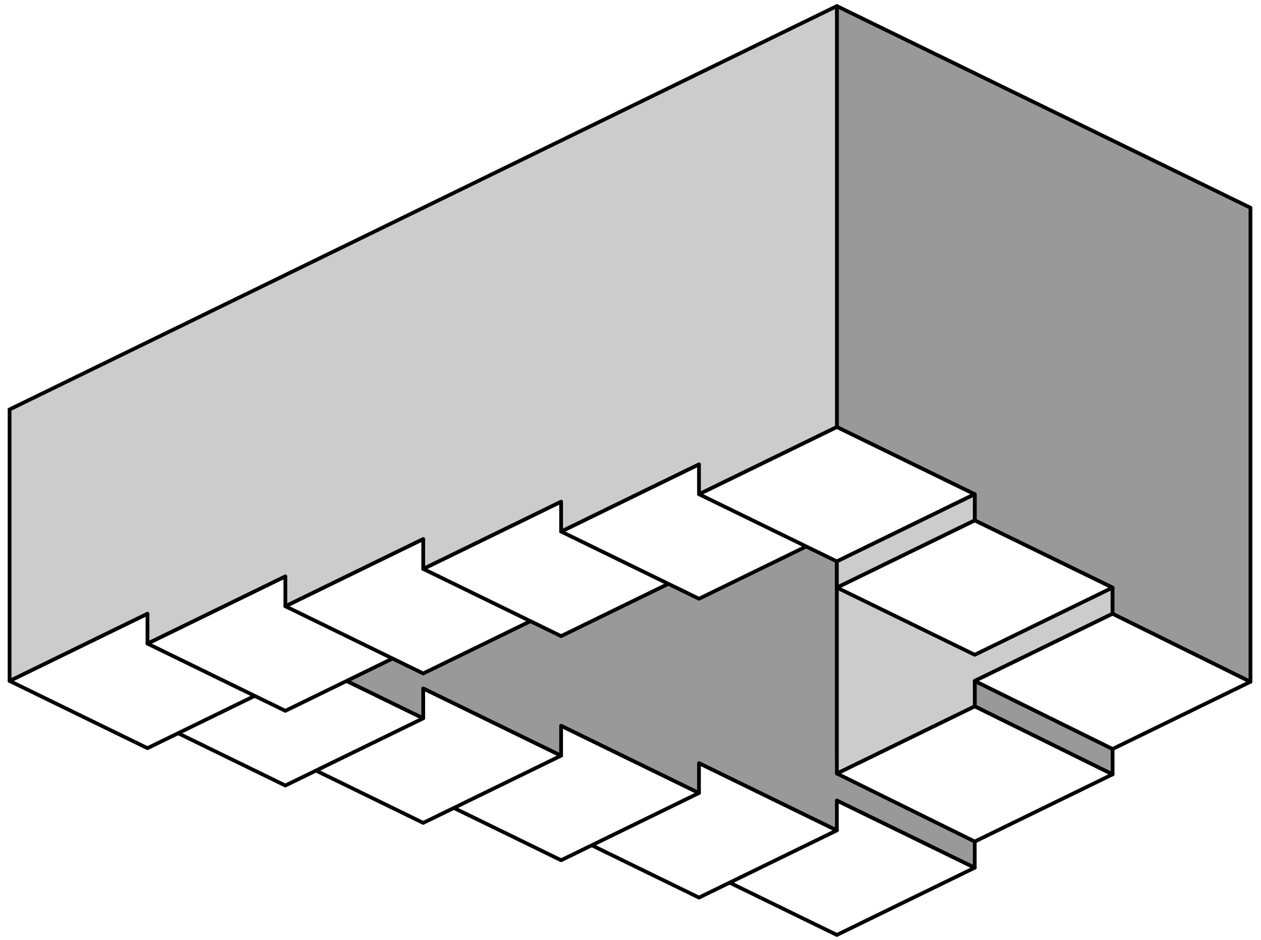
HSLU Lucerne University of Applied Sciences and Arts

Product Security Lifecycle – Post Launch Product Security 2

SPREN
Alex Diekmann



When the world turns upside down…

Information Technology
March 14, 2024

What you will learn

SPREN1

- **Understand** the difference between **Product Cyber Security** and Information Security
- **Explain** to Management and Developers **why** Product Security is essential
- Know and **apply relevant** Laws, Regulations and **Standards** for specific target markets
- **Build and integrate an SDLC** for Product Security purpose based on relevant standards
- How to do **Product Security Risk Management**
- How to deal with Mergers & Acquisitions from the Product Security perspective

SPREN2

- **Vulnerability Management**
- **Incident Handling**
- How to **share Vulnerability & Threat Information**
- How to **deal with Customers** and
- How to ensure **Supply Chain Security**
- **Applying the learnings** to a WIPRO project
- **Presenting findings**, selling measures

