

Security Orchestration Automation Response (SOAR)

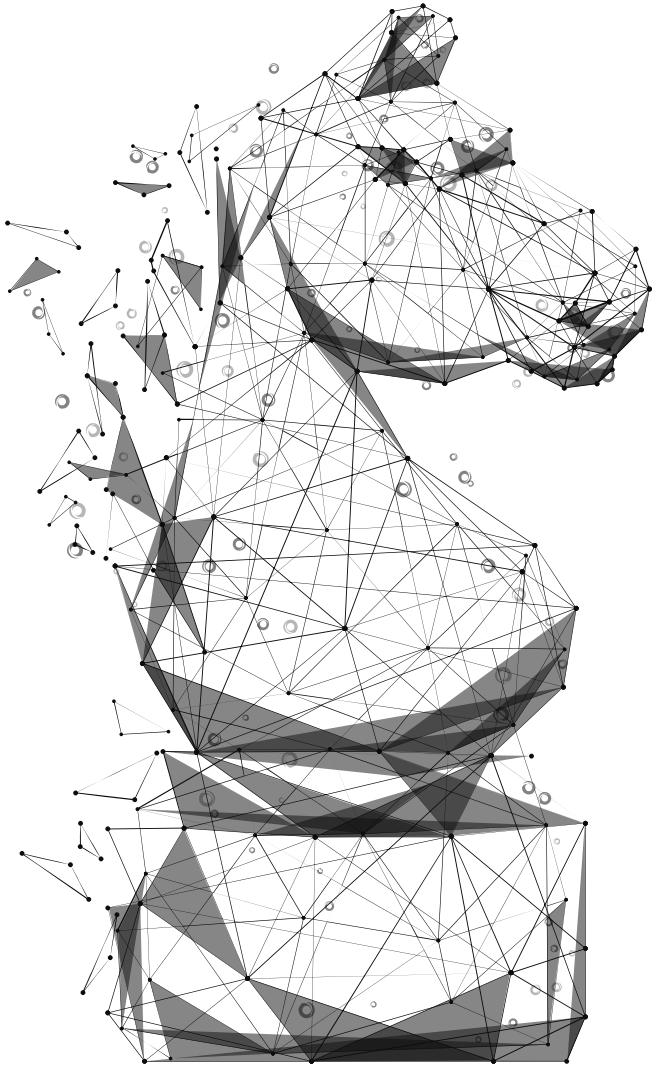
Einblicke, die Rolle in einem
modernen SOC & zukünftige
Perspektiven

27.06.2024
Manfred Nowara

 **accenture**



Agenda



- 00** Speaker profile
- 01** Today's challenges of a SOC
- 02** Addressing the challenges
- 03** SOAR architecture & functions
- 04** Summary & outlook
- 05** Case study

Speaker Profile

Passionate Security Enthusiast

Name Manfred Nowara

Education M.Sc. Business Informatics,
University of Regensburg

Job Accenture Detection & Response Lead DACH,
Senior Manager

Hobbies Hiking, Climbing, Mountainbiking, Motorcycling



Today's SOC Challenges

In addition to the usual operational challenges faced by the SOC—leaders must prepare to also take additional environmental complexities into account

Today's operational challenges of a SOC



Increase of day-to-day alerts



Lack of centralized context & documentation



Long onboarding and training time



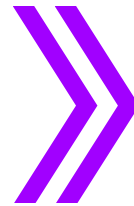
Lots of data with little security value



Increasing threat landscape



Demoralization



Added organizational complexity

Regulatory & Compliance



- Increasing number legislations to obey (e.g. MaRisk, DORA, NIS2, KRITIS, TISAX)
- Lacking transparency of enforcement

Financial



- Software licenses from added tools
- Lack of resources on market causes steady increase in loans to keep employees

IT Architecture



- Increasingly growing environment (Cloud, IoT, Container)
- Lack in documentation & inventory management (CMDB/Asset management database)

SOAR

Using a single platform and a combination of manual and automated tasks to help define, prioritize and standardize alert analysis, triage & incident response activities

Security Orchestration Automation & Response - SOAR



Orchestration & Automation

- **Machine driven interaction** of software & systems
- Contentious **coordination of workflows** – both automated & manual



Incident Response

- Integrating dispersed security data
- **Single collaboration** platform
- Defining & automating processes and workflows



Threat Intelligence Platform

- **Validate quality** of Threat Intelligence used
- **Distribution of validated TI** to tools & other security controls

Security & Organizational Prerequisites



Well defined set of incident response processes & playbooks



Asset inventory & configuration management database



Established security tools (e.g. SIEM, TI, IDS etc.)

