Security Know-How als Erfolgsfaktor

LIMES
SECURITY

Case Studies seit 2022

Case Study #1

AUFBAU JUNIOR-ROLLEN MIT CYBERSECURITY-BEZUG

Ausbildung von expliziten „New Hires“ für 10 benötigte Rollen

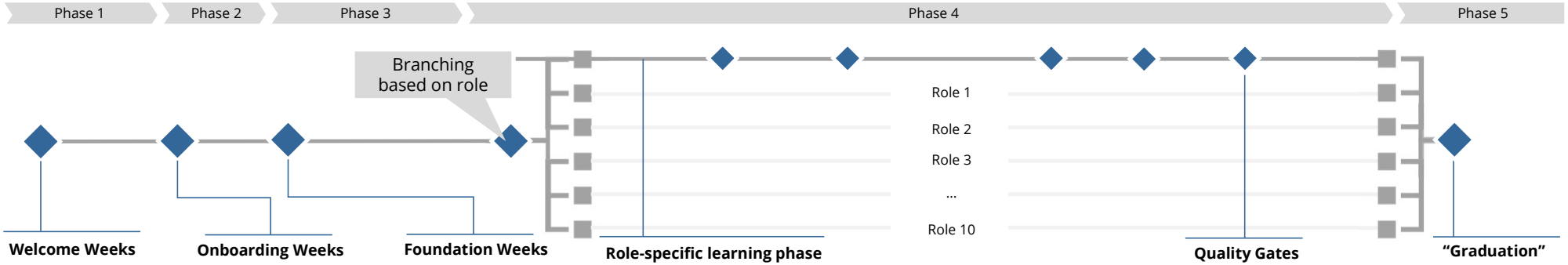
- DevSecOps, Cloud Security Engineer, Secure Solution Architect, …
- 1 Jahr Ausbildungsprogramm mit Vollanstellung (38h)
- Unterschiedliches Ausbildungsniveau und Vorwissen
- Zukünftige Dauer: 6 Monate

Modulares Training für Cybersecurity Expertenrollen in einem industriellen Produktionskonzern

Ausbildung von Cybersecurity Führungsrollen in einem internationalen Konzern

Effizienz durch rollenspezifische Lernpfade

Program duration: 10-12 Months



- Duration: 3 weeks
- Welcome of group
- Team-building
- First introductory content
- Matching with mentors

- Duration: 2 weeks
- Virtual
- Together with all new hires
- Focus on learning
- Broad overview about organization
- Organization-specific security basics

- Duration: 7 weeks including 1 week of Christmas break
- Mostly virtual
- Together with all new hires
- Broad security foundation
- Includes hands-on work assignments

Duration depends on individual situation & pre-knowledge of participant

Recommended weekly schedule with content list with assignments, milestones and checkpoints - but participants can make own decisions

Mix of formats used:
- Mandatory elements
- Online Trainings (self-paced)
- In-person trainings (book in advance, date can be selected)
- Practical work assignments (max. 45% of time)
- Coffee chats with colleagues (weekly)
- Monthly expert presentation & Q&A (e.g. 1h Teams live events)
- Personal mentor / 1:1 coaching (via Teams)
- Best Practices Podcast (bi-weekly)
- Insight newsletter (weekly)
- On-site events
- Supporting measures
- Weekly reminder e-mails
- Communication via management