Other lectures

- Microsoft SDL
- Threat Modeling with STRIDE / DREAD
- Requirements Management

➢ **SPRG**

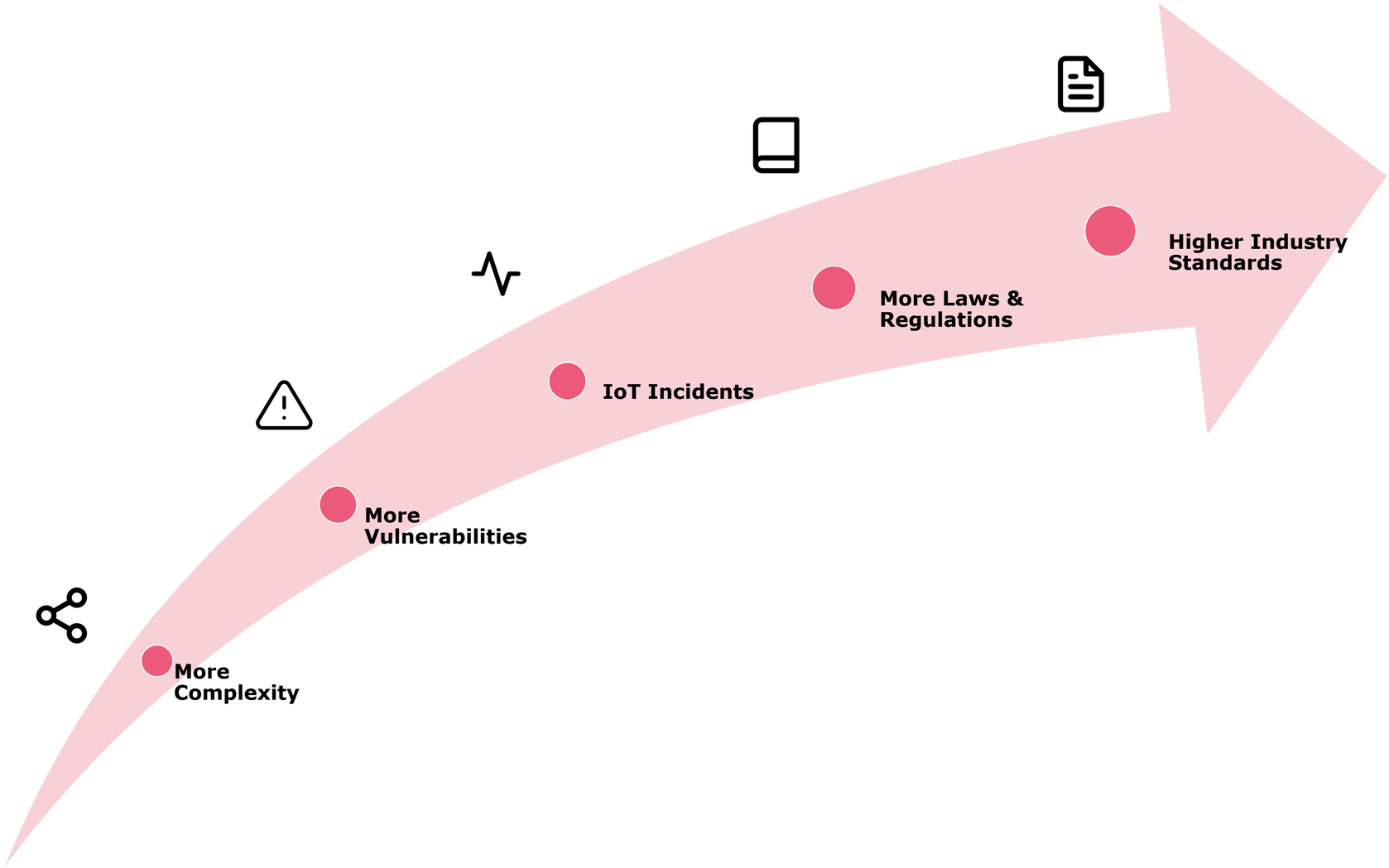
- Hardware Security & Pentesting

➢ **IoT Security**

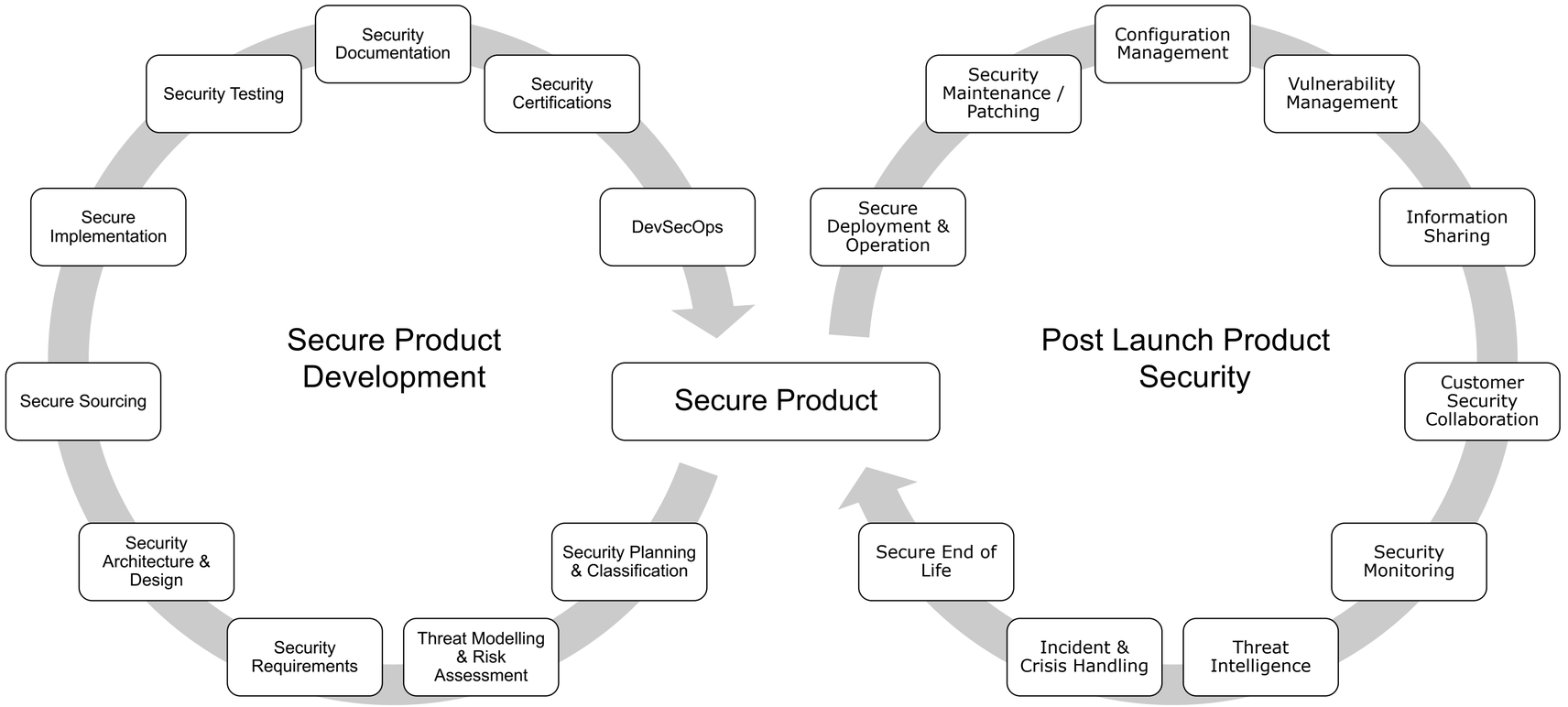
- Safety Risk Management

➢ **Advanced Risk Management**

Recap: External Drivers for Post-Launch Product Security



Product Cybersecurity Lifecycle



Cyber Security Management System(s)