Enables



Allow meaningful reaction and response on an automated basis, relieving human resources



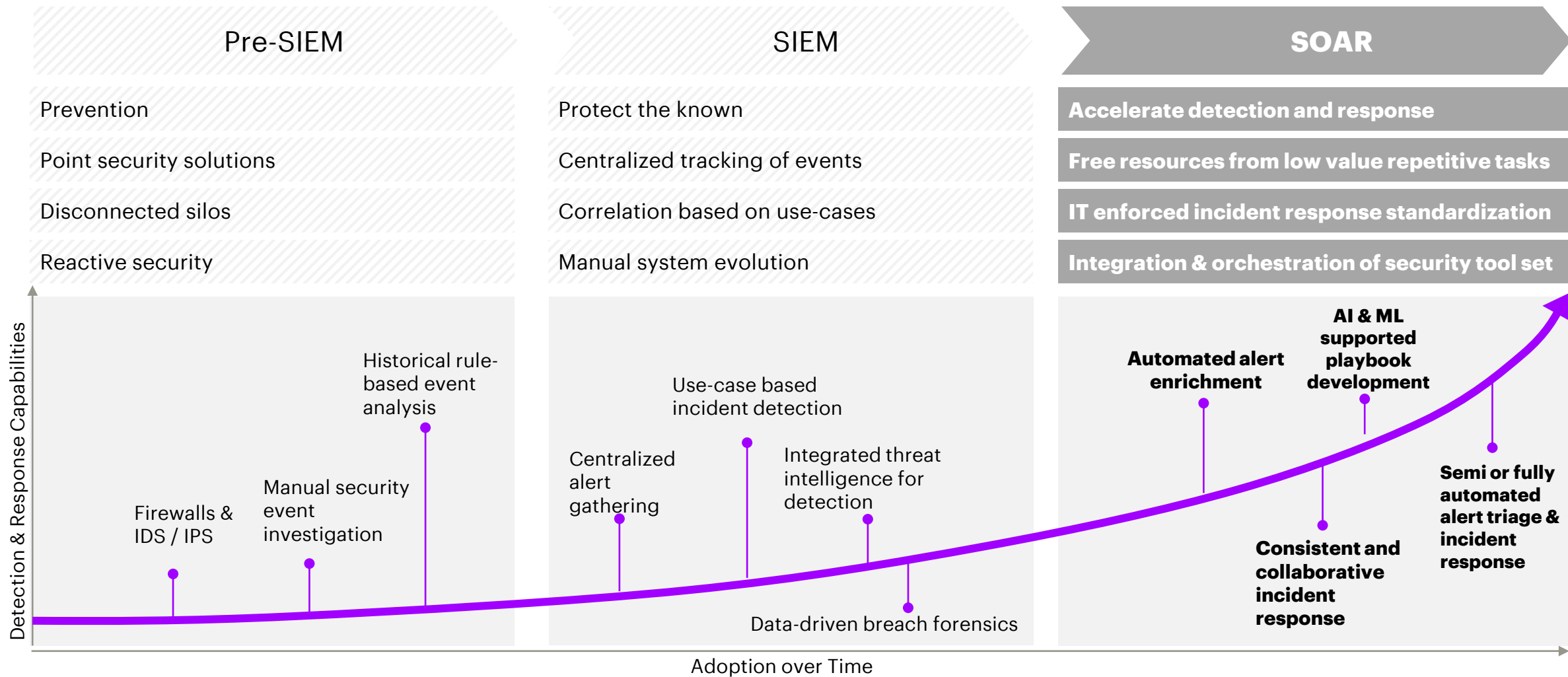
Bridge between human and machine power to **allow a more profound and a more telling security analysis**



Supports analysts **to define, prioritize and expand standardized incident response** activities

