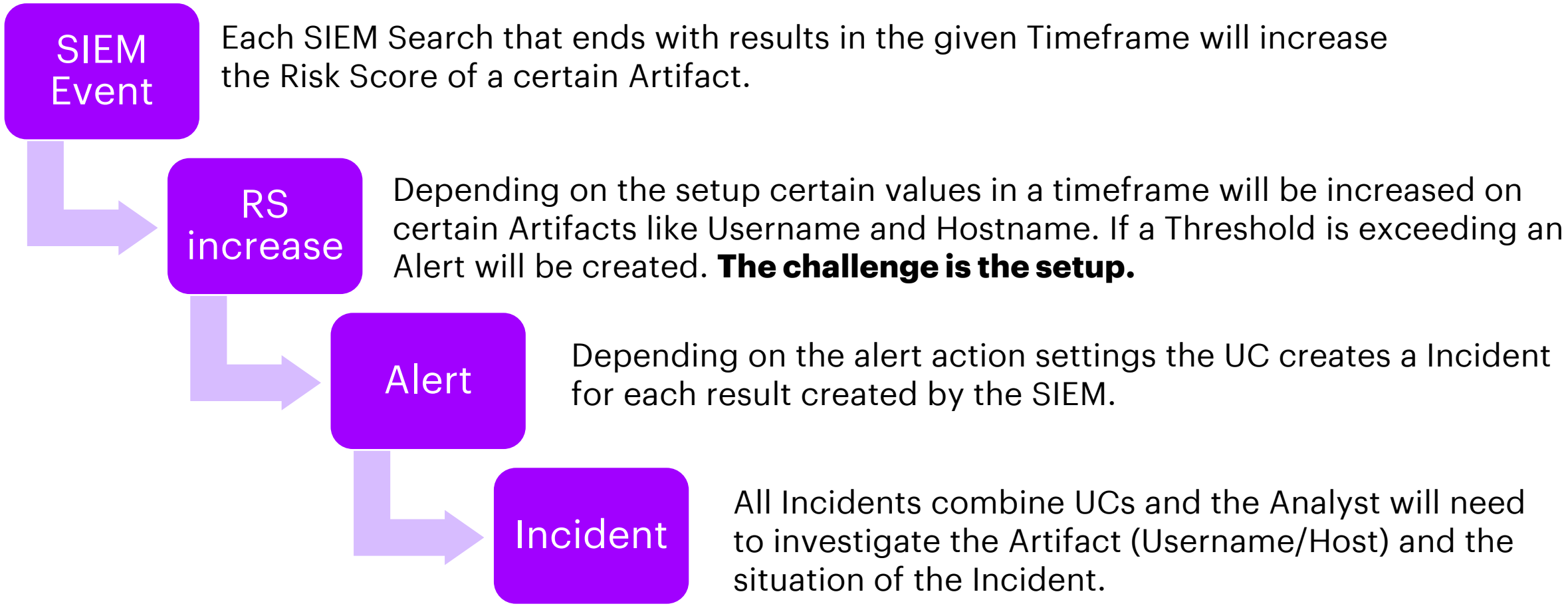
Logs of clients are most commonly availability/health focused

Difference between security and operational incident needs additional context

Risk UC Alert Process

IT-S NOW

Each alert will increase thresholds which can create an Incident. Every UC increase the score of an Artifact.