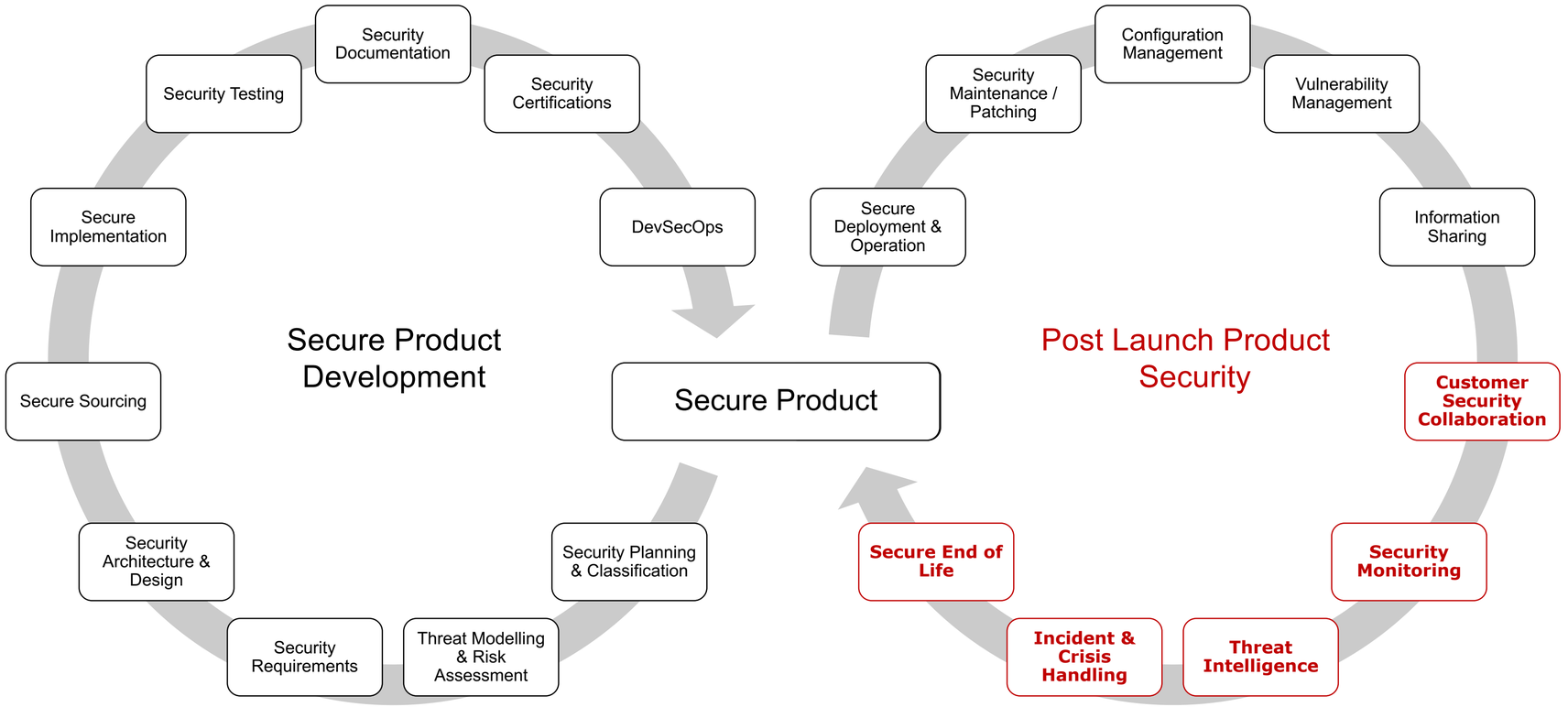
Development & Production Security

Security Risk Management

Organization, Culture, Awareness & Training

Supply Chain Security

Product Cybersecurity Lifecycle



Cyber Security Management System(s)

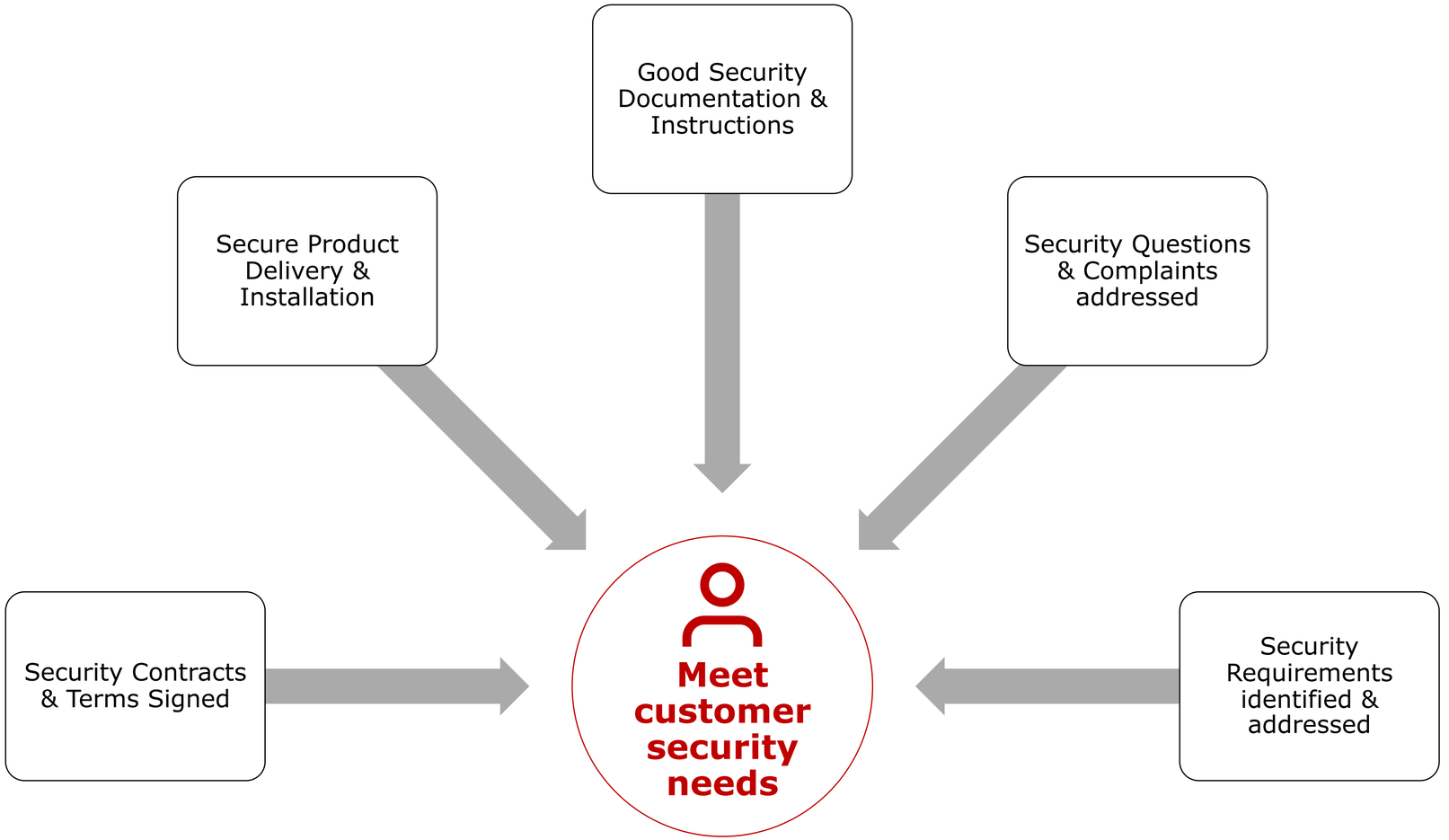
Development & Production Security

Security Risk Management

Organization, Culture, Awareness & Training

Supply Chain Security

Customer Security Collaboration



Customer Security Collaboration – What to prepare

Security Q&A Database

- Customer Questions & provided Answers
- Customer Security Requirements

Product Security Documentation

- Security Architecture / Features
- Installation Instructions
- Environmental Requirements
- Security Feature Configuration & Use
- Known Issues

Security Communication Channels

- Prod. Security Website
- Responsible Disclosure Policy
- Security Mailbox
- CRM Ticket Types & Queues

Trained Product Sales & Support Teams

- Security contract terms
- Secure Installation
- Answering Security Questions
- Identifying & escalating Security Issues

Security Contracts – Terms to Look for

Types

- Framework Contracts with security terms
- NDAs
- ISO21434 Cyber Security Interface Agreements & other responsibility agreements
- Joint Processes / SOPs

Product Security Terms

- (Product & Company) Certification Requirements
- Feature & Process requirements
- Documentation to be shared
- (Security) Support Period
- Security Testing requirements
- Vulnerability handling
  - Responsibilities
  - Notification duties
  - Fix cost

Other terms

- Non-Disclosure
- Right to Audit
- IP Ownership
- Information Security for confidential data
- Business Continuity (Product / Service Delivery)
- Requirements for sub-suppliers

How to interact with Customers

Sales & Contract negotiations

- **Listen** first, paraphrase what you've heared
  - ➢ make the customer feel understood
- **Get customer security experts** into the negotiation
- Don't outright reject problematic terms
  - **Stay curious**, try to understand where the demand comes from
  - **Ask** open "**What**" and "**How**" questions
  - **Acknowledge** your **accountability** for secure products
  - Make counter-proposals
- Directly talk to the customer, but keep sales & legal in the loop