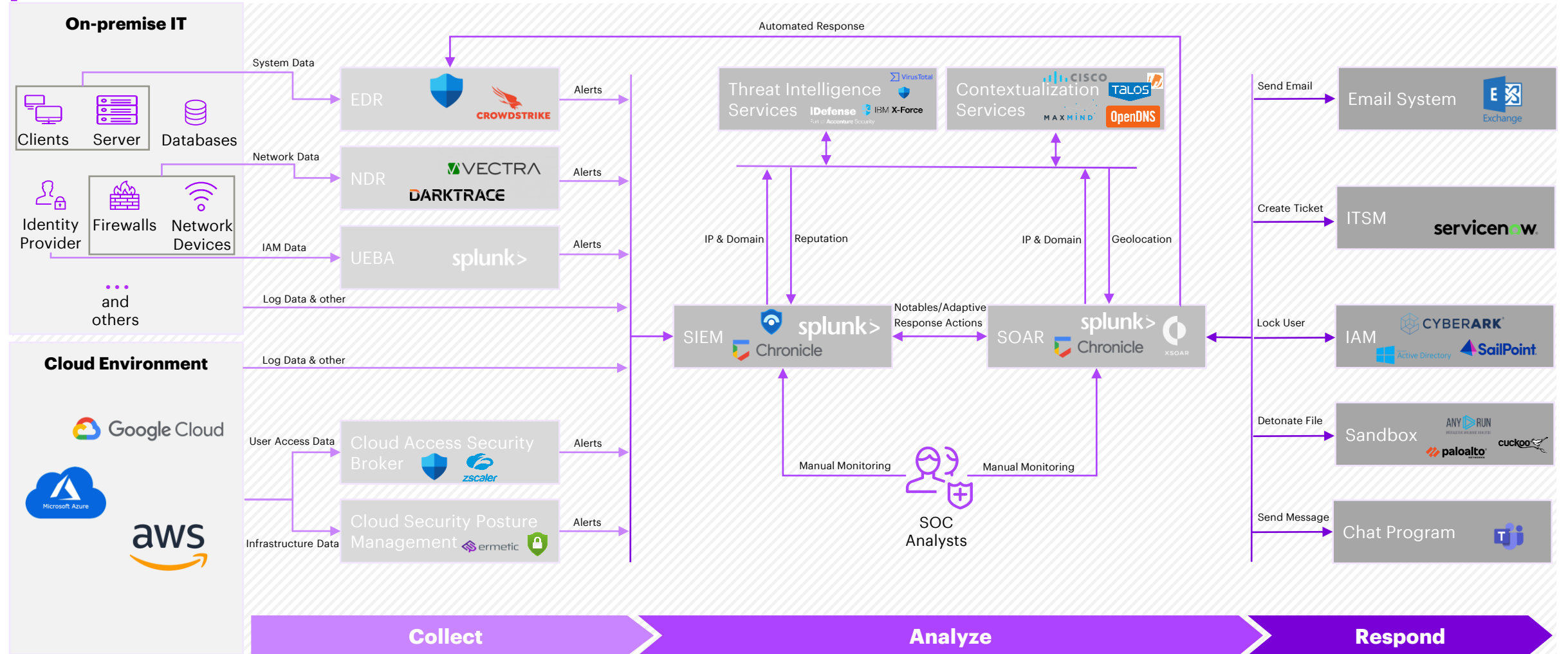
Where to embed SOAR in a SOC Journey

SIEM, TI, UEBA & IPS are tools that will help to detect and respond - being able to efficiently & intelligently orchestrate people, processes & tools is where SOAR comes into play



