AI in Security Operations

No longer optional



Rob van Os | Strategic SOC Advisor

11 November 2026

TLP:CLEAR

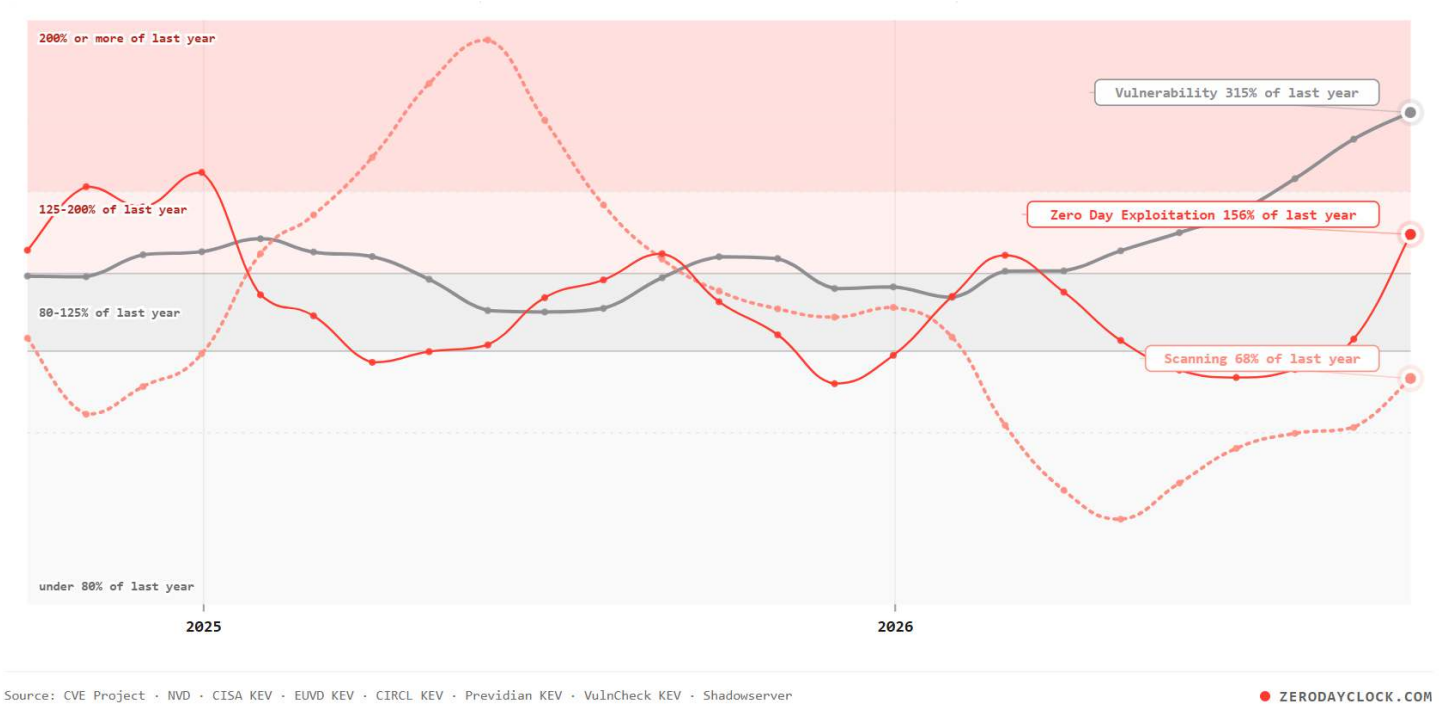
Vulnerability trends

Vulnerability & exploitation growth

- Vulnerability discovery is accelerating
- Zero-day exploitation is faster

→Faster response times are required to manage the attack surface and avoid compromise

→Traditional vulnerability management cannot keep up



Source: [Zero Day Clock: vulnerability exploitation, measured]

AI-enabled adversaries

AI attack landscape

- Adversaries are making increased use of AI
  - AI-assisted
  - AI-powered
  - AI-enabled
  - *Insert your <AI-x> term here*
- Breakout times are decreasing rapidly, requiring a more immediate response for cyber defense teams

