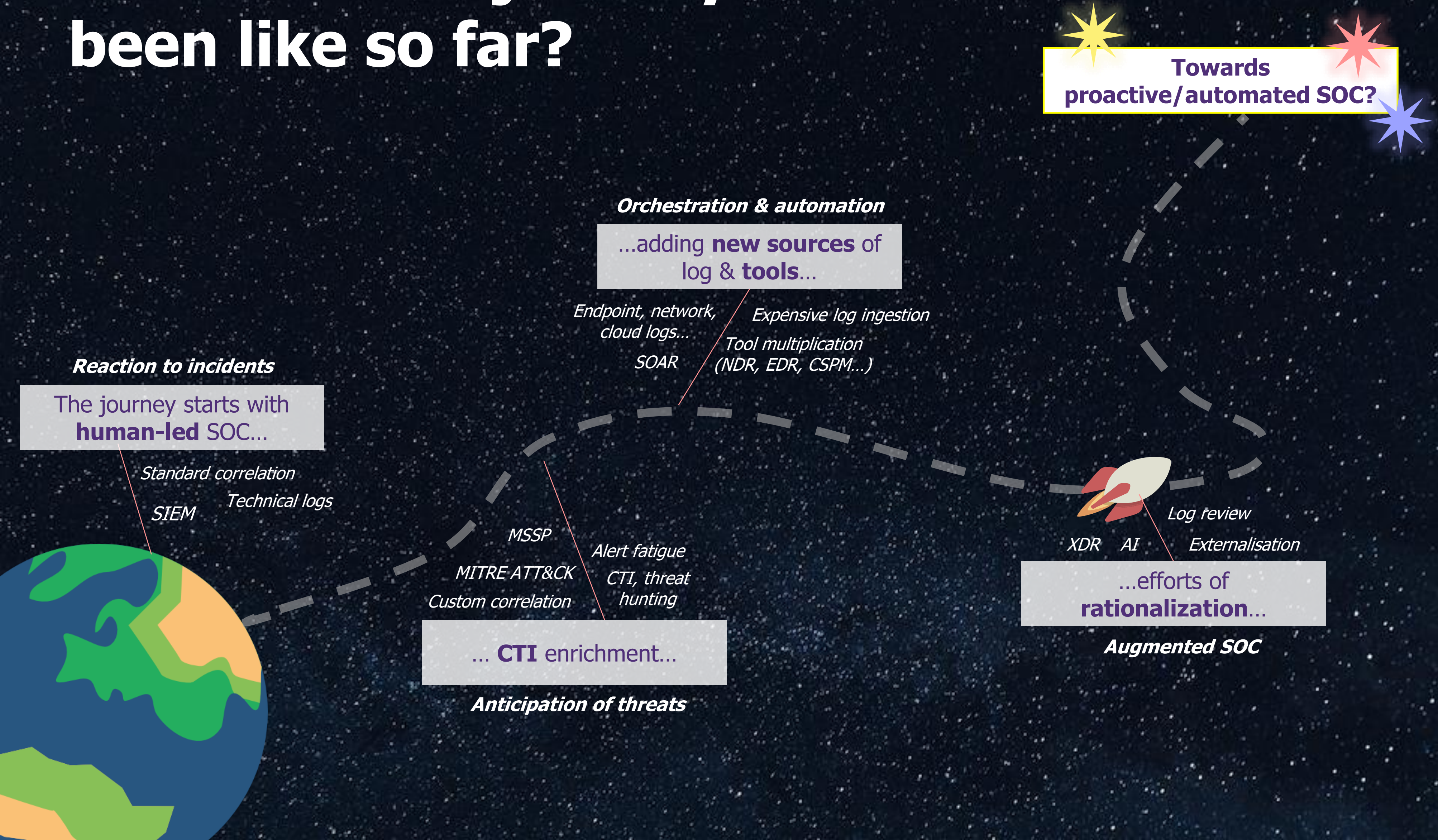
WAVESTONE

Navigating the Nebulae: unveiling new horizons for the SOC

SOC already made a leap in automation, what are tomorrow's challenges to gain efficiency?

Wavestone Insight Day 2024 - 23/04/2024

What has the journey been like so far?



Reaction to incidents

The journey starts with **human-led** SOC…

Standard correlation

Technical logs

SIEM

... **CTI** enrichment...