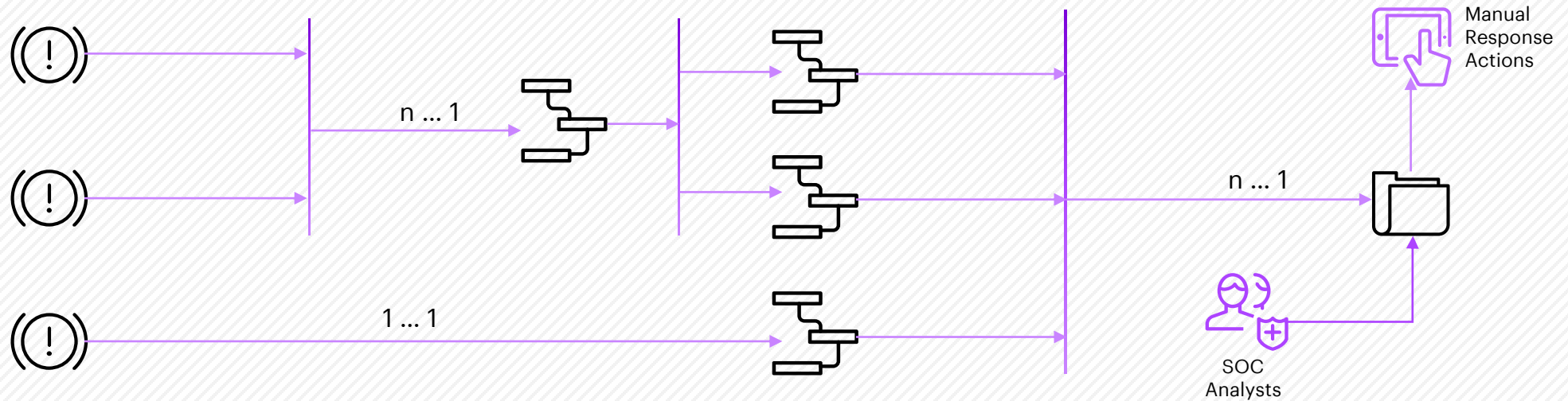
SOAR Technology Landscape Integration

SOAR sits at the heart of your SOC, only when fully integrated it will be able to live up to the promise



Alerts – Playbooks - Cases

Understanding correlation of those concepts is a vital part to the integration of SOAR into your Incident Management



Alerts

- Multiple Alerts arrive in SOAR, from SIEM, EDR, User Help Desk etc.
- SOAR correlates alerts into cases, based on assets, identities & other artefacts involved

Playbooks

- Automated / Partly Automated process of individual actions per alert
- Usually executed before manual interaction of the analyst with the case

Cases

- Collection of Alerts, Artefacts, Entities and other related information
- Collaboration space
- Directly initiate manual actions
- Historical progress view

SOAR Playbooks

Strategic deployment: The essence of SOAR playbooks

DEFINITION



- Structured **workflows** guiding security teams through procedures
- **Automation** or **semi-automation** for tasks
 - Incident trigger
 - Triage
 - Investigation
 - Response actions
 - Communication with external APIs, threat intelligence etc.

TYPES



- **Alert specific** playbooks
 - Customized for individual alerts/scenarios
- General **data enrichment / nested** playbooks
 - Gathering of additional context
 - For multiple alert types or as part of alert specific playbook

BENEFITS



- Reduces **manual** and **repetitive** tasks
- Saves **time** and **money** in the long run
- Supports **automated ingestion** of threat intelligence from various sources (integration of connectors)
- Enables more **efficient** actions against threats like malware or ransomware