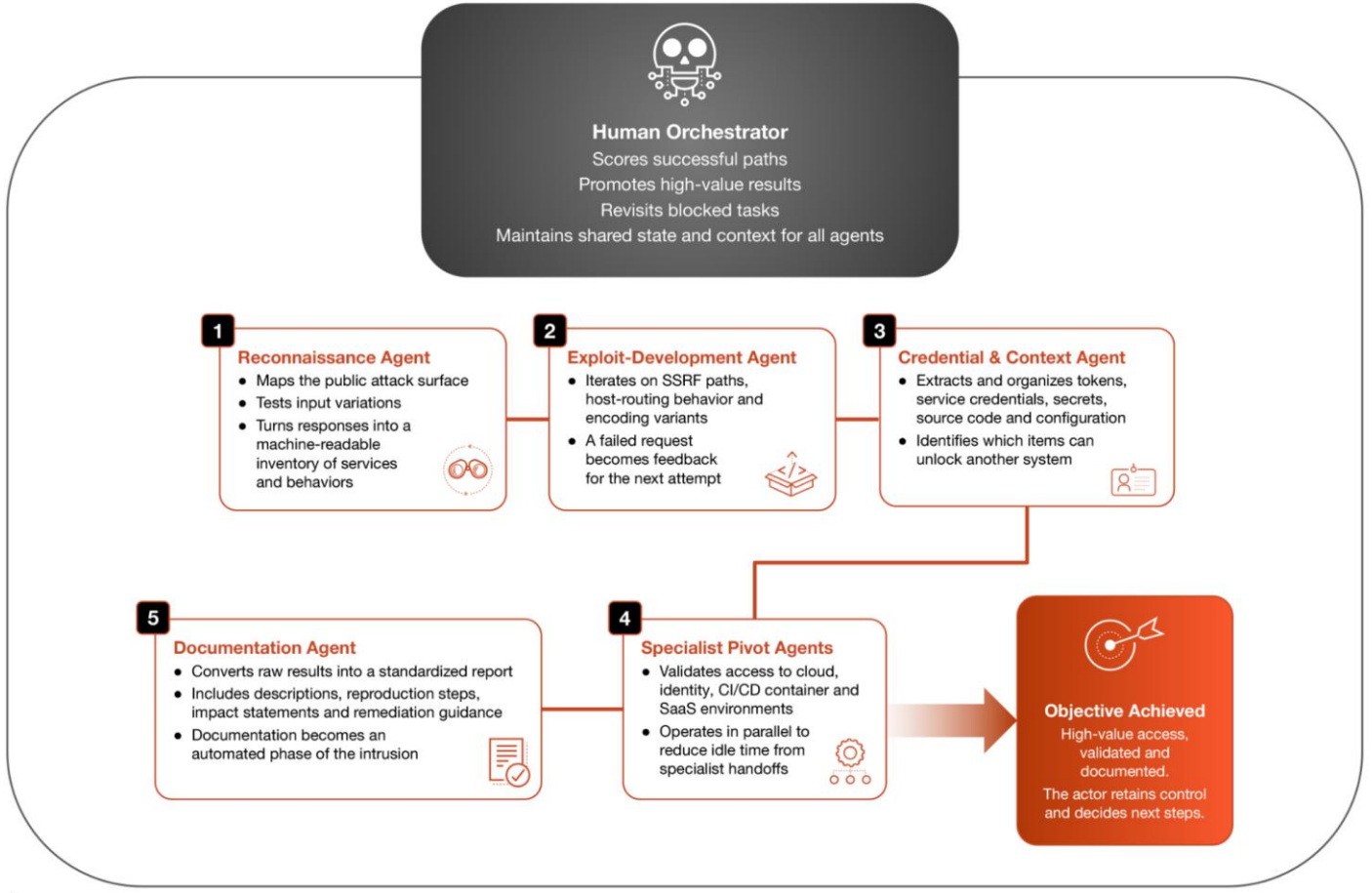


Source: [CrowdStrike 2026 Global Threat Report | Key Cyber Threat Trends]

Attack automation

Attack example

- Attack automation also has a human in the loop
- Multiple agents are begin used that exchange information automatically
- This reduces the human effort required significantly

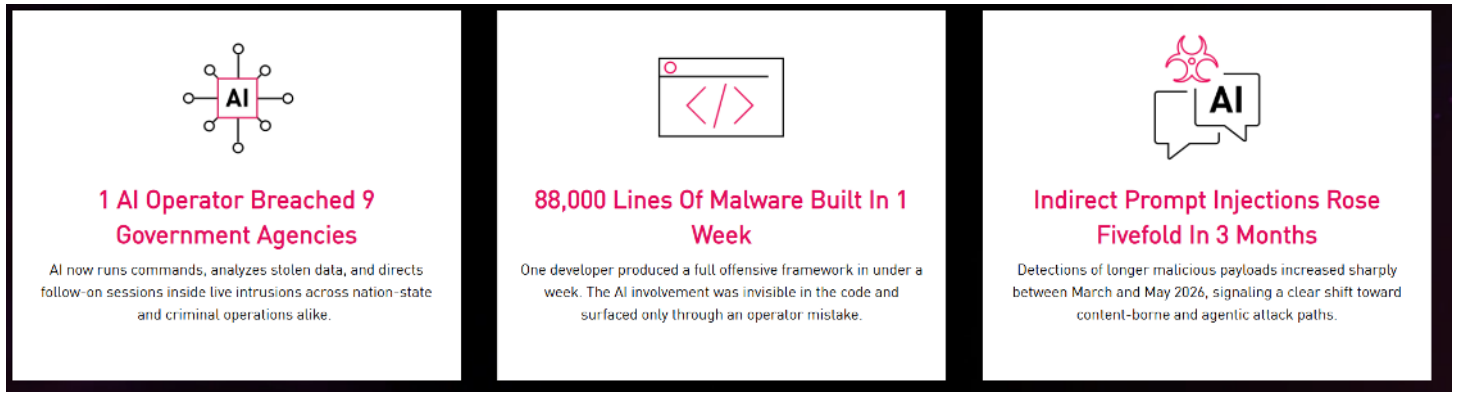


Source: [An AI-Assisted Cyber Attack: Inside a Unit 42 Investigation]

Attack automation

AI-assisted attack implications

- With reduced attack effort, attacks can be scaled up
- AI operaters can attack many targets simultaneously