Anticipation of threats

MSSP

MITRE ATT&CK

Custom correlation

Alert fatigue

CTI, threat hunting

Orchestration & automation

…adding **new sources** of log & **tools**…

Endpoint, network, cloud logs…

SOAR

Expensive log ingestion

Tool multiplication (NDR, EDR, CSPM…)

…efforts of **rationalization**…

Augmented SOC

Log review

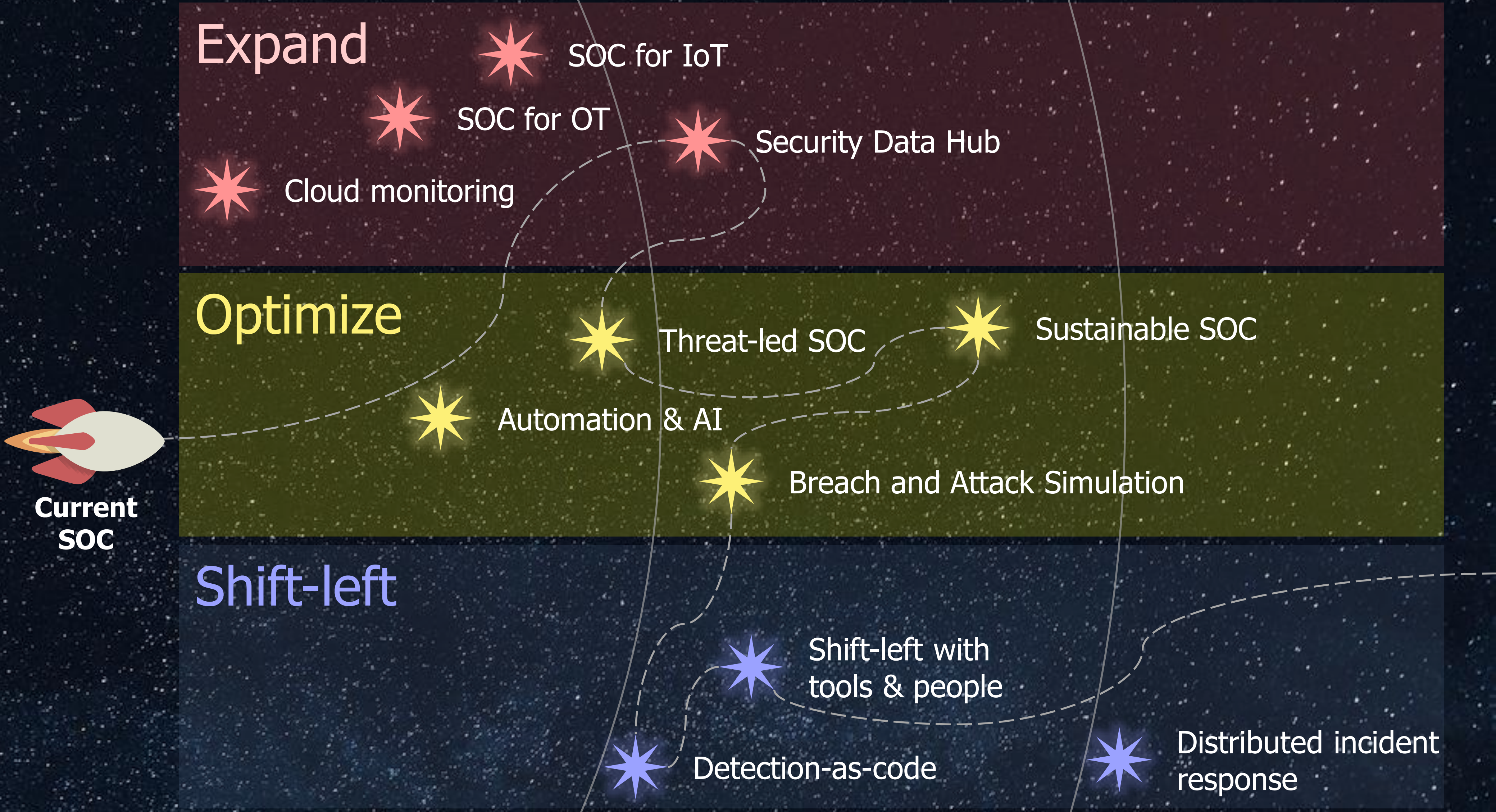
XDR

AI

Externalisation

Towards proactive/automated SOC?

Your flight plan toward automation & proactivity



Expand

SOC for IoT

SOC for OT

Security Data Hub

Cloud monitoring

Optimize

Threat-led SOC

Sustainable SOC

Automation & AI

Breach and Attack Simulation

Current SOC

Shift-left

Shift-left with tools & people

Detection-as-code

Distributed incident response

EXPAND to prepare the field for the next cybersecurity paradigm

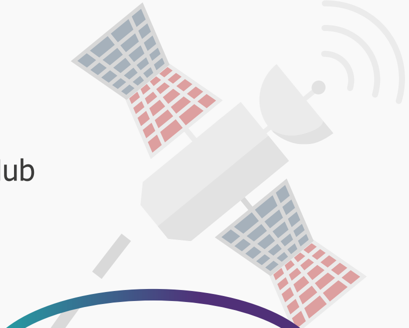
Expanding is a **necessary step** but also an **opportunity** to tackle new scope monitoring & automate reaction

Cloud monitoring

SOC for IoT

SOC for OT

Security Data Hub



Beyond SOC

Beyond Security

Towards new Features

Expand **outside the current SOC scope**:

- Towards **Fusion Center**
- Fraud, OT, physical security, DevSecOps
- Threat Intelligence to feed other teams (new fraud scenarios)

Expand **beyond Security**:

- **DataHubs**, used by businesses, creating new usage for security: reporting, dashboards, observability, next-gen security analytics

Expand **Cybersecurity features**:

- **Vulnerability Operations Center**
- Facilitate integration with other tools (UEBA, SOAR, CTI…)

DATAHUB: benefiting from the trend for cost control and upgrading the security approach

Data has been the riches of enterprise for the last 20 years

It's even more relevant with AI and increasingly powerful Cloud platforms.