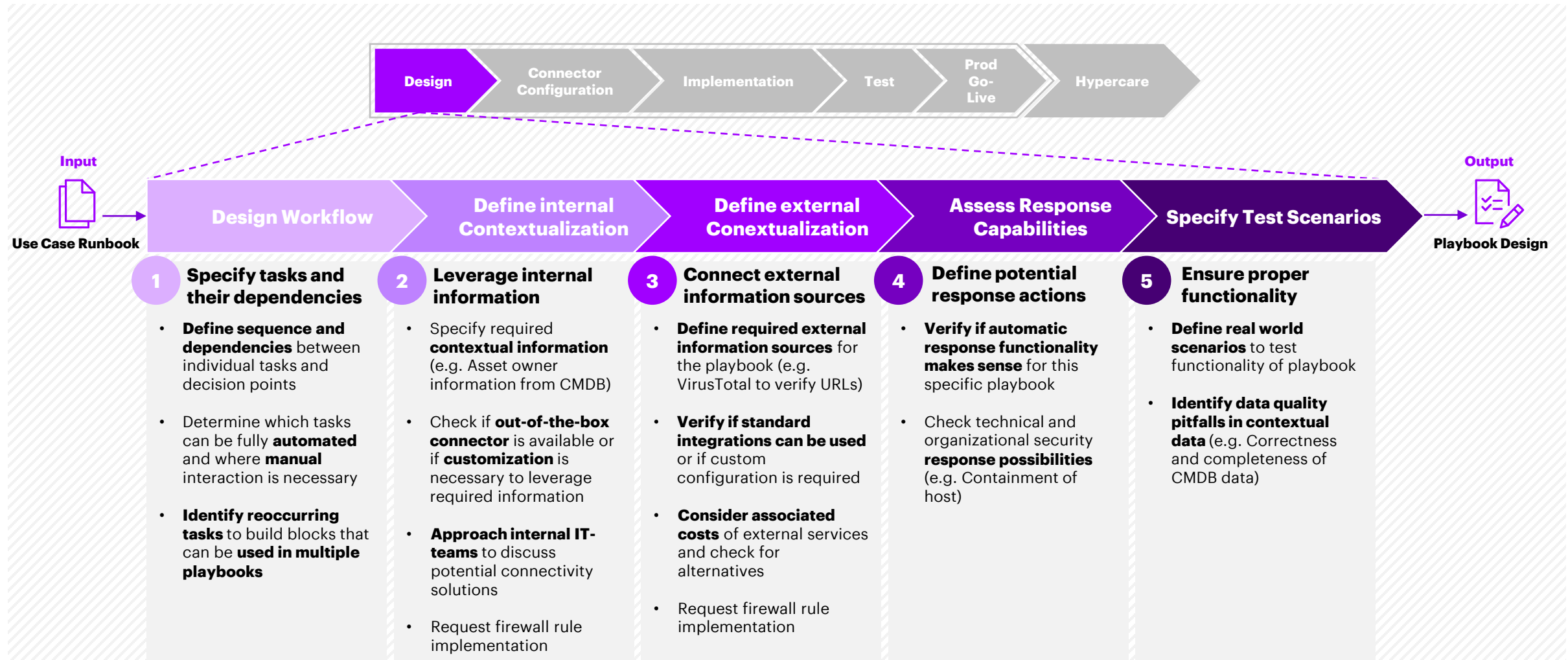
DEVELOPMENT



- Identify **key security procedures** and tasks
- Determine **automation** feasibility for each task
- **Design:** workflow definition, incorporating automated or semi-automated steps
- **Test** and **refine** the playbook
- Playbook **lifecycle** for adaptation