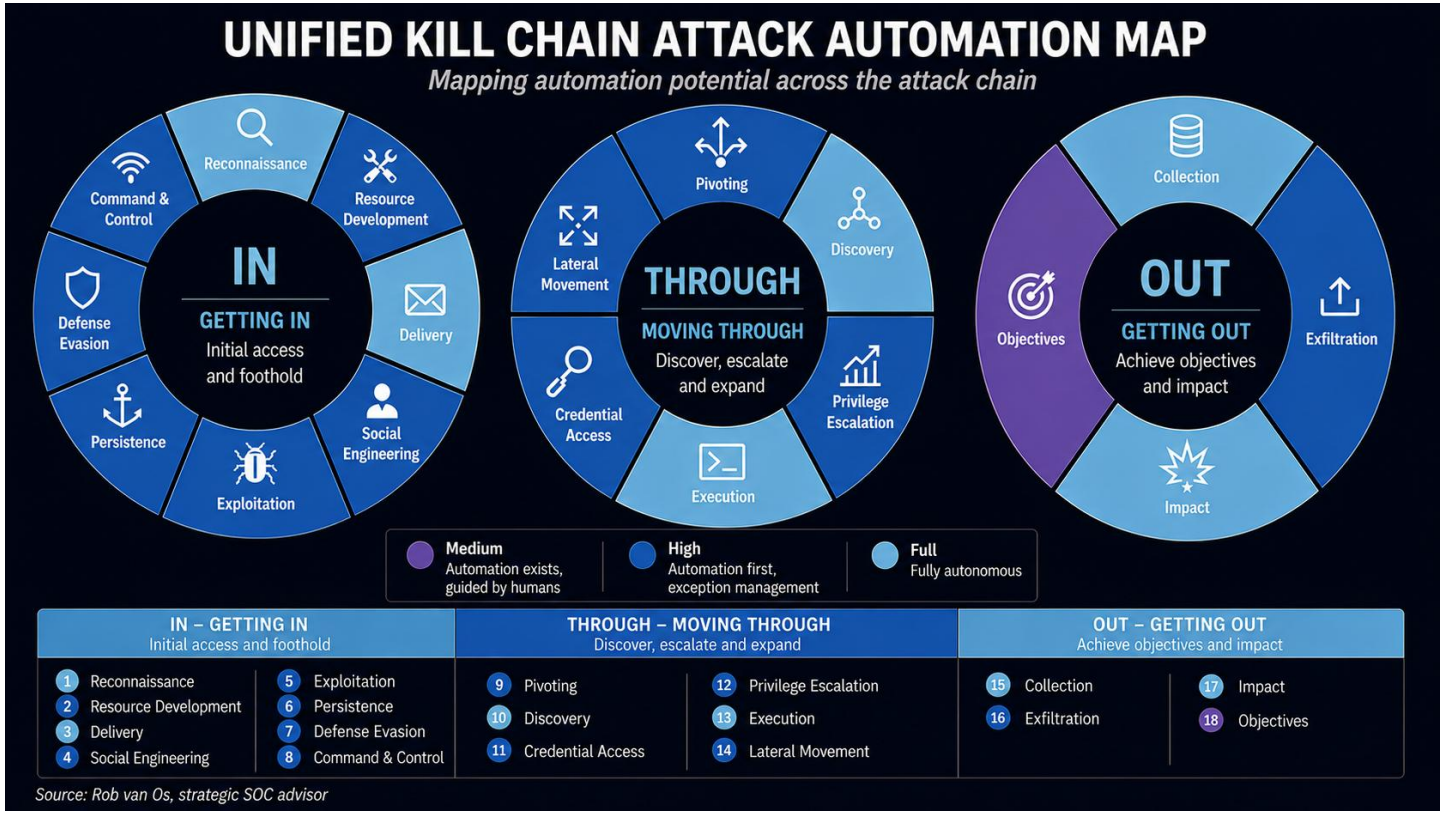


Source: [AI Security Report 2026 | Explore AI Security Threats & Trends | Check Point Software]

Attack automation

Attack chain automation

- Attacks are scaled-up and accelerating, and breakout time is continuously reduced
- This attack chain automation map shows the potential for automation across different steps of the kill chain
  - Medium: 6%
  - High: 61%
  - Full: 33%