Finding Suspicious or Malicious Activities

IT-S NOW

Lets have a look

System Network Configuration Discovery: Internet Connection Discovery

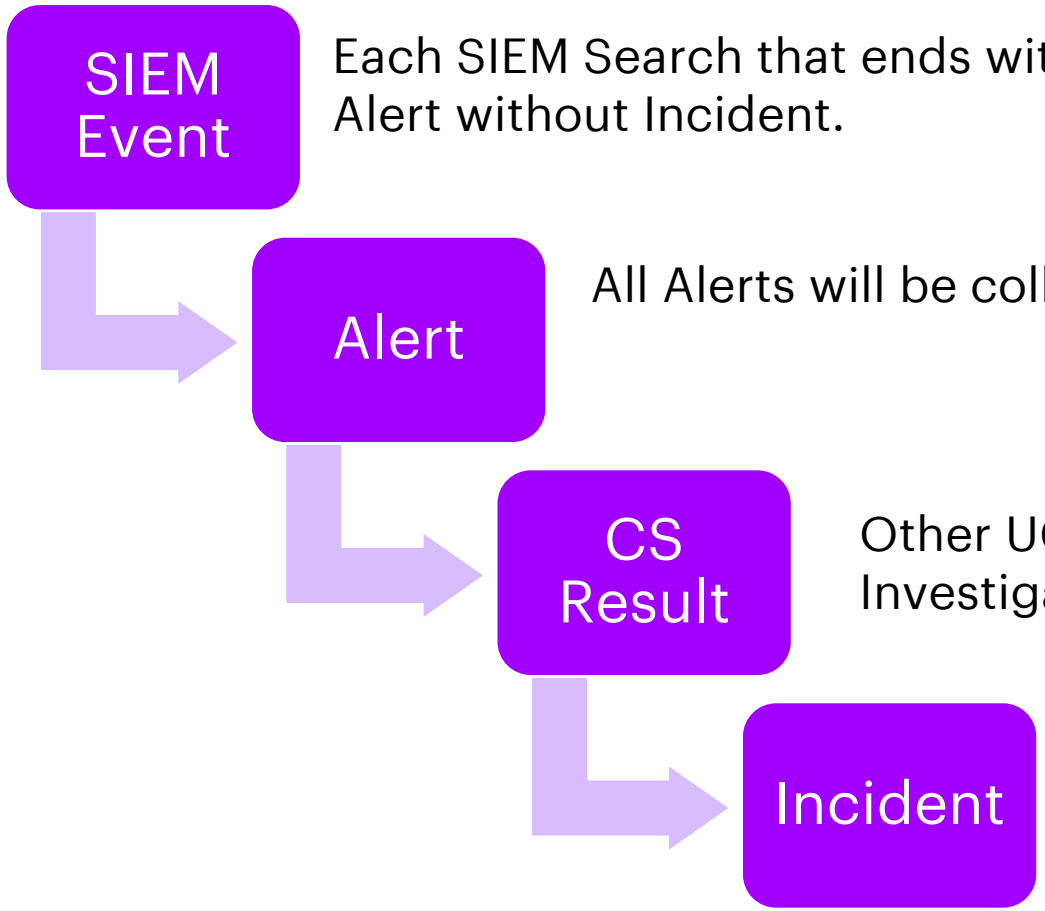
Adversaries may check for Internet connectivity on compromised systems. This may be performed during automated discovery and can be accomplished in numerous ways such as using Ping, `tracert`, and GET requests to websites.

Adversaries may use the results and responses from these requests to determine if the system is capable of communicating with their C2 servers before attempting to connect to them. The results may also be used to identify routes, redirectors, and proxy servers.

MITRE UC Alert Process

IT-S NOW

Each alert will be correlated to investigate attacks after MITRE.



Each SIEM Search that ends with results in the given Timeframe will create an Alert without Incident.

All Alerts will be collected and can be searched to correlate the UCs.

Other UCs can search for MITRE UC Alerts to change the Investigation or create an Incident on its own.

The Analyst can base or extended by the MITRE UCs.

THE CURRENT CHALLANGES WILL REMAIN DUE TO ONGOING IT-OT CONVERGENCE AND INERTNESS OF THE LARGE SYSTEMS

IT-S NOW

Technical Challenges

- Often missing or non-functional updated **visibility** of OT assets, their patch and security status, and their communication relationships.
- Lack of **zoning** and support for the zone model through coordinated network segregation and concepts for secure remote access and on-site maintenance.
- Incomplete protection of **vulnerable systems** through alternative measures such as whitelisting, encapsulation, or intensified monitoring.
- Insufficient support for **patch and vulnerability management** through centralized testing, authorization, implementation, and documentation.
- The threat level requires role-based **access rights management** and secure authentication but implementing them for many existing systems is time-consuming.

Organisation Challenges

- **Security organization** with clear roles and responsibilities, coordinated between OT and IT, at both the strategic and operational levels.
- **Governance** through coordinated policies, procedures, and directives, especially for essential processes such as asset, change, and patch management.
- Recruitment, training, succession planning, and ongoing awareness campaigns for employees in a tight, **specialized** labor market in OT security.
- **Supplier and vendor management**, particularly in contract/order management, remote access, on-site services, and patch management.
- Tested alerting, **crisis response** planning, and communication planning (security incidents), as well as **recovery** planning and restart planning (especially regarding backup and recovery).

Correlation is key

IT-S NOW

- AI/ML
- Attack Simulation
- CTI
- MITRE
- Risk based
- Purple Teaming

Thank you!

Any Questions?