Defined mandatory requirement to complete a phase

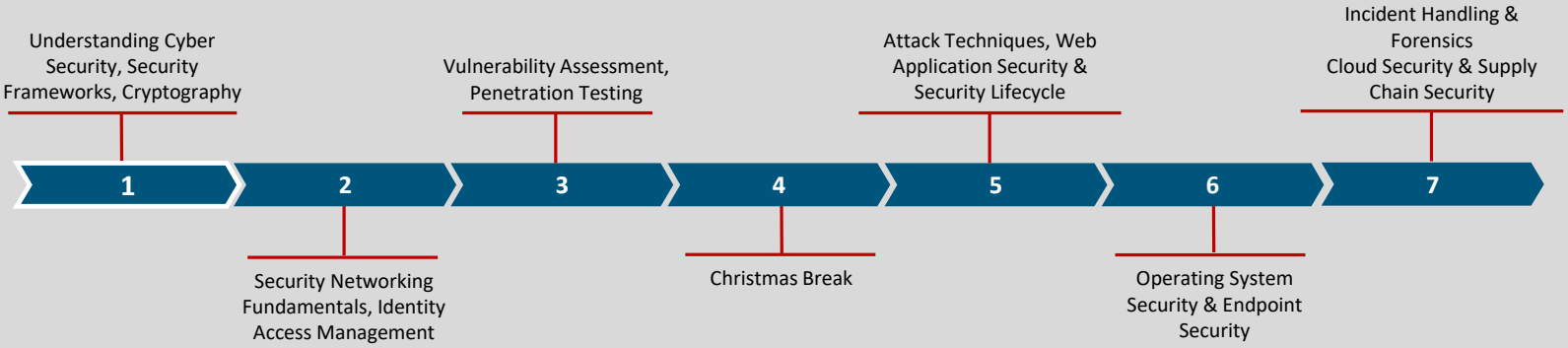
Example:
- Online training xx finished
- Live training xx finished
- Participation in at least 3 analysis
- >3 coaching sessions with risk expert

- Certificate of completion of programm
- Celebratory event

Klare Strukturen und abwechslungsreicher Medienmix

LIMES SECURITY

Example Focus Topic Weeks For Foundation Week (Phase 3)



Example weekly structure for week 1:

	Monday	Tuesday	Wednesday	Thursday	Friday
Introduction • Introduction email with weekly content • **Quality gates and milestones**	**Start of week email**				**Weekly Insights Email**
Content • Online content and activities • **Knowledge transfer and practical activities**	**Learning content** Online or in-person	**Learning content** Online or in-person	**Learning content** Online or in-person	**Learning content** Online or in-person	**Learning content** Online or in-person
Exercises & work assignments • Hands-on experience • **New skills are practised**		**Work assignment** ("on the job")	**Exercises and use cases**		
Groupwork & discussions • **Community building with colleagues**			**Coffee chats**	**Group discussion and retro**	
Tutoring • **Online learning with an mentor and topic expert**		**Mentoring 1:1**			**Live Event with an Expert**

Exemplarischer Stundenplan für “Foundation Weeks”

Um den Einstieg in das Trainingsprogramm möglichst einfach zu gestalten wurden für die ersten 7 Wochen “Stundenpläne” entworfen, die als Vorschlag an die Teilnehmer übermittelt wurden. Gelbe Blöcke sind fix eingeplante Live-Events. Alle anderen Blöcke können beliebig verteilt werden.

<table>
<tr><th>Time (CET)</th><th>Monday</th><th>Tuesday</th><th>Wednesday</th><th>Thursday</th><th>Friday</th></tr>
<tr><td>09:00</td><td rowspan="2">Flex time</td><td rowspan="4">Security Testing Essential Training (3h)</td><td rowspan="3">Penetration Testing Essential Training (2,5h)</td><td>OWASP Top 10 - Risks 6-10 (3h)</td><td rowspan="2">Endpoint Security Design and Implementation (1,5h)</td></tr>
<tr><td></td><td></td></tr>
<tr><td>10:00</td><td>Weekly Team Check-In</td><td>Group work web risks 1 (1h)</td></tr>
<tr><td>10:30</td><td rowspan="3">CompTIA Security+ (SY0-601) Cert Prep: 1 Threats, Attacks, and Vulnerabilities (2,5h)</td><td rowspan="2">Flex time</td><td rowspan="2">Learning SSL/TLS (2.5h)</td></tr>
<tr><td>11:00</td><td rowspan="2">HTTP Essential Training (1h)</td></tr>
<tr><td>11:30</td><td>Flex time</td></tr>
<tr><td>12:00</td><td>Flex Time</td><td rowspan="2">Lunch break</td><td rowspan="2">Lunch break</td><td rowspan="2">Lunch break</td></tr>
<tr><td>12:30</td><td rowspan="2">Lunch break</td></tr>
<tr><td>13:00</td><td rowspan="4">Penetration Testing, Incident Response and Forensics (week 1) (4h)</td><td rowspan="6">OWASP Top 10 - Welcome and Risks 1-5 (4,5h)</td></tr>
<tr><td>13:30</td><td>CompTIA Security+ (SY0-601) Cert Prep (cont'd) (2,5h)</td><td rowspan="2">OWASP Top 10 - Risks 6-10 (3h)</td><td>Lunch break</td></tr>
<tr><td>14:00</td><td rowspan="2">Cybersecurity Awareness: Malware Explained (1h)</td><td rowspan="3">Flex Time</td></tr>
<tr><td>14:30</td><td>Group work web risks 2 (1h)</td></tr>
<tr><td>15:00</td><td>Cybersecurity Awareness: Phishing Attacks (1h)</td><td>Learning VPN (1h)</td><td>Weekly Learning Report</td></tr>
<tr><td>15:30</td><td rowspan="3">Flex time</td><td>PKI Foundations (0,5h)</td><td rowspan="2">Weekly Q&A (1h)</td></tr>
<tr><td>16:00</td><td rowspan="2">Flex Time</td></tr>
<tr><td>16:30</td><td></td></tr>
<tr><td>17:00</td><td></td><td></td><td></td><td></td></tr>
<tr><td>17:30</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Detailplanung für “role-specific learning phase”