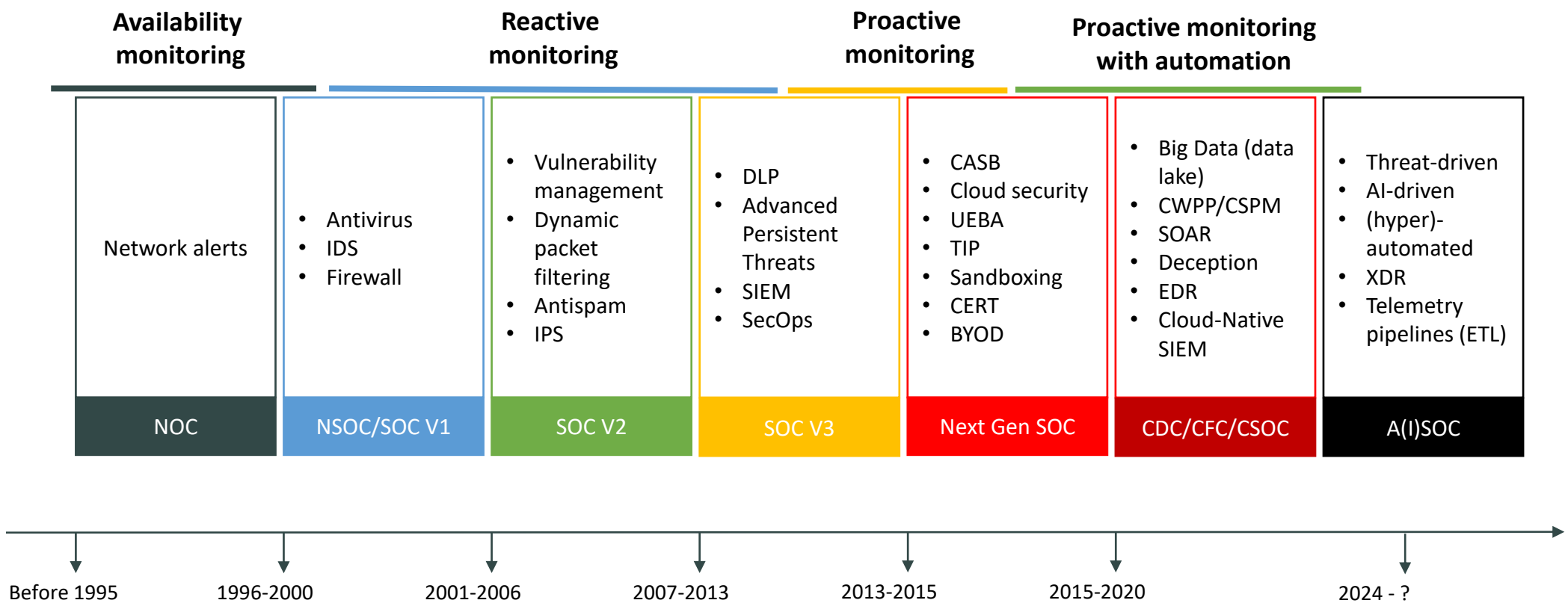


SOC EVOLUTION

AI-ENABLED SECURITY OPERATIONS

SOC evolution

Evolution of SOCs

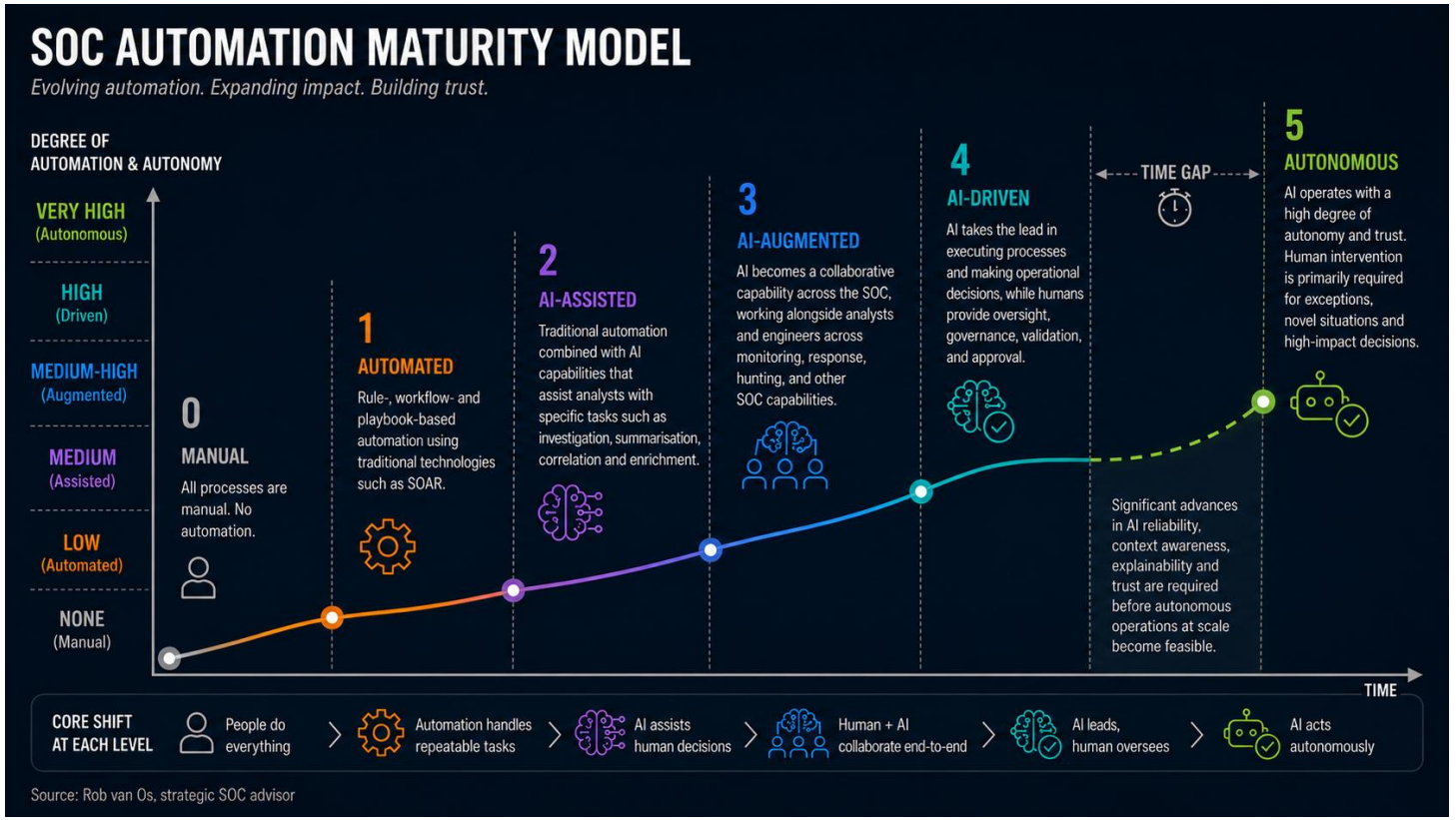


Based on: [2021 Volume 5 The Evolution of Security Operations and Strategies for Building an Effective SOC]