This translates into:

- **Enterprise Datahubs** (one or several)
- Need for **fastest query** possibilities
- *Emerging Datamesh with the growing use of CI/CD (Dev-centric approach)*

Security could benefit from the Enterprise Datahubs…

Reducing the volume of data ingestion by the SIEM

Scope evolves and so does log volume. To deal with it, sending some logs to the SIEM or to a datalake can reduce overall licensing costs for SIEM.

Getting **new KPI possibilities**: next-gen security analytics

With the right security tags, creation of new behavioral analytics and real time observability.

Expanding the SOC activities

For fusion center, new business scenarios, audit, compliance, cyber threat hunting, use of AI & ML… SIEM should be capable of performing search query across multiple datasets.

…(even if it comes with challenges)

Cold/hot storage

Cost

Query speed (via SIEM)

Data structuration

Data gouvernance

Data quality

Data security

3rd party integrations

Compliance

Tools integration

Data format

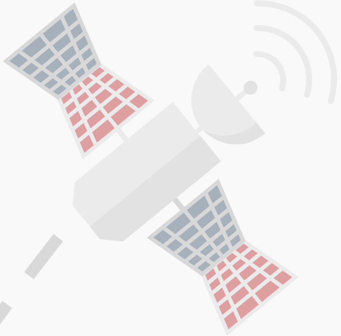
Optimize towards **automated & realistic** continuous improvement

Threat-led SOC

SOAR, automation & AI

Sustainable SOC

Breach and Attack Simulation



To expand more efficiently and monitor new scopes, SOC will have to **optimize tooling & costs**

Optimize the SOC by **focusing on critical points**:

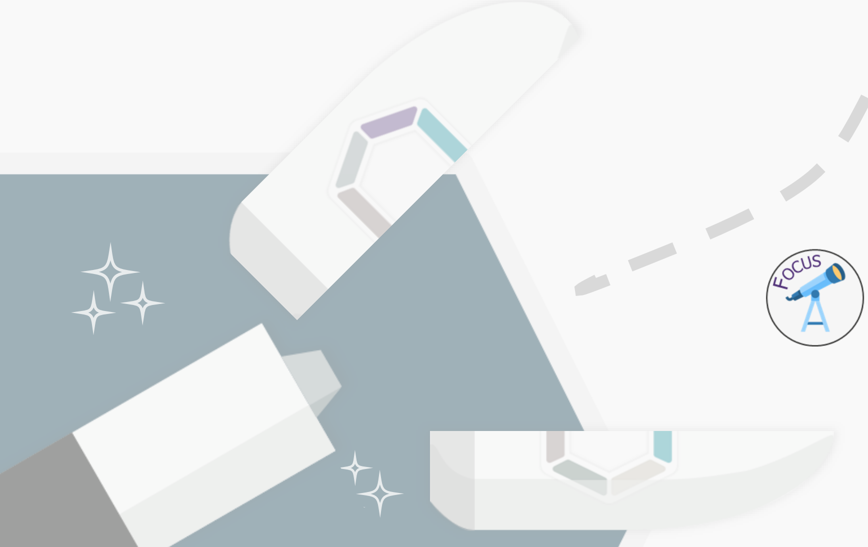
- **Threat-led SOC** leverages on Threat intelligence and Critical asset identification to **test critical scenarios and alerts**

Optimize the SOC performance thanks to **new tools**:

- **Breach and Attack Simulation tools** impersonate red-team like exercise to move toward a **threat-centric approach to cyber and automate continuous improvement (with Detection as Code)**
- SOAR & AI offer new possibilities to **fine tune detection and automate reaction**

Optimize by **reducing costs**:

- A **more sustainable SOC** could help reducing costs (log generation, storage) **while keeping the same security level**