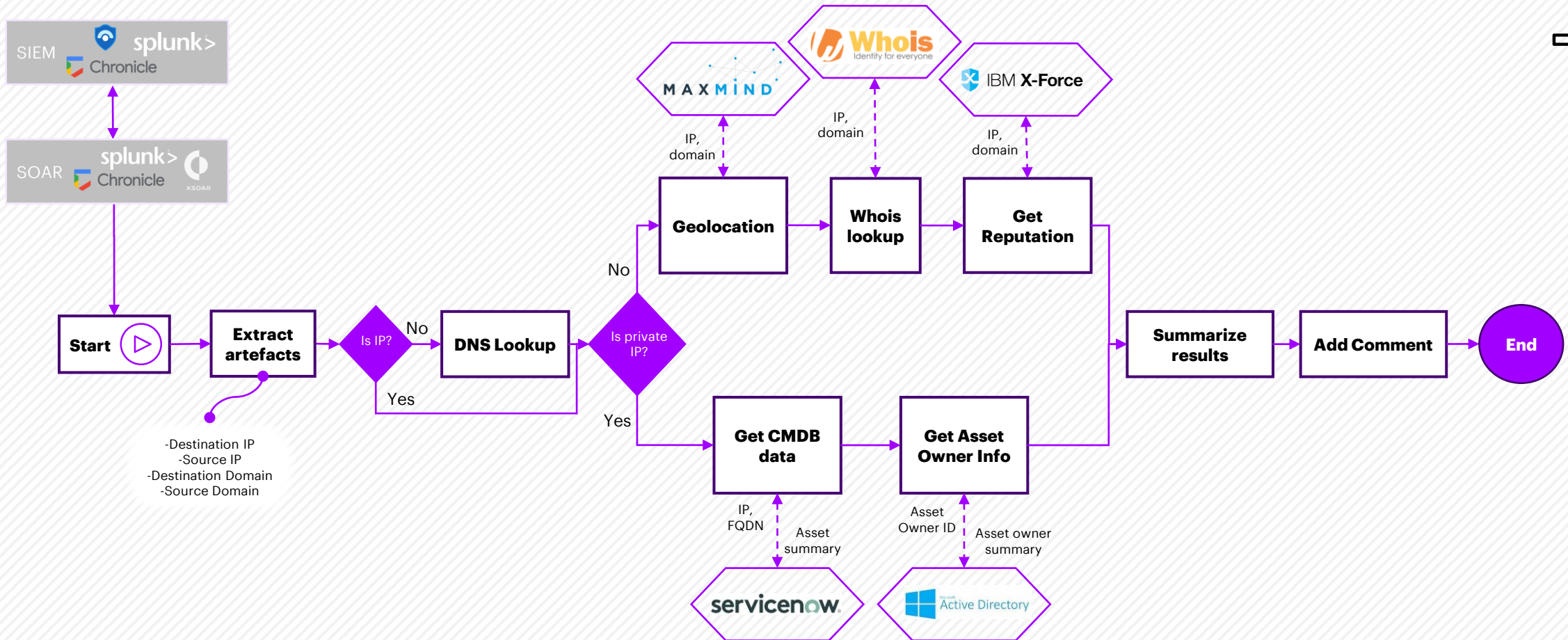
Playbook Development: Design-Phase

The design phase forms the basis for the entire development of the playbook



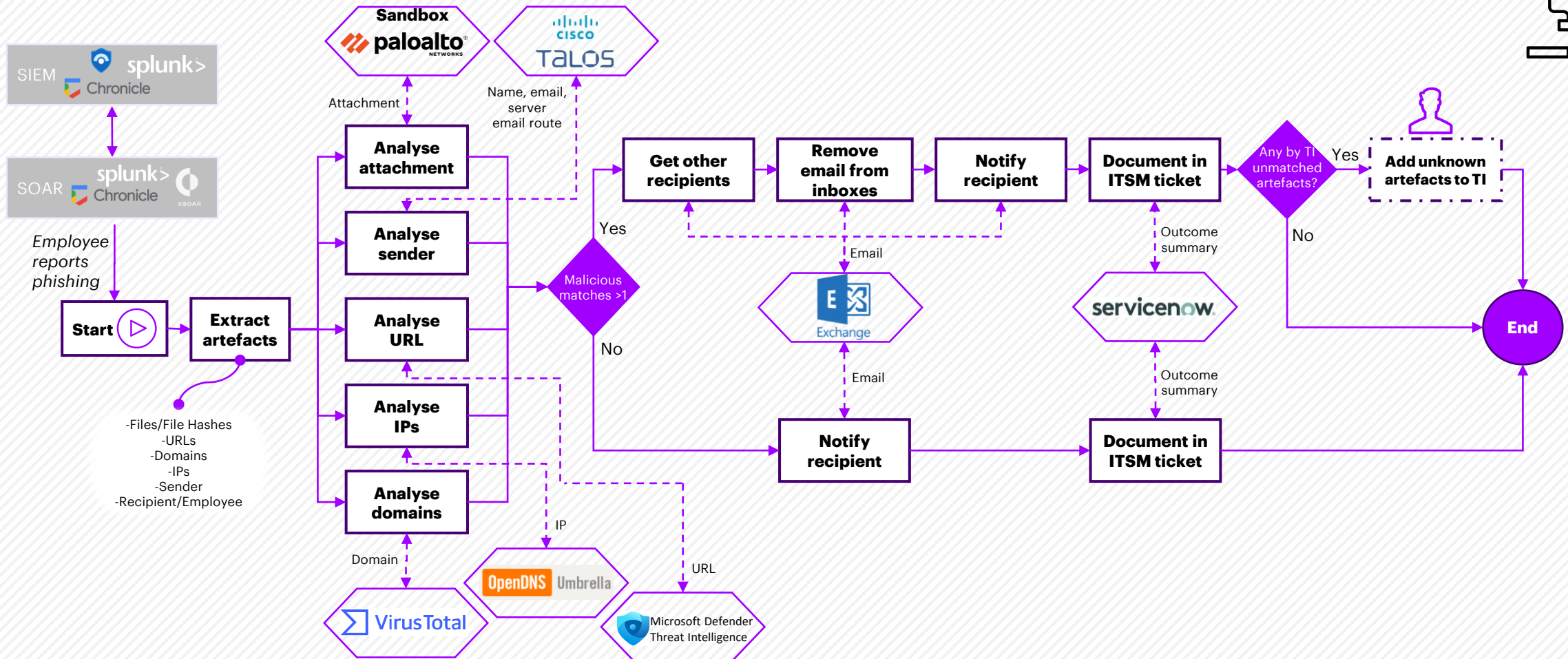
Example Playbook 1 / 2

Network Data Enrichment



Example Playbook 2 / 2

Phishing Investigation & Response



Drivers & Benefits for SOAR

SOAR addresses most of the challenges in today's SOC's enabling significant operational benefits around incident management & response, incident prioritization & cost structure