Automation maturity

SOC Automation Maturity Model (SAMM)

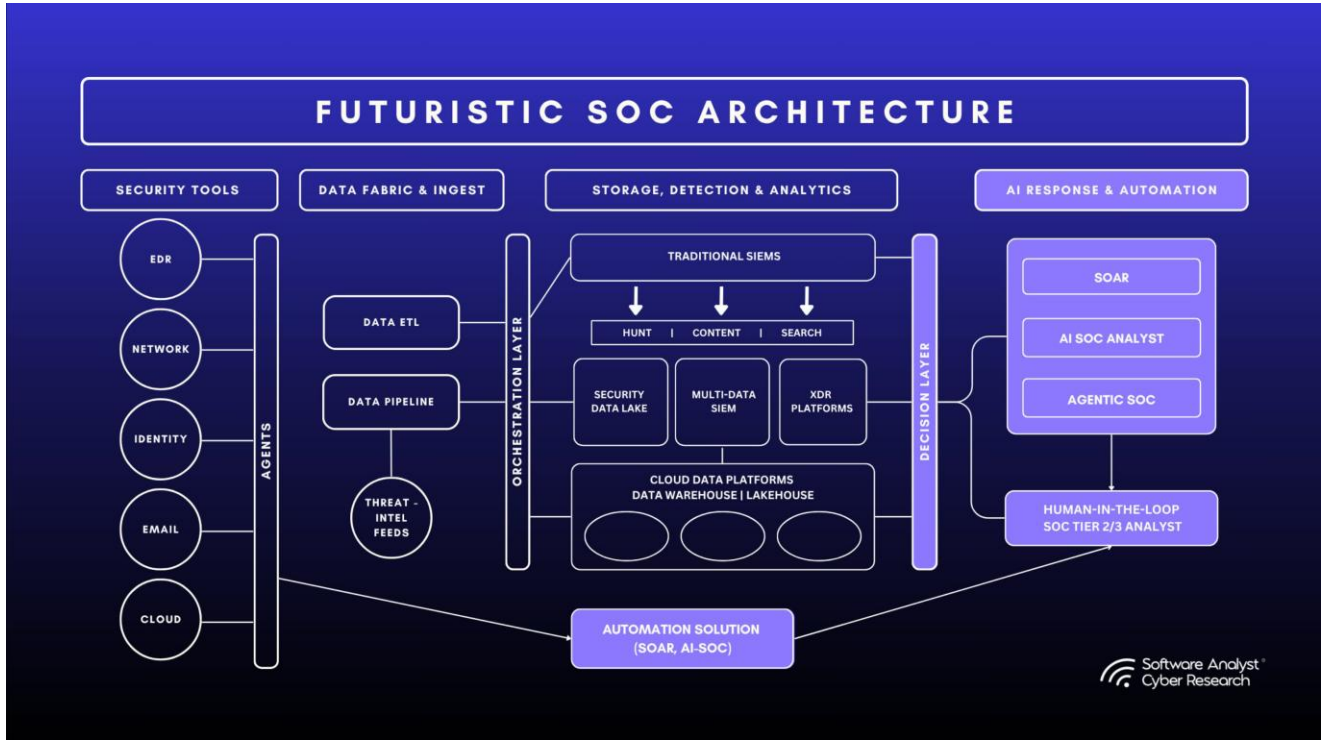
- Automation is a means for increasing efficiency and response speed in SOCs
- AI is a tool in the automation toolbox
- How much automation is possible?
  - Context is everything for decision making
  - Trust can be built over time



Further reading: [SOC Automation Maturity Model - AI & Automation - SOC-CMM User Community]

Futuristic SOC architecture

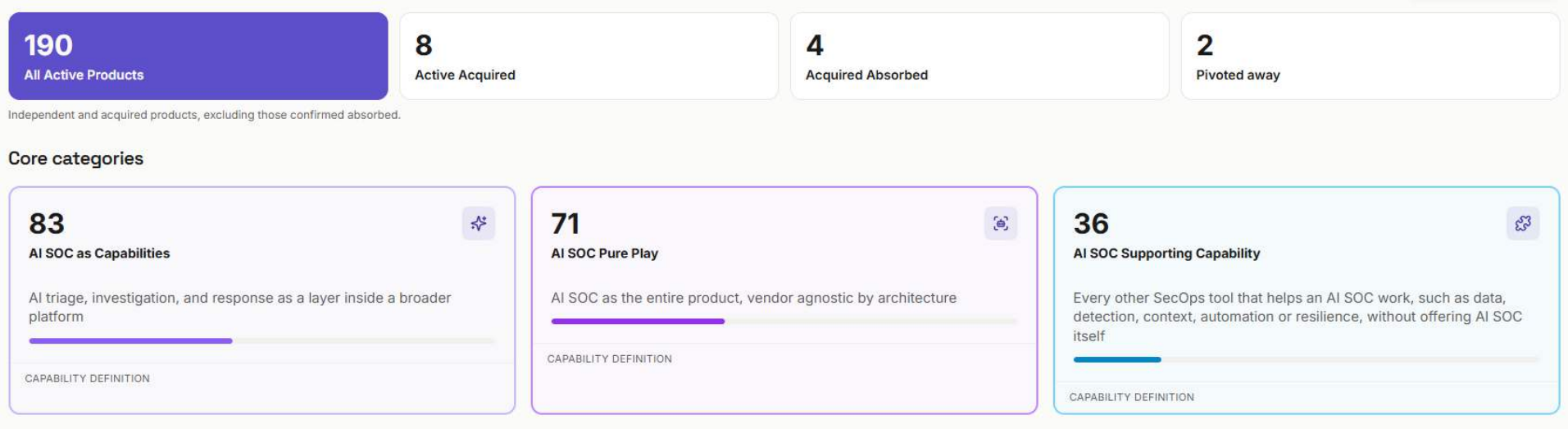
- The future SOC will rely heavily on automation, both traditional automation and AI-driven automation