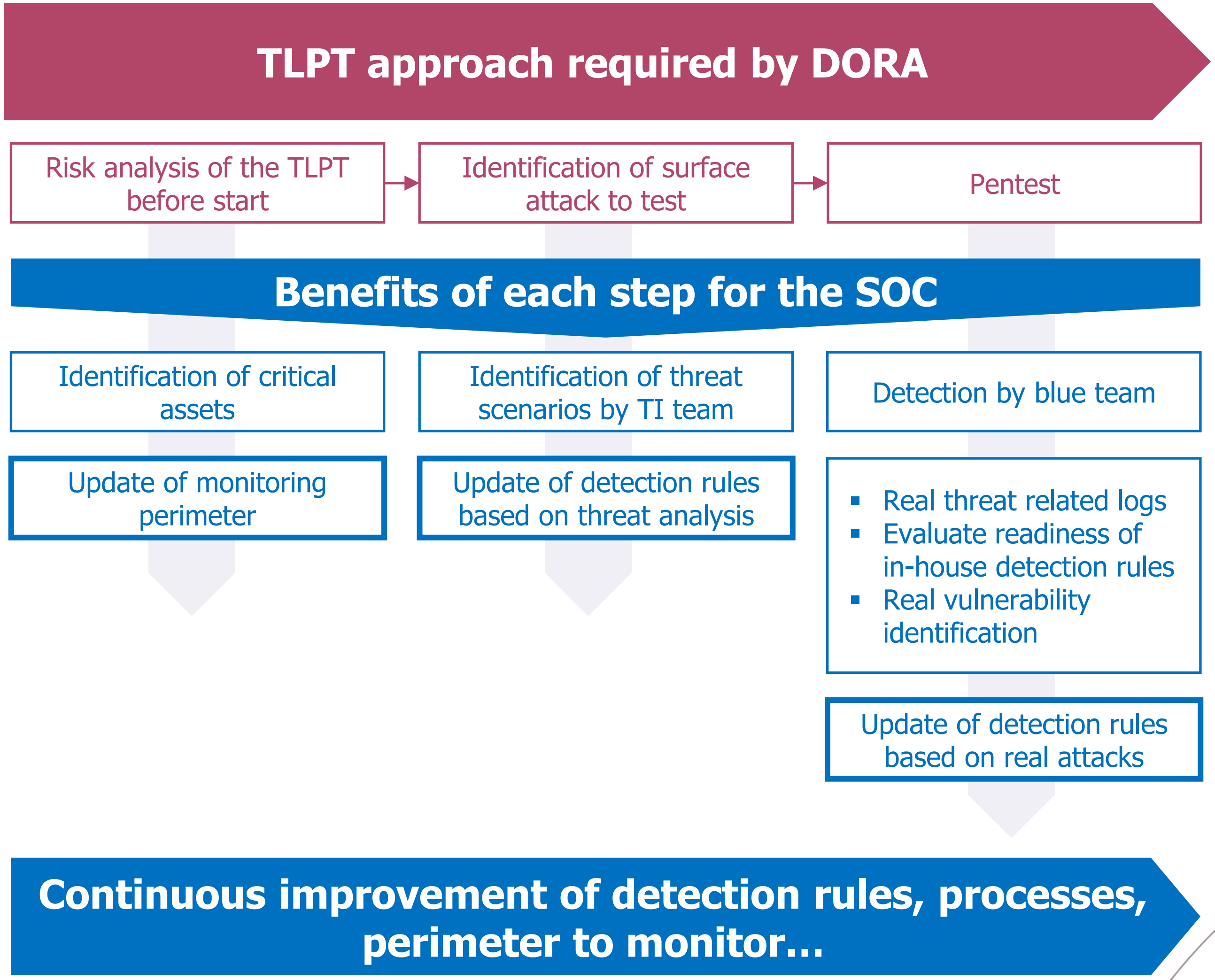


THREAT-LED SOC: ideas from Threat-led pentests (TLPT) to optimize the SOC capabilities

DORA regulation
(Digital Operational Resilience Act - 2022)

Goals:
- **Strengthening the IT security** of financial entities such as banks, insurance companies and investment firms
- Making sure that the financial sector in Europe is able to **stay resilient** in the event of a severe operational disruption.

Threat Led Pentests (TLPT):
- Threat-led red teaming (simulating real attacks to critical assets),
- Involving blue and TI teams,
- Identify and remediate vulnerabilities,
- Strengthen security posture.



TLPT approach required by DORA

Risk analysis of the TLPT before start → Identification of surface attack to test → Pentest

Benefits of each step for the SOC

Identification of critical assets

Update of monitoring perimeter

Identification of threat scenarios by TI team

Update of detection rules based on threat analysis

Detection by blue team

- Real threat related logs
- Evaluate readiness of in-house detection rules
- Real vulnerability identification

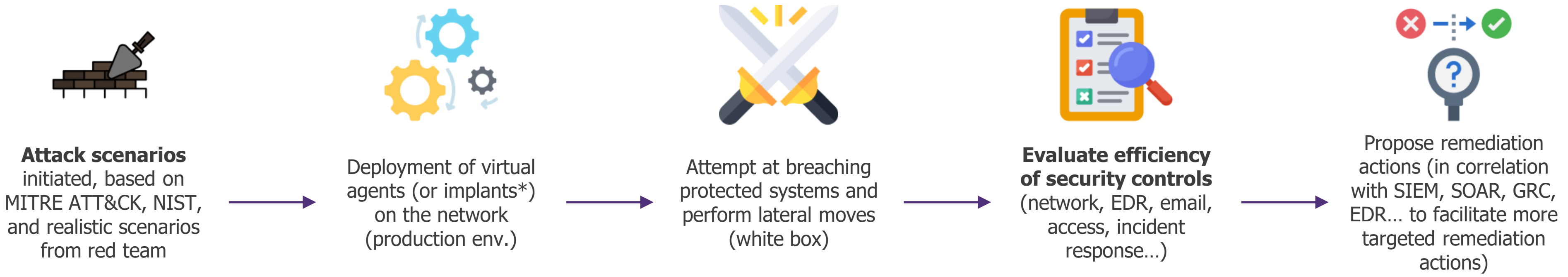
Update of detection rules based on real attacks

Continuous improvement of detection rules, processes, perimeter to monitor…

Breach & attack simulation tool: a threat-centric & proactive approach to detection rules testing

How does it work?