Support / Questionnaires

- **Immediately acknowledge** the request: "Thank you! We're analyzing…"
- Provide **regular** status **updates**
- **Ask questions** back
  - ➢ Clarifies scope and intention of requests
  - ➢ Buys time
  - ➢ Customer feels heared
- **Answer within** set **deadlines**, even if the reply is incomplete

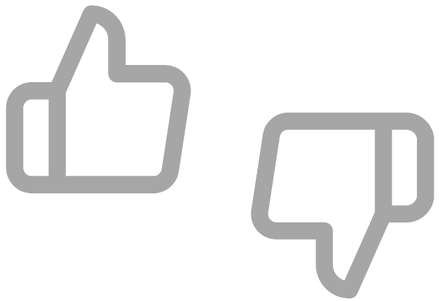
Security Issues

- **Immediate response** "We're analyzing"
- Establish **direct contact** between security experts working on the response
- **Clarify responsibilites** for the issue
  - Who fixes
  - Who pays
  - For incidents: help first, discuss payment later
- Issue on your side:
  - Ensure affected customers get **notified within agreed timelines** (latest within a week)
  - Provide regular status updates

Customer Security Collaboration - How to Execute

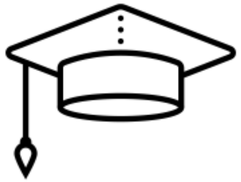
1. Conclude Security **Contracts / Agreements**
2. Secure **Deployment & Installation**
3. Answer Security **Questions / Complaints**
4. Identify and Address **Vulnerabilities / incidents**
5. **Lessons Learned**

- Maintain & Use the Q&A Database
- Answer FAQ in Product Documentation
- Involve Product Management



- Unreviewed communication
- Downplayed complaints
- Slow response

Quiz



A customer has vulnerability-scanned your product and found a couple of CVEs in the product. They demand all vulnerabilities must be fixed wihtin 30 days.
They furthermore announce that they will scan all your products sold to them on a monthly basis.

1. What's your first answer to the customer?

a) Based on our contracts, you are responsible for operating the product in a secure environment

b) This security testing was unauthorized, you'll hear from our lawyers

c) Thank you! We're analyzing, and will get back to you.

d) Thank you! We'll provide fixes for all of them in due cause.

2. What to do first with the vulnerability list?

a) Verfiy

b) Trigger fixes

c) Update Risk Assessments

d) Identify further affected products

3. How to deal with the continued testing?

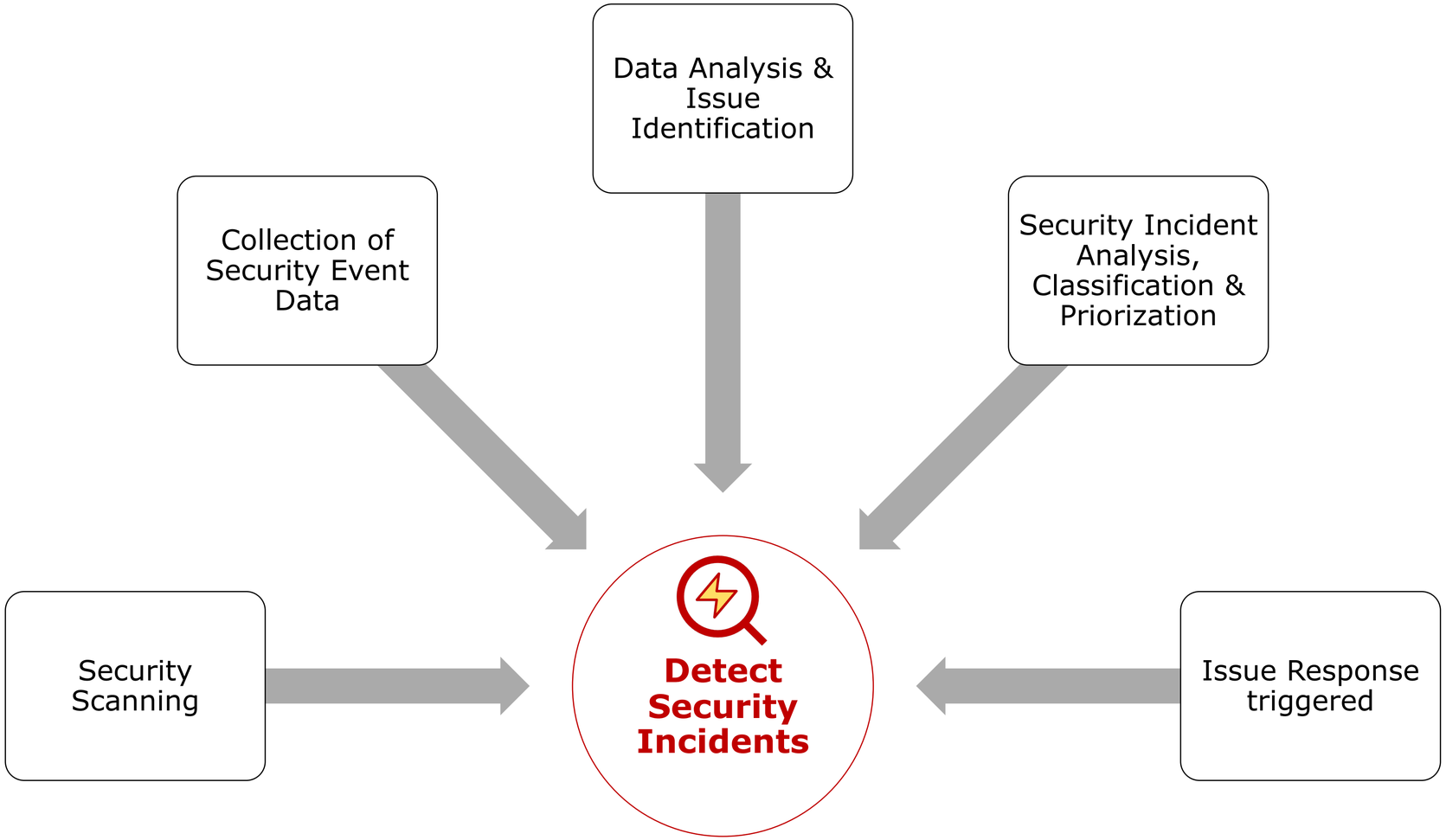
a) Be happy about the free security testing.

b) Improve internal testing to preventatively identify and handle known CVEs

c) Ignore further requests. The customer needs our product anyway

d) Rework the product design to prevent vulnerability scans from the outside

Security Monitoring



Security Monitoring – What to prepare

Asset Information

- Asset List
- Purpose
- Classification & Contacts
- Architecture
- 3rd Party Components

Data Sources

- Cloud / System / Event / Security Logs
- EDR / NDR Tools
- Vulnerability / Threat Information
- Notifications

Analysis tools

- IDS / IPS
- Cloud Security Proxies
- Behavioral / Reputation Analysis Tools
- Monitoring policies / rules

SIEM

- Aggregates Event Data
- Highlights issues
- Ticket Handling
- Self-Hosted or Cloud

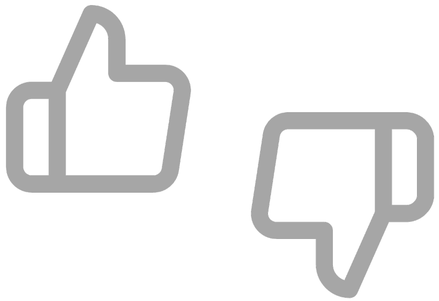
SOC

- Skilled Security Analysts
- 24/7 Operation
- Up-to-date Information, capabilities & toolchain