From: [The AI SOC Market Landscape 2025 - Software Analyst Cyber Research]

Challenging landscape

- The AI-SOC landscape is difficult to navigate: many vendors, different approaches, different levels of capability and maturity
- Objective evaluation is necessary



From: [SecOps Unpakced - 190 AI SOC Platforms and Vendors: 2026 List]



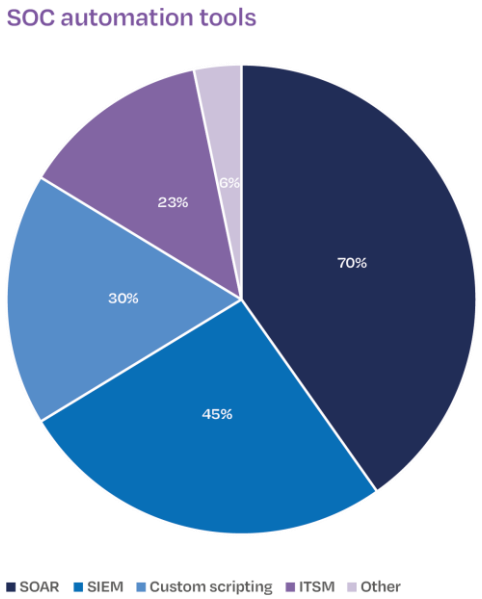
SOC MATURITY SURVEY OUTCOMES

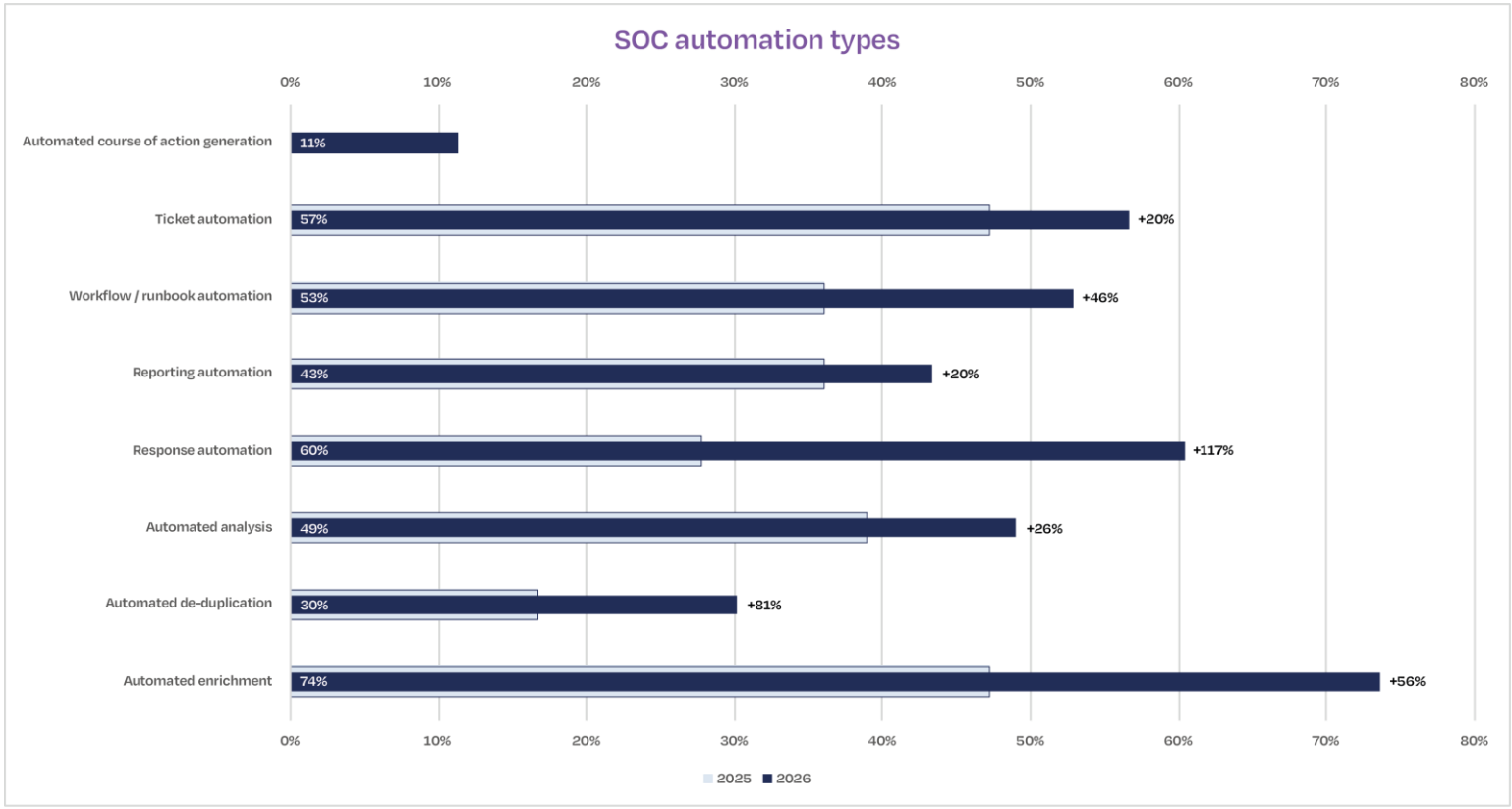
AUTOMATION AND AI

Survey outcomes