	Programm week	20	21	22	23	24	25
	Mo	27.03	03.04	10.04	17.04	24.04	01.05
Role							
Role 1	Topic	Docker Introduction	Vacation	Docker Introduction	DevSecOps Concepts	Web Application Security Fundamentals	Web Application Security Fundamentals
Role 2	Topic	Git Lab	Vacation	Cloud Security Essentials	Backup and Recovery	Linux Security and Hardening	Linux Security and Hardening
Role 3	Topic	Hack the Box Academy	Vacation	Hack the Box Academy	Hack the Box Academy	Hack the Box Academy	Hack the Box Academy
Role 4	Topic	IAM Refresher	Vacation	Ruby Essentials	Ruby Essentials	Linux Security and Hardening	Linux Security and Hardening
Role 5	Topic	AWS Educate	Vacation	IAM and OU policies	IAM and OU policies	Cloud Network Configuration	Cloud Network Configuration
Role 6	Topic	AWS Educate	Vacation	IAM and OU policies	IAM and OU policies	Cloud Network Configuration	Cloud Network Configuration
Role 7	Topic	Secure Software Development Principles & Basics	Vacation	Secure Software Development Principles & Basics	DevSecOps Concepts	Web Application Security Fundamentals	Web Application Security Fundamentals
Role 8	Topic	Power BI for data analysts	Vacation	Power BI for data analysts	Power BI for data analysts	Power BI for data analysts	Power BI for data analysts
Role 9	Topic	Solution Architect	Vacation	Enterprise Architect	Enterprise Architect	Enterprise Architect	Enterprise Architect
Role 10	Topic	Information Security Policies	Vacation	Information Security Policies	Risk Management Deep Dive	Risk Management Deep Dive	Contracts

Detailplanung für “role-specific learning phase”

	Programm week	20	21	22	23	24	25
	Mo	27.03	03.04	10.04	17.04	24.04	01.05
Role							
Role 1	Topic	Docker Introduction	Vacation	Docker Introduction	DevSecOps Concepts	Web Application Security Fundamentals	Web Application Security Fundamentals