It's like a **red team exercise**, with **simulated, realistic & automated attacks** paths, vectors and scenarios, to **test the security posture of an organization**, identifying its **vulnerability, weaknesses and detection & incident response** capabilities.



Attack scenarios initiated, based on MITRE ATT&CK, NIST, and realistic scenarios from red team

→ Deployment of virtual agents (or implants*) on the network (production env.)

→ Attempt at breaching protected systems and perform lateral moves (white box)

→ **Evaluate efficiency of security controls** (network, EDR, email, access, incident response…)

→ Propose remediation actions (in correlation with SIEM, SOAR, GRC, EDR… to facilitate more targeted remediation actions)

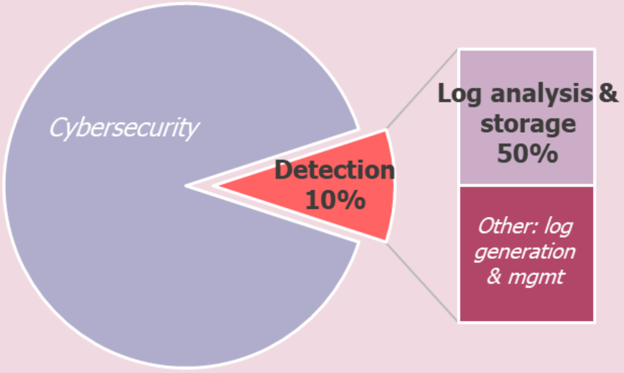
- Use of real Tactics, Techniques & Procedures to **proactively** identify and **mitigate** security vulnerability, before they can be exploited
- **Fully automated**
- Continuous testing of detection rules (**reduction of false negative alerts**)
- Developer-centric model

- Improved accuracy of detection rules (reduction of false positive but risk of overfitting)

*implants are deployed in RAM, to mimic stealthy attacks

SUSTAINABLE SOC: it could help optimize your SOC's costs!

Detection activities amount for 10% of the GHG emissions of Cybersecurity



Percentage of Greenhouse Gas (GHG) Emission by activities

How to reduce the SOC impact (& cost), while keeping the same security level ?

Optimize the volume of logs

- Reduce the volume of collected and stored logs (avoid log duplication when not necessary).
- Reduce verbosity and storage time (hot vs cold storage).

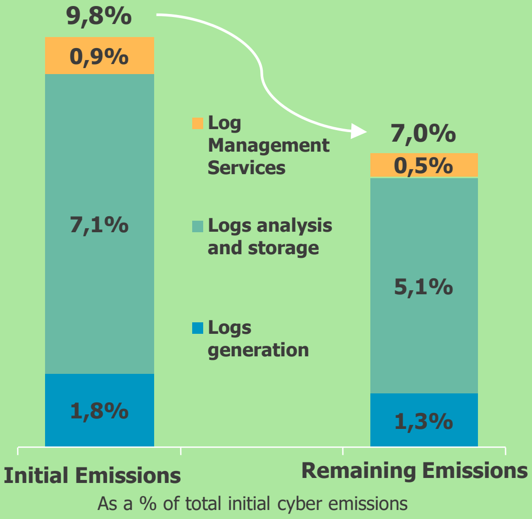
Optimize resources usage

- Using shared resources (ex. Public cloud, MSSP infrastructure) when possible.
- Train SOC analysts to optimize queries (limiting queried data and CPU).

Theoretical example

Reduction potential with the following actions:

- Reduce the volume of logs collected and stored by 20%
- Use an MSSP to optimize by 10% thanks to mutualization



As a % of total initial cyber emissions

With these measures, the impact of detection could be reduced to 7% of cyber emissions.

By reducing log verbosity and avoiding unnecessary log duplication, **Wavestone reduced the volume of its logs collected and stored by 56%.**

*From Wavestone study: "**Sustainability: Cybersecurity has a role to play**" by G. Billois, N. Gauchard & H. Bérard., Jan. 2024*
Security measure studied: logs are collected, centralized in a SIEM and analyzed to detect security alerts.