Automation and AI – SOC automation

- Automation is getting more common in SOC rapidly
- SOAR plays a major role in automation for many SOCs

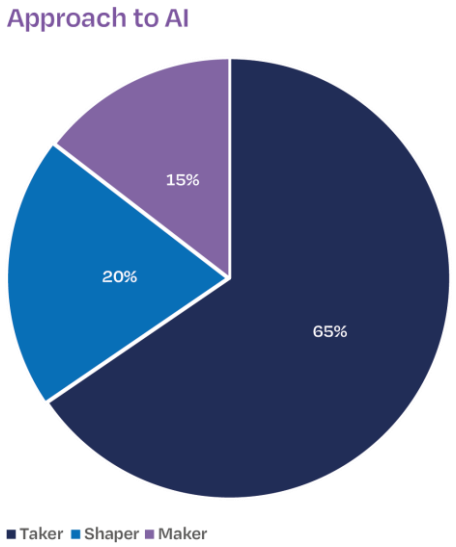


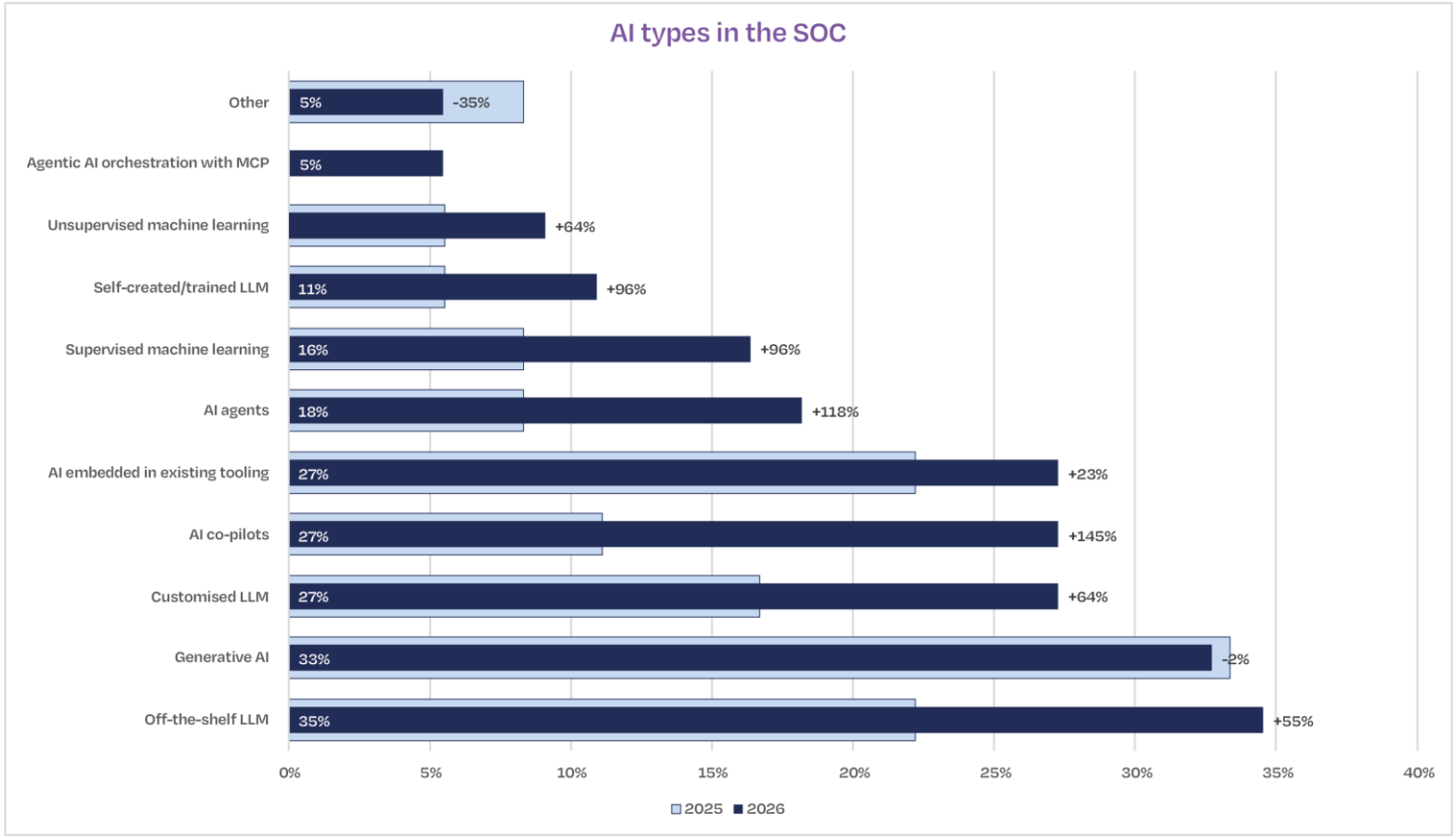


Survey outcomes

Automation and AI – SOC AI

- AI is still dominating the SOC discussion
- Increase of AI usage in SOCs is seen for almost all types of AI
- Most SOCs are primarily *takers* to their approach in adopting AI: using off-the-shelf products / tools