Challenges mitigated by SOAR

-  SOC staff shortages
-  Long mean time to respond
-  Lot of routine work
-  Alert triage quality issues
-  Long training time
-  Lack of ability to measure outcomes
-  Difficulties in establishing process control and KPIs



Quantified Benefits*



Inceased efficiency in incident resolution



Shorter response times



Opex savings by decomissioning legacy IR tools

Other Benefits*



Improved IT staff productivity by automatization








Improved visibility into security posture



Improved collaboration between IT and security

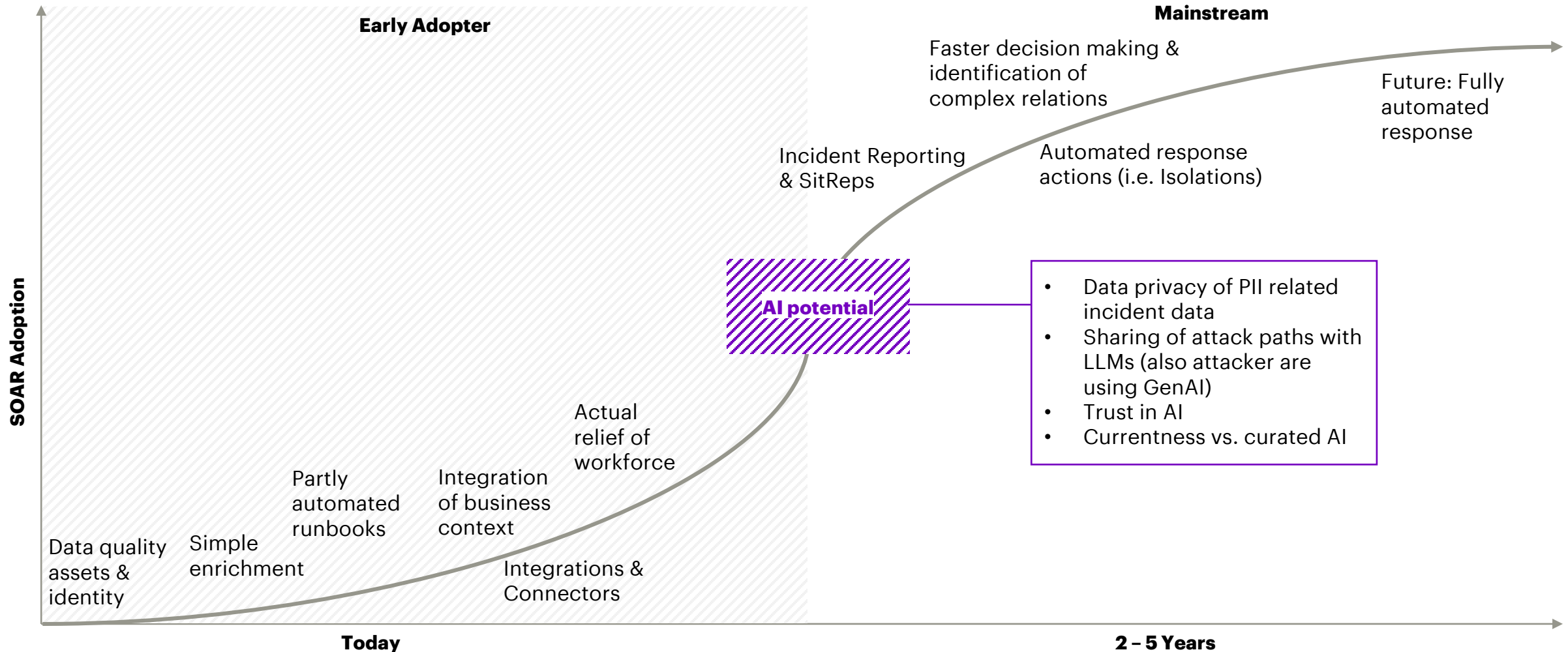
In Numbers*:

-  +40% in efficiency for L1
-  +60% in efficiency for L2
-  +70% in vulnerability identification & priotization
-  -30% in vulnerability response times
-  Up to 200.000 USD in savings from legacy IR tools

* Taken from: 2020 Forrester – The total economic impact of service now security operations
Copyright © 2024 Accenture. All rights reserved.