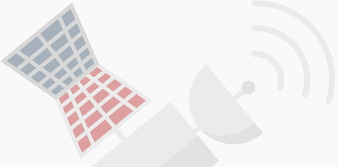
SHIFT-LEFT to ensure security reaction is as fast as attackers are creative

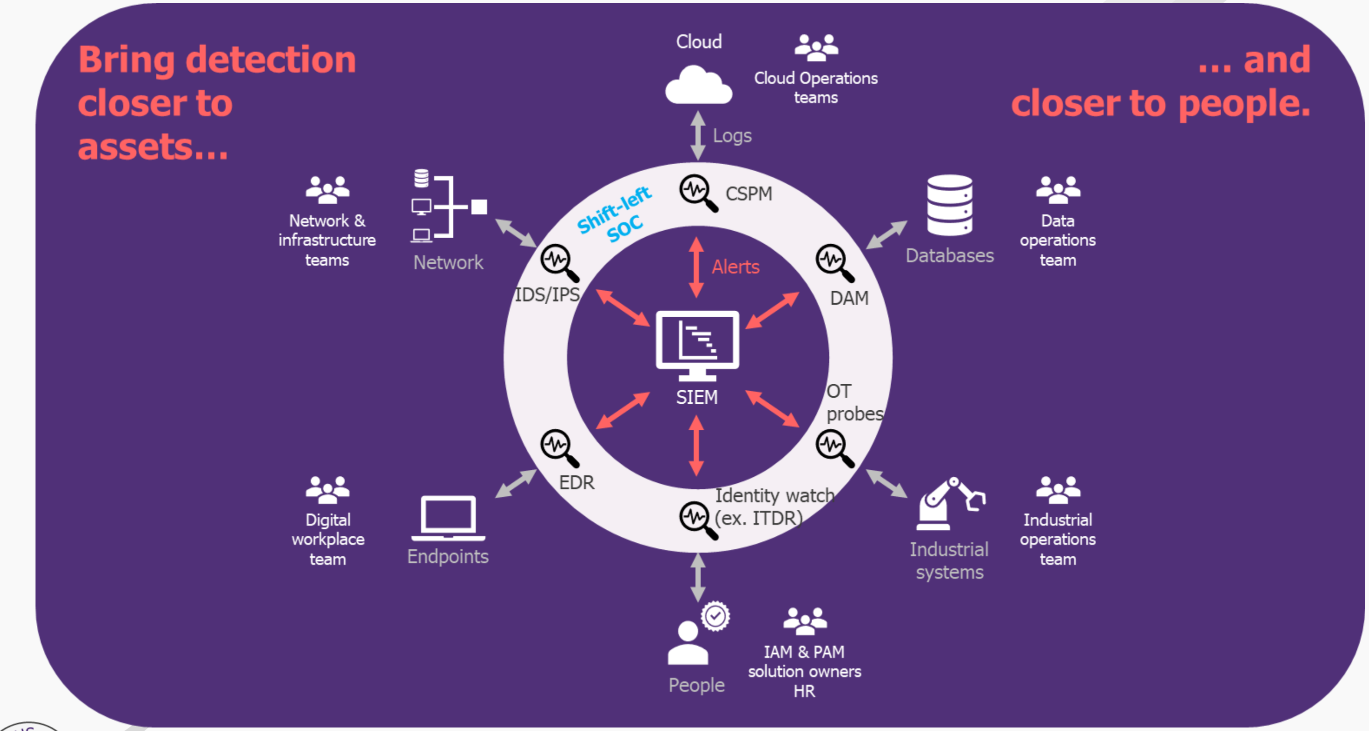
To really push optimization at its best, **shift-left is the next step for faster detection & remediation** capabilities

Shift-left tools: NDR, XDR

Detection as code

Distributed incident response





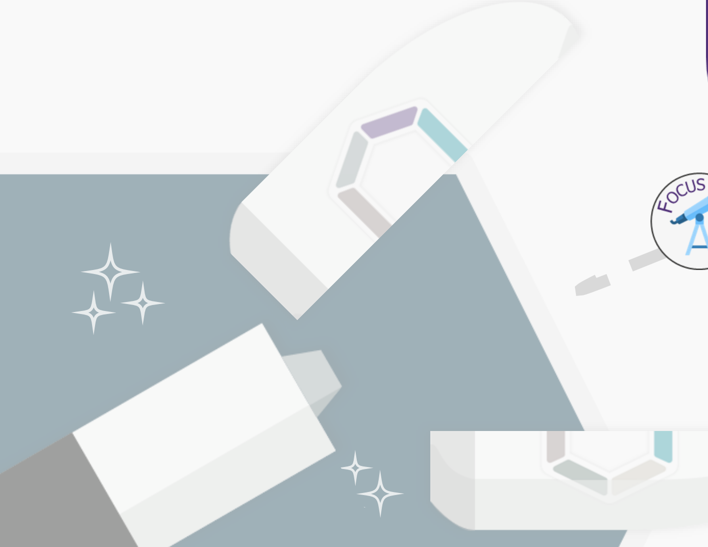
Bring detection closer to assets…

… and closer to people.

- **Detection as code** eases use-case addition and detection rules **automated mass-deployment**.