	Programm week	20	21	22	23	24	25	26	27	28
	Mo	27.03	03.04	10.04	17.04	24.04	01.05	08.05	15.05	22.05
Role										
DEF DevOps	Topic	Docker Introduction	Vacation	Docker Introduction	DevSecOps Concepts	Web Application Security Fundamentals	Web Application Security Fundamentals	DevOps	DevOps	Live Event Munich
	Content (reference to Mosse institute unless indicated)			In General: https://training.play-with-docker.com/ recommended starting exercises - https://training.play-with-docker.com/ops-stage1/ - https://training.play-with-docker.com/dev-stage1/	https://platform.mosse-institute.com/#/education/library/devsecops MDSO-001: Introduction to DevSecOps - 4 exercises MDSO-002: Introduction to Continuous Integration (CI) and Continuous Delivery (CD) - 4 exercises	MDSO-101: Web Application Security Fundamentals - Part 1 - 5 exercises MDSO-102: Web Application Security Fundamentals - Part 2 - 5 exercises MDSO-103: Web Application Security Fundamentals - Part 3 - 4 exercises	MDSO-101: Web Application Security Fundamentals - Part 1 - 5 exercises MDSO-102: Web Application Security Fundamentals - Part 2 - 5 exercises MDSO-103: Web Application Security Fundamentals - Part 3 - 4 exercises	MDSO-201: DevOps with Jenkins - 11 exercises	MDSO-201: DevOps with Jenkins - 11 exercises	
					▪ Research about DevSecOps and explain the benefits of using it over traditional practices ▪ Research the different ways of implementing security in DevOps ▪ Identify the Key Security Metrics in DevSecOps ▪ Explain the differences between AppSec and DevSecOps ▪ Research about the basic concepts in CI/CD ▪ Research about the relationship between CI/CD and DevSecOps ▪ Explain what 'Value Stream Mapping' is and it's benefits when applied to DevSecOps ▪ Research about the various software deployment strategies available	▪ Write a web application that automatically logs out users after 5 minutes of inactivity ▪ Write a web application that detects and safely handles crashes and exceptions ▪ Write a web application that prevents clickjacking ▪ Write a web application that correctly utilises the HTTP Only Cookie flag ▪ Write a web application that correctly utilises the Secure Cookie flag ▪ Write a web application that enforces a strong password policy and displays a password strength meter ▪ Write a web application that detects and blocks brute force attacks ▪ Write a web application that blocks cross-site request forgery ▪ Write a web application that logs account events and displays them to users ▪ Write a web application that validates URL redirection parameters ▪ Write a web application that prevents session fixation ▪ Write a web application that uses Prepared Statements to prevent SQL injection ▪ Write a web application that detects and blocks automated input submission tools ▪ Write a web application that provides a secure login form	▪ Write a web application that automatically logs out users after 5 minutes of inactivity ▪ Write a web application that detects and safely handles crashes and exceptions ▪ Write a web application that prevents clickjacking ▪ Write a web application that correctly utilises the HTTP Only Cookie flag ▪ Write a web application that correctly utilises the Secure Cookie flag ▪ Write a web application that enforces a strong password policy and displays a password strength meter ▪ Write a web application that detects and blocks brute force attacks ▪ Write a web application that blocks cross-site request forgery ▪ Write a web application that logs account events and displays them to users ▪ Write a web application that validates URL redirection parameters ▪ Write a web application that prevents session fixation ▪ Write a web application that uses Prepared Statements to prevent SQL injection ▪ Write a web application that detects and blocks automated input submission tools ▪ Write a web application that provides a secure login form	▪ Set up Jenkins in a Docker container ▪ Create a freestyle project in Jenkins to build a Java-based Application ▪ Create a Jenkins Pipeline to push a Docker Image to your Docker Hub repository ▪ Create a pipeline in Jenkins to deploy your custom web application on a local Kubernetes cluster ▪ Configure a reverse proxy for your Jenkins installation using Nginx ▪ Implement Project-based Matrix Authorization Strategy in Jenkins to manage access to projects ▪ Configure Role-based authorization in Jenkins to manage access to projects ▪ Configure your standalone Jenkins installation to take regular backups ▪ Configure your Jenkins-on-Docker installation to take regular backups ▪ Create a custom Docker image for Jenkins ▪ Perform user activity monitoring on your Jenkins installation	▪ Set up Jenkins in a Docker container ▪ Create a freestyle project in Jenkins to build a Java-based Application ▪ Create a Jenkins Pipeline to push a Docker Image to your Docker Hub repository ▪ Create a pipeline in Jenkins to deploy your custom web application on a local Kubernetes cluster ▪ Configure a reverse proxy for your Jenkins installation using Nginx ▪ Implement Project-based Matrix Authorization Strategy in Jenkins to manage access to projects ▪ Configure Role-based authorization in Jenkins to manage access to projects ▪ Configure your standalone Jenkins installation to take regular backups ▪ Configure your Jenkins-on-Docker installation to take regular backups ▪ Create a custom Docker image for Jenkins ▪ Perform user activity monitoring on your Jenkins installation	

Case Study #2

Aufbau Junior-Rollen mit Cybersecurity-Bezug für einen multinationalen Mischkonzern