Security Monitoring - How to Execute

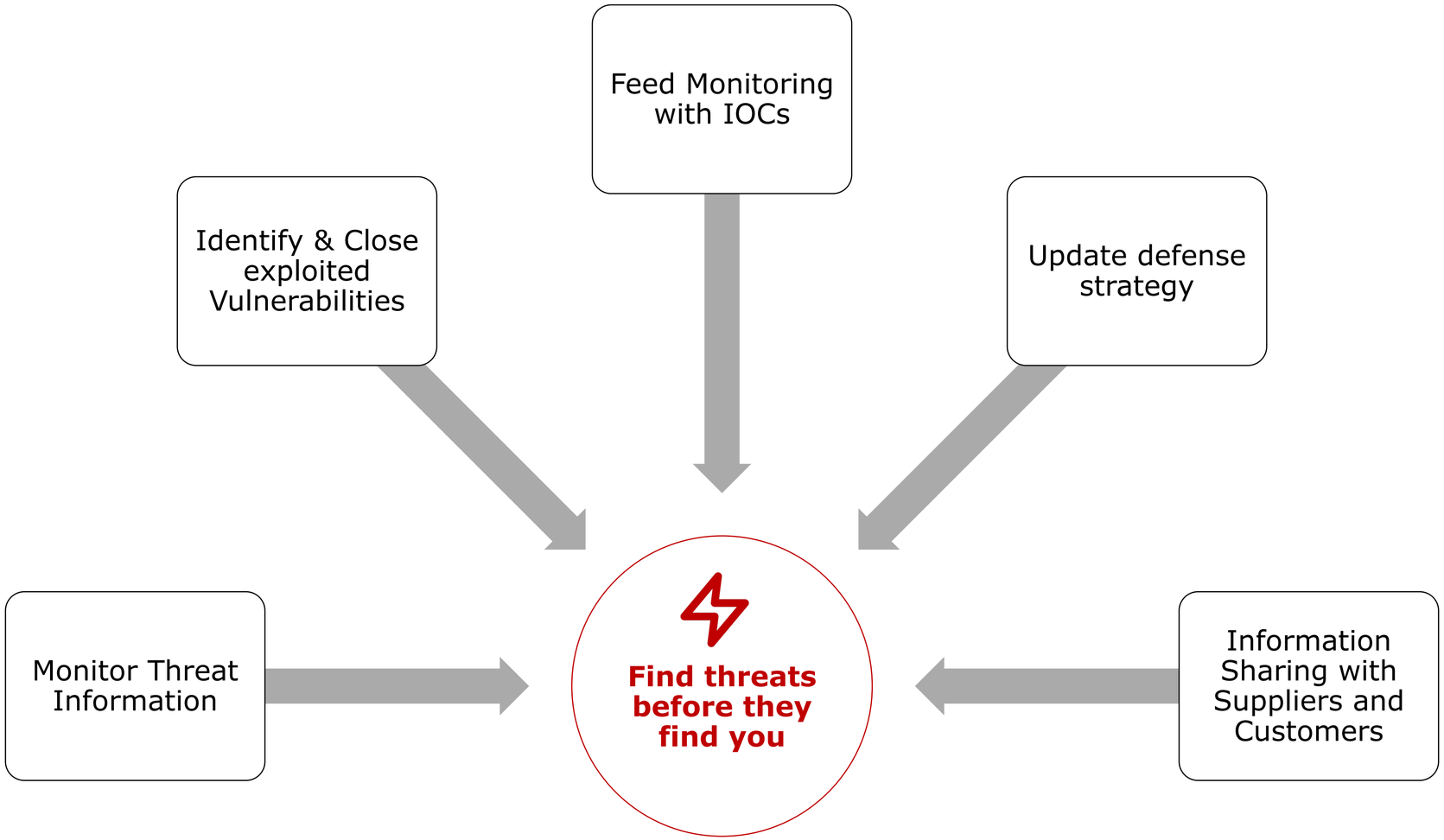
1. Capture Security Events → 2. Aggregate & Filter → 3. Classify & Triage → 4. Escalate & Follow-Up

- Corporate SOC Monitors Products
- Detailed Information improves detection
- Learning-phase before go-live

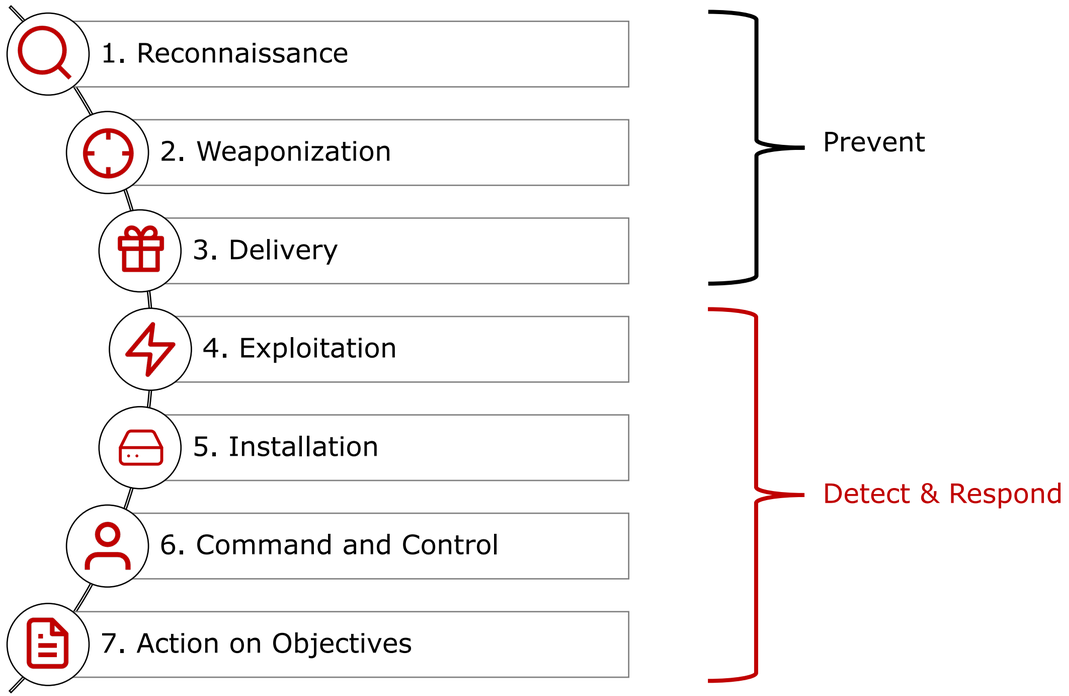


- Small companies building their own SOC
- SOC handling Product Security Incidents alone
- Lack of exit strategy for outsourced SOC

Threat Intelligence



Threat Intelligence - The Cyber Killchain



- Model to explain attacks
- Checklist for Controls
- Communication tool

- Not “one size fits all”
- Too Generic
- Not Standardized

Threat Intelligence – What to prepare

Threat Information

- Governmental CERTS
- ISACs / ISAOs
- Industry Organizations
- Industry Peer Groups
- Public Media

Partnerships

- Customers / Suppliers / Peer Groups
- NDA & Sharing Policies
- Information Exchange Interfaces

Tools

- Threat Information Gathering
- Ticket Handling
- Media Monitoring
- Security Monitoring Interfaces

Security Experts

- SOC
- CSIRT / PSIRT
- Other Security Experts

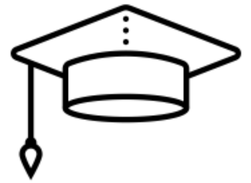
Threat Intelligence - How to Execute

1. Monitor Threat Information → 2. Identify relevant Threats → 3. Gather Detailed Information → 4. Analyze Impact → 5. Prepare & Monitor → 6. Share Learnings

- Integrate Threat Intelligence with Security Monitoring
- Learnings to improve product / system protection
- Potential to reduce Incident Response cost

- Badly calibrated filters
- Overinvestment
- Lack of diversity in data sources

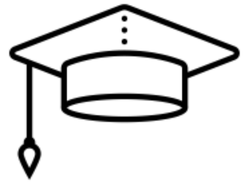
Threat Intelligence - Excercise



Your Threat Intelligence feed notifies you about a large cybercriminal operation with ransomware that has targeted suppliers and competitors of yours. Vulnerabilities used in the attack are present in your products.