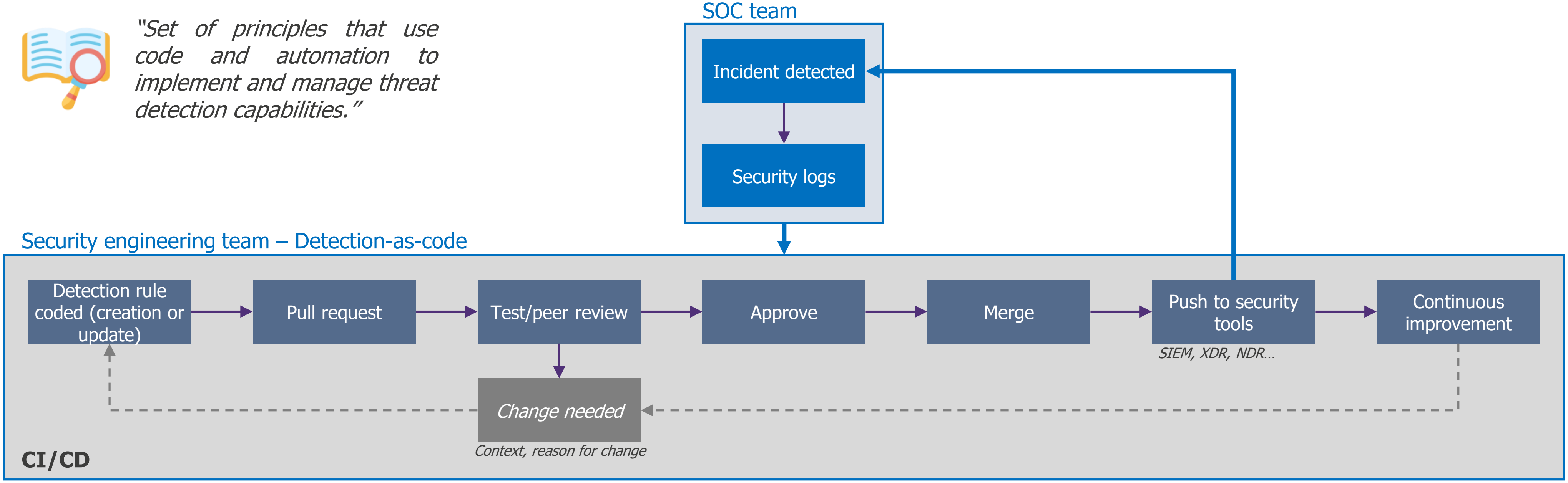
Shift left to keep on optimizing the SOC

- **Early detection** means issues could be resolved sooner with fewer resources and less downtime



DETECTION-AS-CODE: a necessity vs. emerging threats

"Set of principles that use code and automation to implement and manage threat detection capabilities."



Agility

- Programming language (**tailored** detection rules, benefiting from **community** inputs like third-party libraries, e.g. YARA-L rules)
- **Reusable code** between detection rules (share functions)
- **Quick creation/modification** to rules in front of emerging threats

Test-driven approach

- **Changes** are made easier without fear of breaking alerts
- **Test** by peers
- **Version control** with context