CYBERSECURITY EXPERTENROLLEN

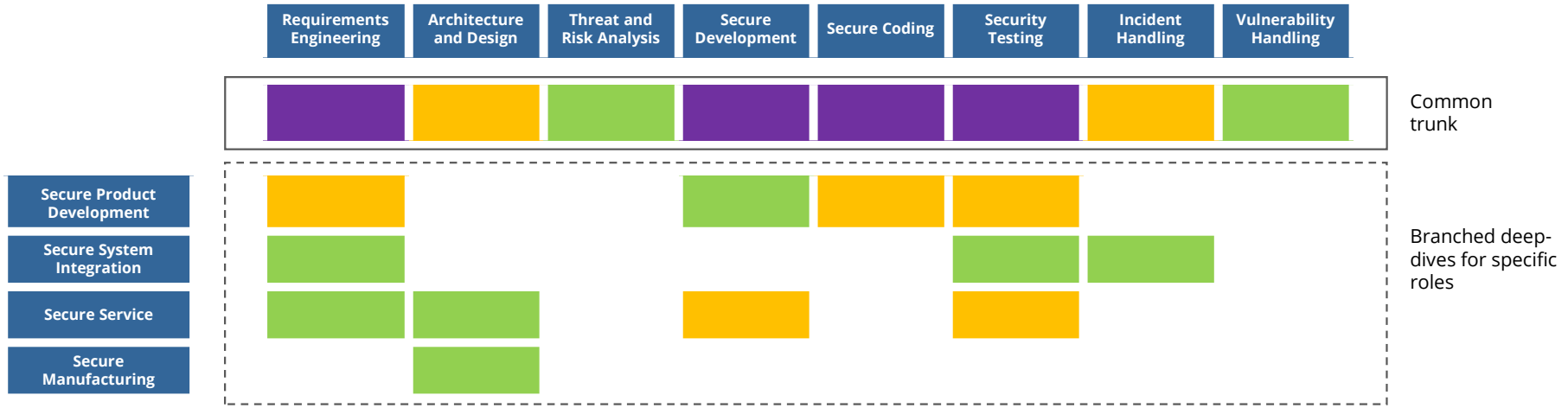
Weiterbildung bestehender Mitarbeiter zu Experten für Industrial Cybersecurity mit verschiedenen Fachbereichen

- Für Secure Product Development, Secure Manufacturing, Secure Integration und Secure Service
- Hohe Flexibilität gefordert aufgrund von Projektarbeiten
- Aufwand pro Woche maximal 2 Stunden
- Laufzeit über 1 Jahr

Ausbildung von Cybersecurity Führungsrollen in einem internationalen Konzern

Pilotierungsframework

Die Ergebnisse der Teilnehmerumfrage zeigten einen gemeinsamen Nenner. Bei Themen mit signifikant unterschiedlichen Rückmeldungen wurde der Lernpfad um Verzweigungen („Branching“) ergänzt.



Level 1: Know basics of a topic

Level 2: Participate in it and know about the process; maybe do a deep dive on occasion

Level 3: Own it/do it on a daily basis; be the expert in it; know how to use the tools

Formatmix für eine pragmatische Durchführung des Pilots

Für die Abhaltung des Pilots wird auf eine pragmatische Erstlösung zur Bereitstellung der Inhalte gesetzt. Hochwertige Produktionen werden erst nach einer erfolgreichen Pilotphase und ausführlichen Lessons-learnt angestrebt.

	Live Events			Self-paced			
	Expert presentations	Q&A sessions	Group work	Existing WBTs	Expert recorded webcasts	Converting wiki content to WBT	Use Wiki as repository
Customer role	Live presentation	Answer Q&A questions about topics covered recently	Moderate a group exercise or lead discussion after offline group exercise	Optional: Validate shortened/improved content	Speak to topic while presenting slides and record screen	Review WBT	n/a
Customer time investment	30-60 min live + 1-2 h preparation	30-60 min live + 15-30 min pre-reading of questions	30-60 min live + 30 min preparation call	30-60 min	30-60 min recording + 1-2 h preparation	30-60 min	n/a
Planned support activities	Optional: Content is proposed (or prepared) to shorten prep time	Questions are collected and provided upfront to the expert If the topic allows for it, the expert can also be provided	Group works are prepared Support with moderation If the topic allows for it, the expert can also be provided	Optional: Content is shortened or improved	Transfer recording into WBT (e.g. cut into 3-5min videos, add slides, ...) If the topic allows for it, the expert can also be provided	Convert Wiki content into simple WBTs for the pilot (slides, simple video with speaker, ...)	Provide resources to participants