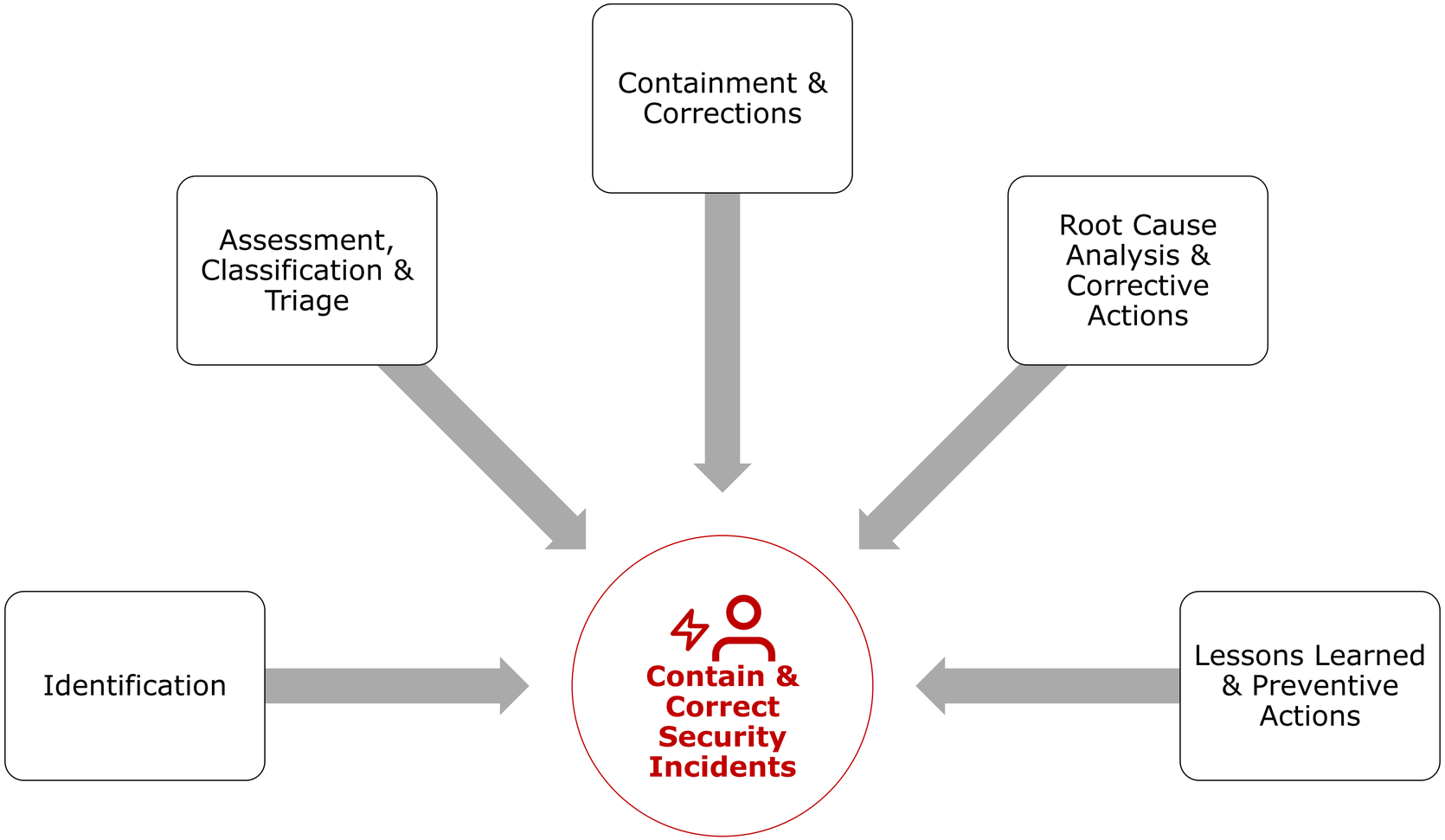
How to react?

Time to rest



10 Min Break

Incident Handling



Incident Handling – What to prepare

Incident Response Process & Plans

- Response Process, Roles & Responsibilities
- Incident Response Plans
- Regular Trainings / Excercises
- Communication Plans

Product / System Information

- Classification & Contacts
- Architecture & Components
- Usage & Customers
- Configuration Information

Response Tools & Infrastructure

- Ticket Handling System
- NDR / EDR
- Emergency Accounts / Comm. Channels
- Recovery Plans / Backups / Spare Devices

Incident Response Team

- Security Analysts
- Product / System Owners
- Technical Experts
- Customer Support / Marketing
- Communications / legal

Incident Handling - How to Execute

1. Identify, Classify & Triage → 2. Contain → 3. Correct → 4. Root Cause Analysis & Follow-up → 5. Lessons Learned

- Prepared contact lists
- Regular excercises
- Interfaces with suppliers & customers

- Escalating small incidents
- Compromised chain of custody
- Not learning the lesson

Crisis Handling

Crisis Definition

- Large scale incident or series of incidents that threatens the entire organization
- Response directly managed by Senior Executives
- Escalated based on defined criteria / triggers
- Unknown situations, no response plans exist

Prerequisites

- Defined Process, Triggers, Roles & Responsibilities
- Crisis Team
- Prepared Templates
  - Crisis Log
  - Action Plan
  - Communication Plan & Statements

1. Identify Crisis → 2. Form Crisis Team → 3. Define Action & Comm. Plan → 4. Resolve Crisis → 5. Lessons Learned

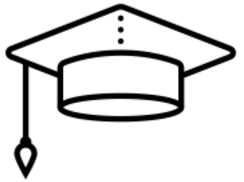
- Escalate directly
- Apply need-to-know principle
- Clear delegation of authority

- Unmanaged panic
- Involving too many people
- Deviating from the plans

Comparison Incident / Crisis

	Incident	Crisis
Scenario	• Unexpected or expected individual issue • Potentially recurring	• Unexpected event or series of events • First-time occurrence
Impact	• low > high severity • Temporary damage • Fast recovery	• critical severity • Permanent damage • Slow recovery
Scope	• Individual Customer(s) / Product(s) / System(s) affected • Impact affects only a part of the organization	• Many customers / products / systems / product lines affected • Impact affects the entire organization
Response Team	• Product Management • Specialists	• Senior Executives • Heads of Organizations • Experts

Quiz



Attackers have compromised a developer laptop with production signing keys for the firmware of your smart door lock solution.
The public key that verifies the signature in the lock is programmed in OTP memory, the lock has been sold 500.000 times to companies of all sizes and to individuals.