Automation

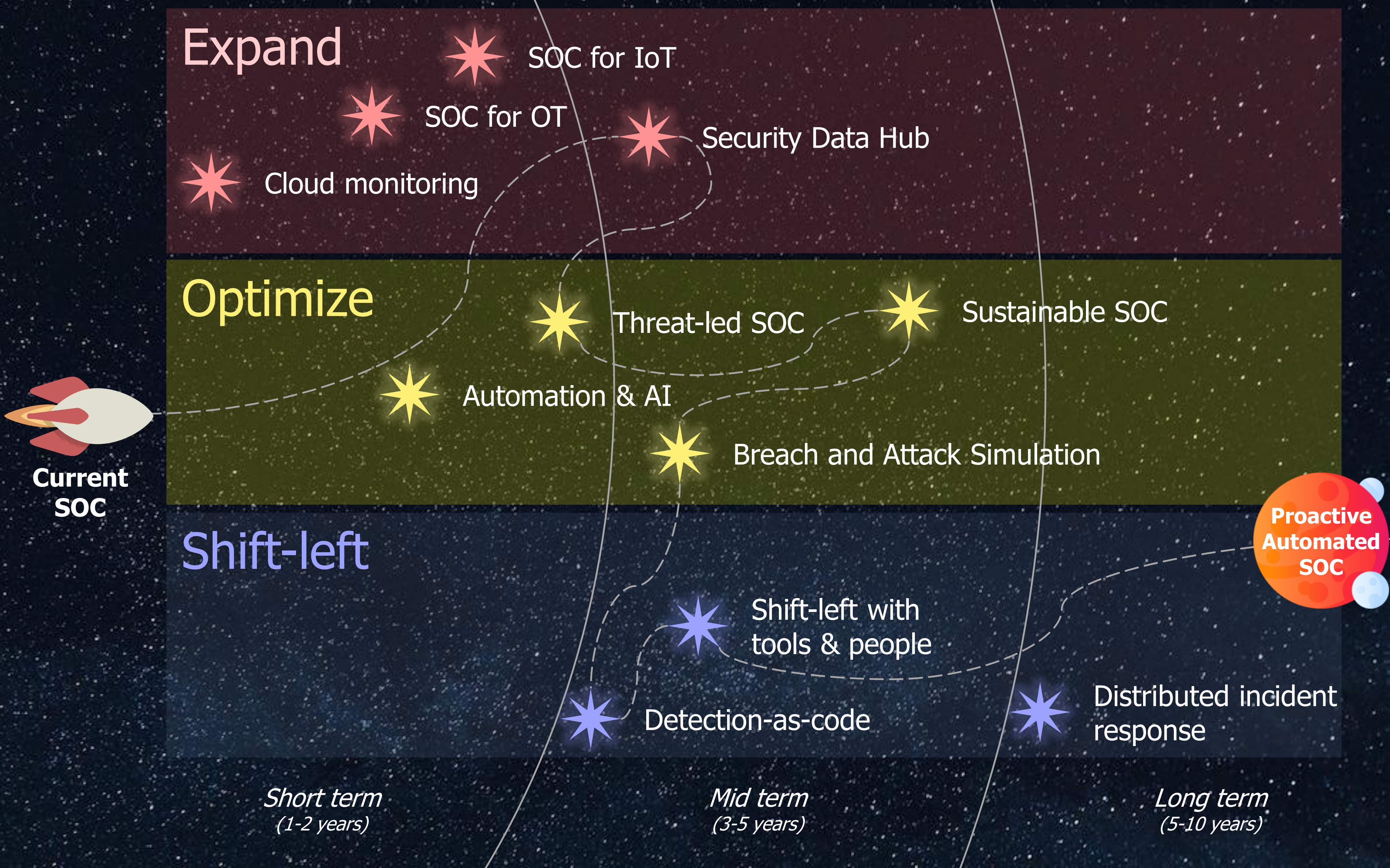
- Automated **delivery** to security tools

And to go further:

- *Automated **testing** (BAS: test for false alerts & have real-time up-to-date detection)*
- *Automated **response** (coupling with SOAR-like tools)*

Restricted distribution

Welcome to your destination!



Expand

SOC for IoT

SOC for OT

Security Data Hub

Cloud monitoring

Optimize

Threat-led SOC

Sustainable SOC

Automation & AI

Breach and Attack Simulation

Shift-left

Shift-left with tools & people

Detection-as-code

Distributed incident response

Current SOC

Proactive Automated SOC

Short term
(1-2 years)

Mid term
(3-5 years)

Long term
(5-10 years)

The Positive Way

WAVESTONE

Emma BARFETY Manager	M +33 (0)6 67 78 71 85 emma.barfety@wavestone.com
Benoît MARION Senior Manager	M +33 (0)6 83 62 37 55 benoit.marion@wavestone.com
Antoine D’ESTALENX Consultant	M +33 (0)7 61 59 97 95 antoine.destalenx@wavestone.com

And special thanks to the Wavestone SOC Core Team.

wavestone.com

in Wavestone

Sources

Topic	Title	Author / Company	Link
SOC models	State of SIEM 2021	Panther	Link
SOC models	Wavestone 2024 SOC panorama	Wavestone	Publication to come
SOC models	SOC Model Guide	Gartner	Link
SOC models	Modern Security Operations Center (SOC) Strategies	Gartner	Link
SOC models	SANS 2023 SOC Survey	SANS Institute	Link
SOC models	Carson Zimmerman Versus Anton Chuvakin: A Live SOC Debate!	Google Security Operations	Link
Optimize	Future of the SOC: Evolution or Optimization —Choose Your Path	Google Cloud | Deloitte	Link
Optimize	Fusion center : Le futur du SOC	Wavestone	Link
Optimize	Evolution du SOC en France: Migration vers une Solution Cloud augmentée par l'IA pour renforcer la cyber-résilience et l'efficacité opérationnelle	IDC |Microsoft	Link
Threat-led	DORA regulation (REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL)	European Union	Link
Threat-led	Draft Regulatory Technical Standards specifying elements related to threat led penetration tests	European Union	Link
Threat-led	Being "Threat-Led" is the answer. Your ISO certificate won't save you from a breach!	Vectra AI	Link
Threat-led	Lessons From the Trenches: Building a Threat Led Security Operations Capability (SOC)	AttackIQ	Link
Sustainable SOC	Sustainability: Cybersecurity has a role to play	Wavestone	Link
Shift-left	Shift the SOC left: Why your organization should integrate DevOps with Security Operations	Christopher R. Wilder, ReversingLabs	Link
Detection as code	From soup to nuts: Building a Detection-as-Code pipeline	David French	Link
Detection as code	How to Create a Code-Based Detection	Panther labs	Link

Authors also consulted multiple Wavestone SOC experts who gave their insights on the topics based on their experience.

Restricted distribution