Case Study #3

Aufbau Junior-Rollen mit Cybersecurity-Bezug für einen multinationalen Mischkonzern

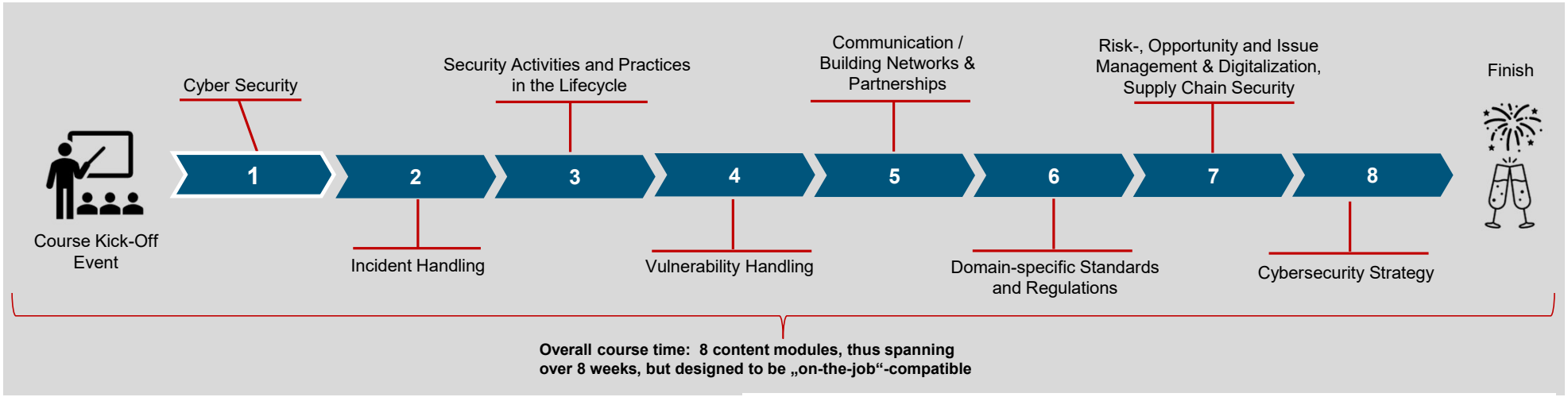
Modulares Training für Cybersecurity Expertenrollen in einem industriellen Produktionskonzern

CYBERSECURITY FÜHRUNGSROLLEN

Training von Cybesecurity Führungsrollen und verwandte Funktionen mit anspruchsvollen Aufgaben

- Lehrplan muss kompatibel mit engem Zeitplan der Teilnehmer sein
- Maximal 6 Stunden pro Woche
- Gesamtdauer 8 Wochen
- Zusätzlich zu flexiblen E-Learning-Inhalten muss der Community-Building-Aspekt bedient werden

Struktur und Outline



Weekly structure:

eLearning Content

- Time effort: 90-240 min. per module
- Aiming at developing:
  - General skillset
  - Company specifics

Live Remote Events

- Content-module specific live event, e.g. exercise, expert presentation with Q&A
- Time effort: ~90-120 min.