1. Is this an incident or a crisis?

a) An incident, because it only affects one product

b) An incident, because one information asset was stolen

c) A crisis, because critical customers will be annoyed

d) A crisis, because of the potential impact and lack of response plan

2. Which of the following actions to take first?

a) Inform affected customers

b) Exchange the production signing keys

c) Understand the impact

d) Set up an action log

3. Which of the following measures will not help to prevent reoccurrence?

a) Implementing multiple signing keys and enabling key switching via firmware update

b) Using an HSM for key generation & storage

c) Providing updated door locks with new signing keys

d) Training developers in credential handling

Secure End of Life

End of Security Support

- Usually after end of sales
- Date planned from Production Start
- Announced through
  - End of Life websites (e.g. Microsoft)
  - Contractual agreements
  - OpenEoX
- Mandated by newer standards (e.g. ISO21434)
- Minimum support period upcoming (EU CRA)

Secure Data Migration

- Enable customers to transfer their data to a newer product
- Provide upgrade path based on your own successor products
- Enable signed and encrypted transfers, e.g. via inbuilt features

Secure Wiping / Destruction

- EoL proructs may contain sensitive data
- Avoid customer returns that may include sensitive data
- Instead, offer secure wiping on site and done by the customers (inbuilt functionality)
- Ensure secure physical destruction of products (included storage devices) with customer files (e.g. DIN 66399 E5 / H5)

Secure End of Life – Clean finish for the Product Lifecycle

Secure End of Life

- Clear End of Life / End of Security Support
- Secure Data Migration
- Secure Data Wiping

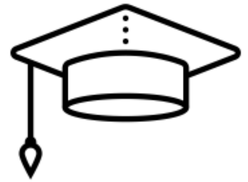
Prerequisites

- Defined Product Roadmap
- Channel to announce end of life
- Means for secure data migration
- Means for secure deletion

1. Announce EoL → 2. Stop Sales → 3. End Security Support → 4. Migrate data securely → 5. Wipe data securely

- Clear, public, early announcement
- Provide successor / target for migration
- Test secure migration / wipe before EoL

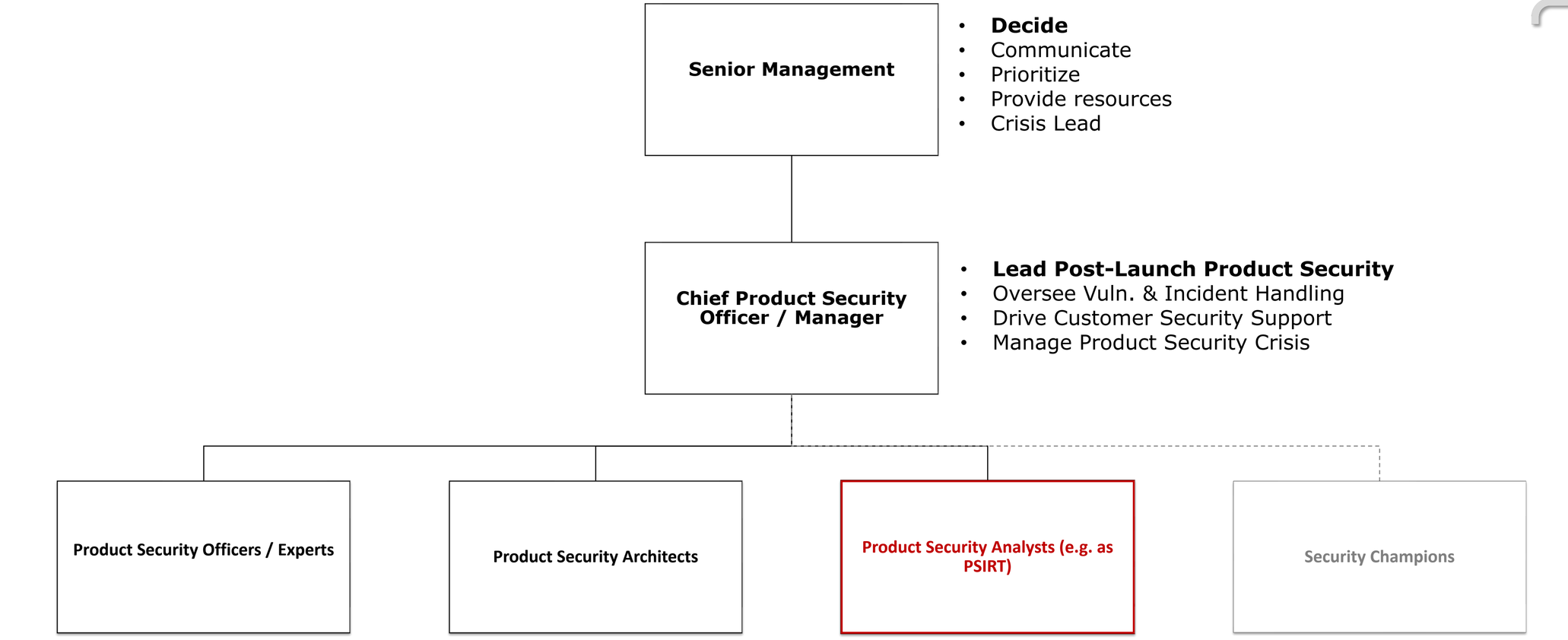
- Eternal products
- Lack of upgrade path
- Taking back systems with customer data



Who?

Post Launch Security Organization

Product Security Organization – Post-Launch Responsibilities



- **Decide**
- Communicate
- Prioritize
- Provide resources
- Crisis Lead

- **Lead Post-Launch Product Security**
- Oversee Vuln. & Incident Handling
- Drive Customer Security Support
- Manage Product Security Crisis