SOAR – A suggestion for an outlook

Increased pressure from the environment will boost SOAR adoption over the next years in nearly all industry segments – The degree in adoption can vary due to multiple factors



Case Study: One Year Splunk SOAR

Milestones and outlook

The SOAR Splunk journey started from scratch in August 2022. By August 2023, several milestones have been reached. Break-even will be reached in July 2025.

Achievements



6 Playbooks live in production and 5 connectors developed



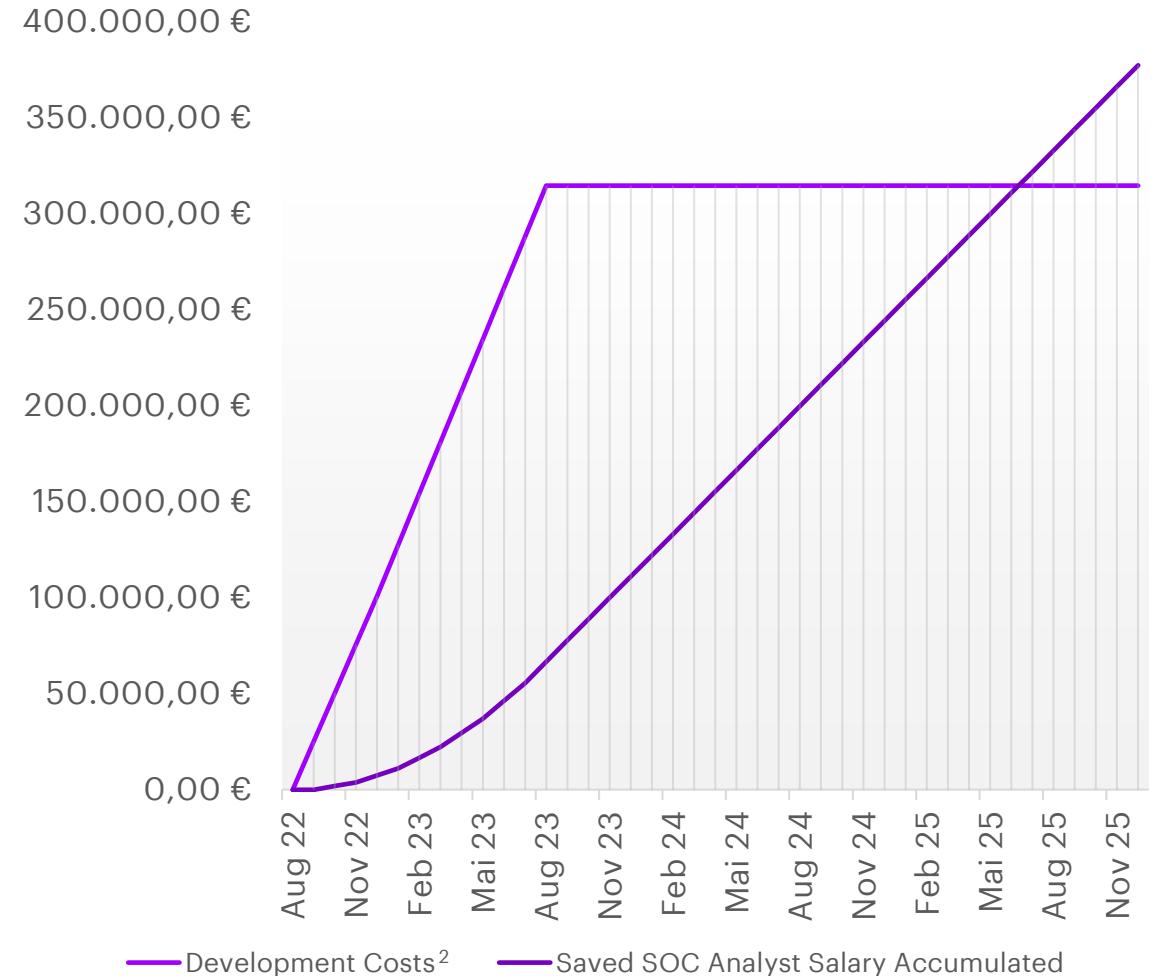
17,44 Minutes saved on average per alert



1,83 FTE saved each month since August 2023



11.090,24€¹ savings in SOC Analyst salary per month since August 2023



¹ Assumption: SOC Analyst salary 72.756,00€

² SOAR license cost not included



Thank You