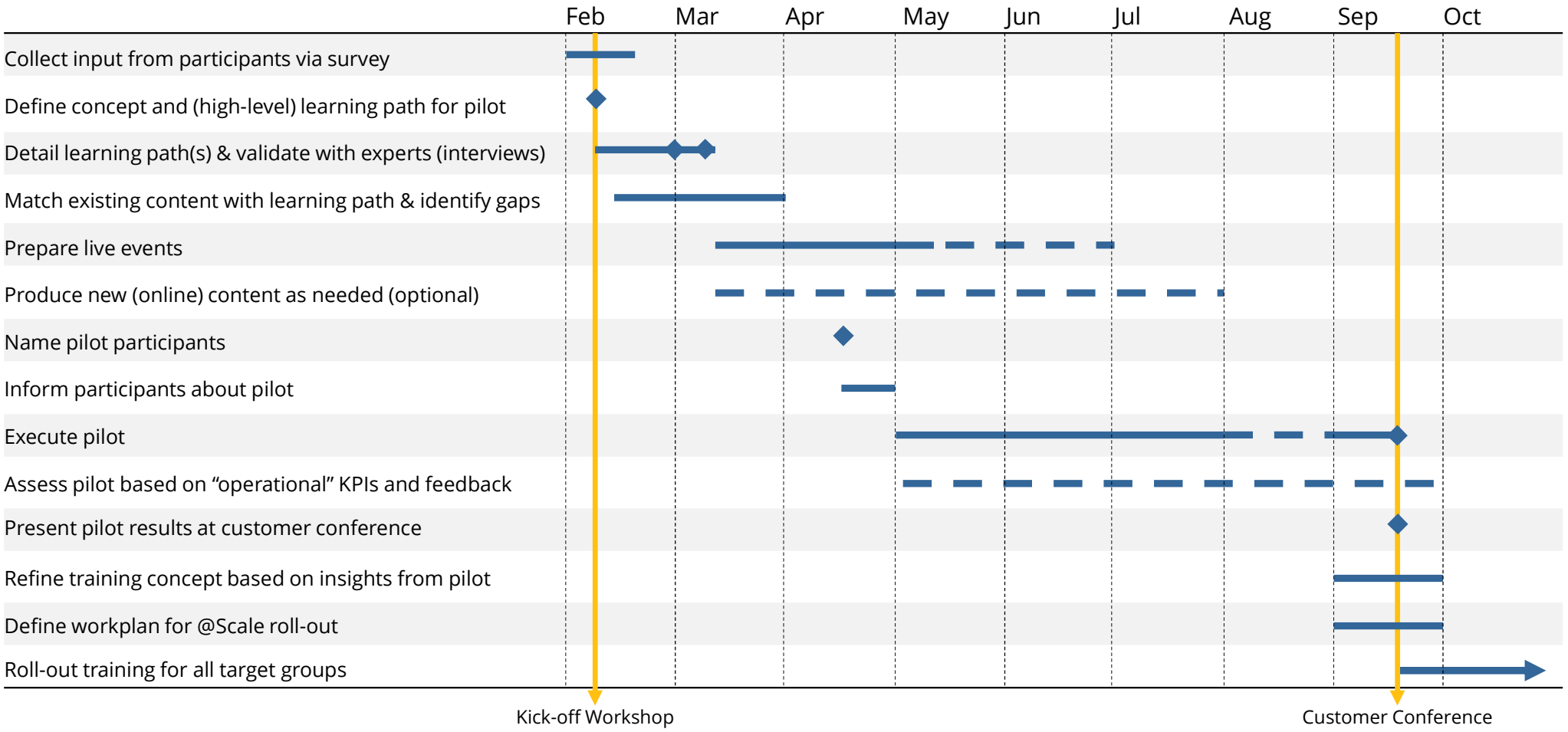
Monday	Tuesday	Wednesday	Thursday	Friday
eLearning content Online				
				Live Remote Check-in-Event with an Expert

Know-How als Erfolgsfaktor

Wenn das Ziel ist, den Fachkräftemangel zu lösen, sollte die Strategie sein, so vielen Personen wie möglich den (Berufs-)Einstieg und Umstieg in die Security zu ermöglichen.

- → Nicht nur Ausschau halten nach “einer Person mit dem passenden Profil”
- → Passende Profile für zukünftige Security-Aufgaben können in den unterschiedlichsten Personen gefunden werden

Projektaufbau für Pilotierung



Pilot Facts

8 week net program duration; no vacation weeks included

<6h net time investment per week
1 virtual live event per week (90-120 min); rest of the program is self-paced

Pilot size: **2x 10 participants**

Format: existing WBTs + live sessions via MS Teams + assignments

Experts from the customer will pose as speakers at live events for company-specific know-how

Aspirations:
- Curriculum areas are aligned with **role capabilities**
- Enable participants to perform future role
- Self-paced (online) learning whenever suitable
- Covering holistic cybersecurity aspects
- Use **pilot** as **proof-of-concept** & to learn for future roll-out

Bild: dpa