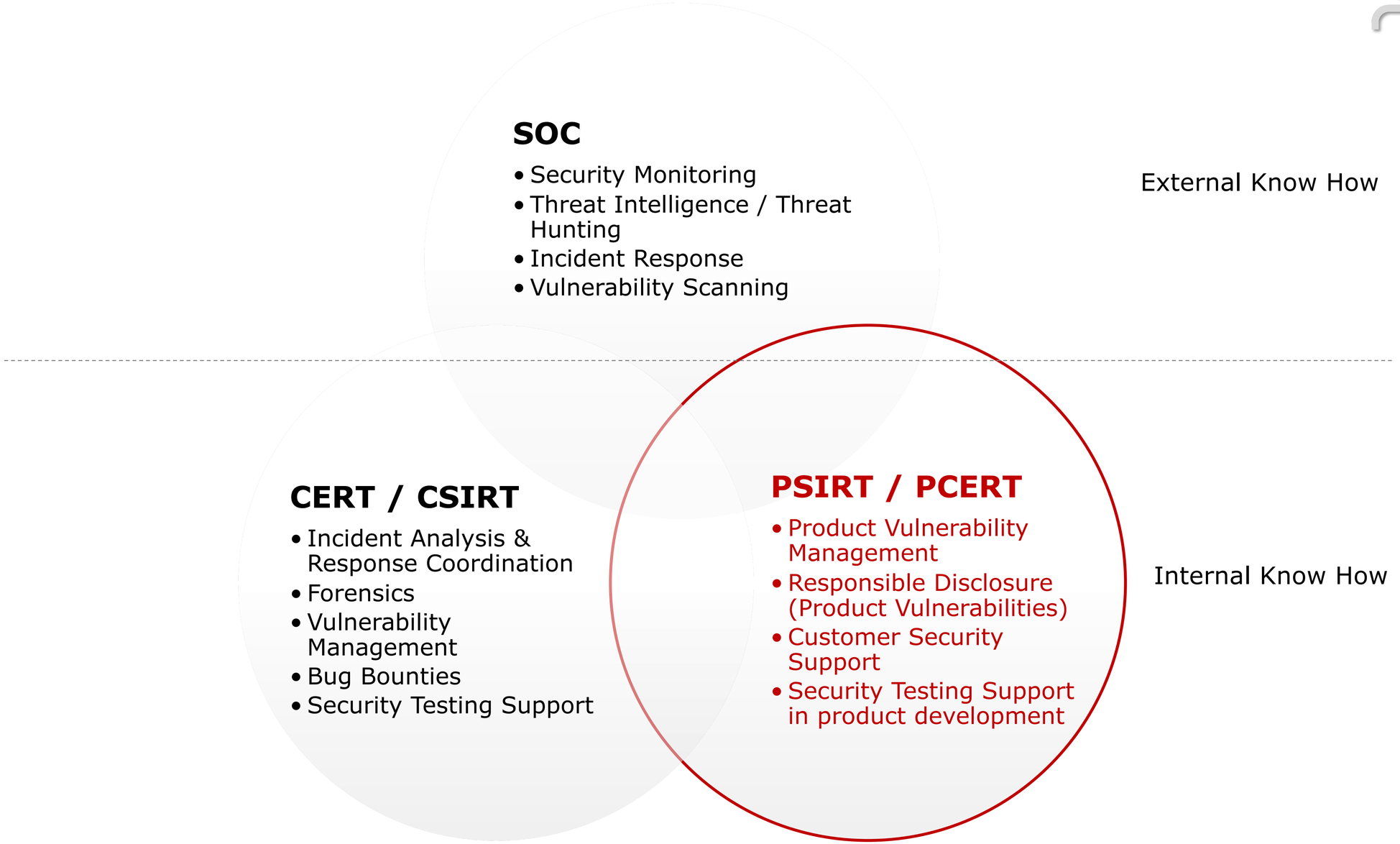
- Security Risk Assessments
- Support Patch Development
- Maintain Documentation
- Customer Security Requirements

- Support issue analysis
- Support vulnerability resolution / patch development

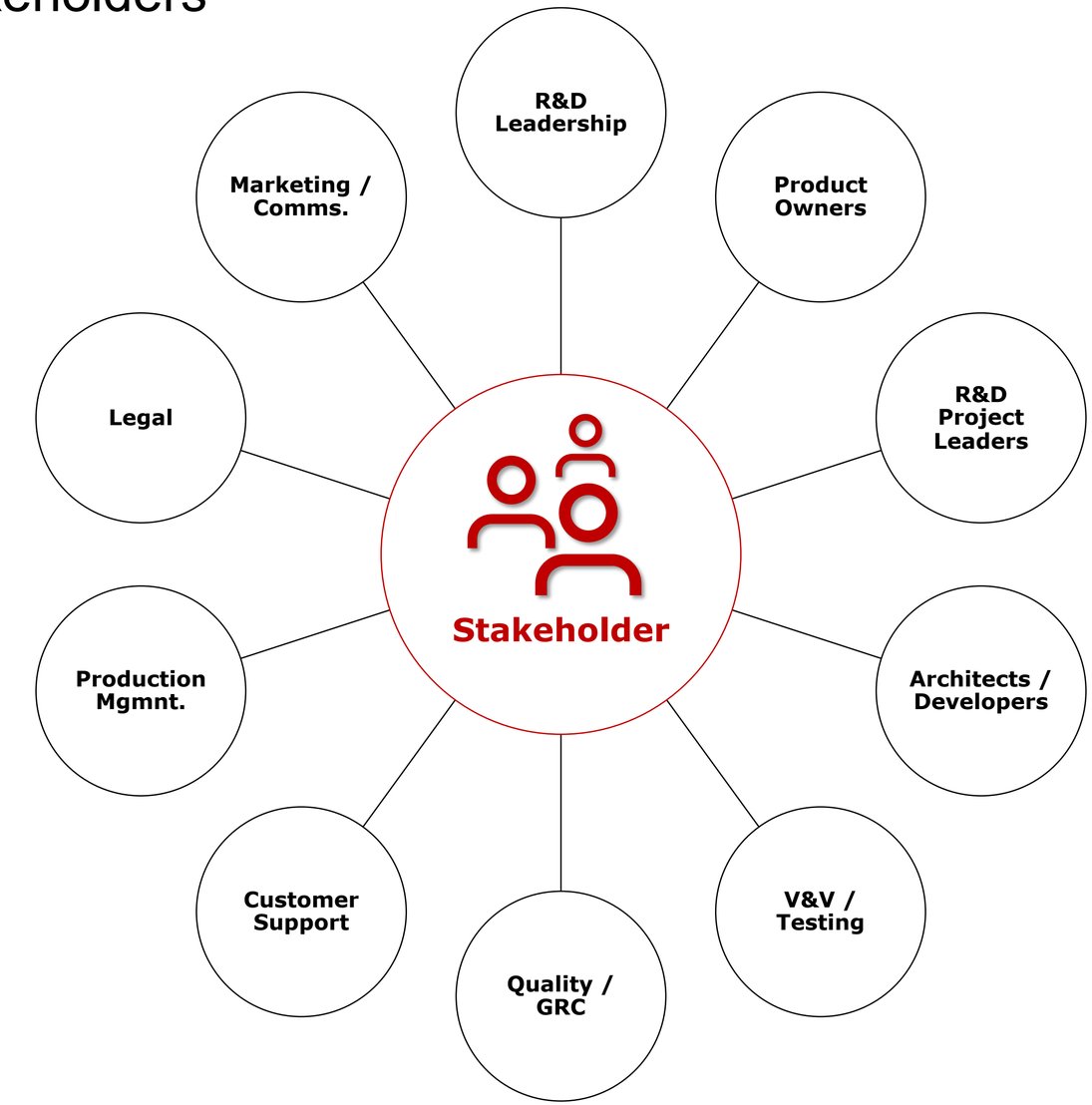
- **Vulnerability & Incident Handling**
- Vulnerability Monitoring / Threat Intelligence
- Responsible Disclosure
- Information Sharing
- Customer Sec. Support
- Security Testing

- Identify and raise security issues
- Support Patch development

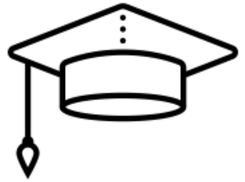
Operative Security Teams - comparison



Post Launch Security Stakeholders



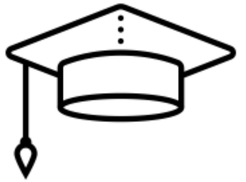
Post Launch Security Organization - Exercise



Should a PSIRT be set up centrally or as a decentral / virtual team?

Find arguments for both sides

Time for questions



Contact Details

Alex Diekmann

e-Mail: alexander.diekmann@hslu.ch

Threema: 7SBWM9V7

LinkedIn: https://www.linkedin.com/in/alexdiekmann/