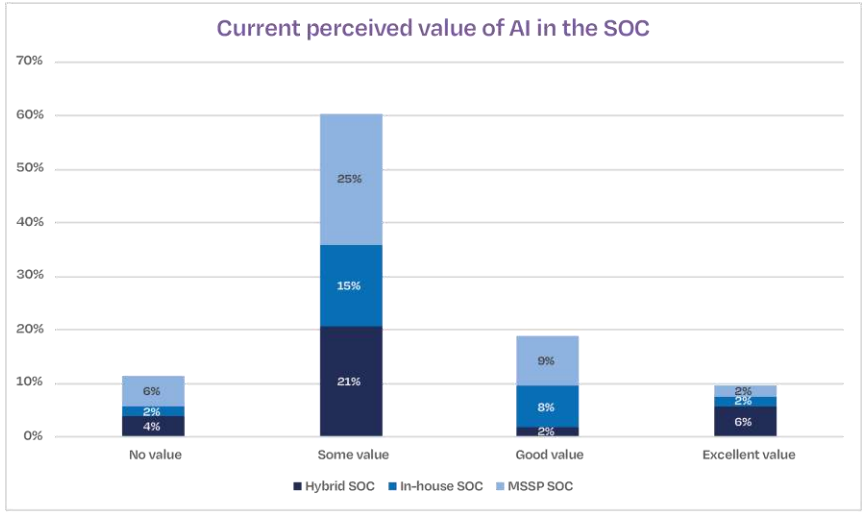


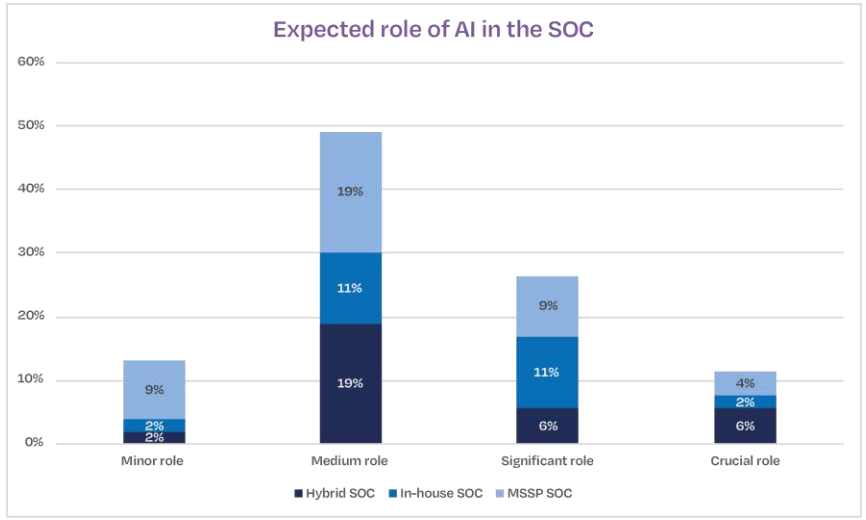


Survey outcomes

Automation and AI – AI value & role

- Currently, the perceived value of AI is still limited.
- The expected role of AI in security operations is deemed ‘medium’ by most respondents
- Only a small portion of respondents see AI playing a crucial role in security operations
- Regional analysis shows some variety with Asia, Middle East and European respondents the only ones foreseeing a crucial role

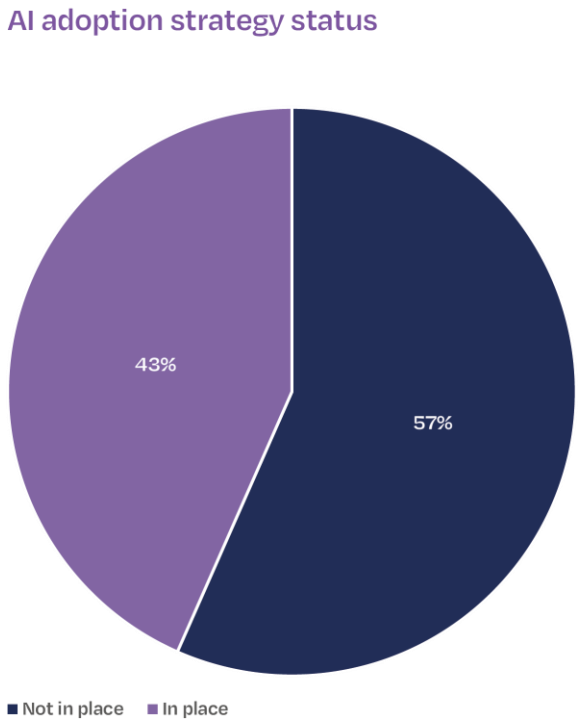




Survey outcomes

Automation and AI – AI adoption

- Optimizing AI in the SOC starts with clear strategy and direction
- This includes:
  - Overall strategy
  - AI types
  - Task to be replaced/augmented by AI
  - AI customization level
  - AI risks and guardrails
  - Metrics
  - Adoption timeline





MATCHING THE ADVERSARY

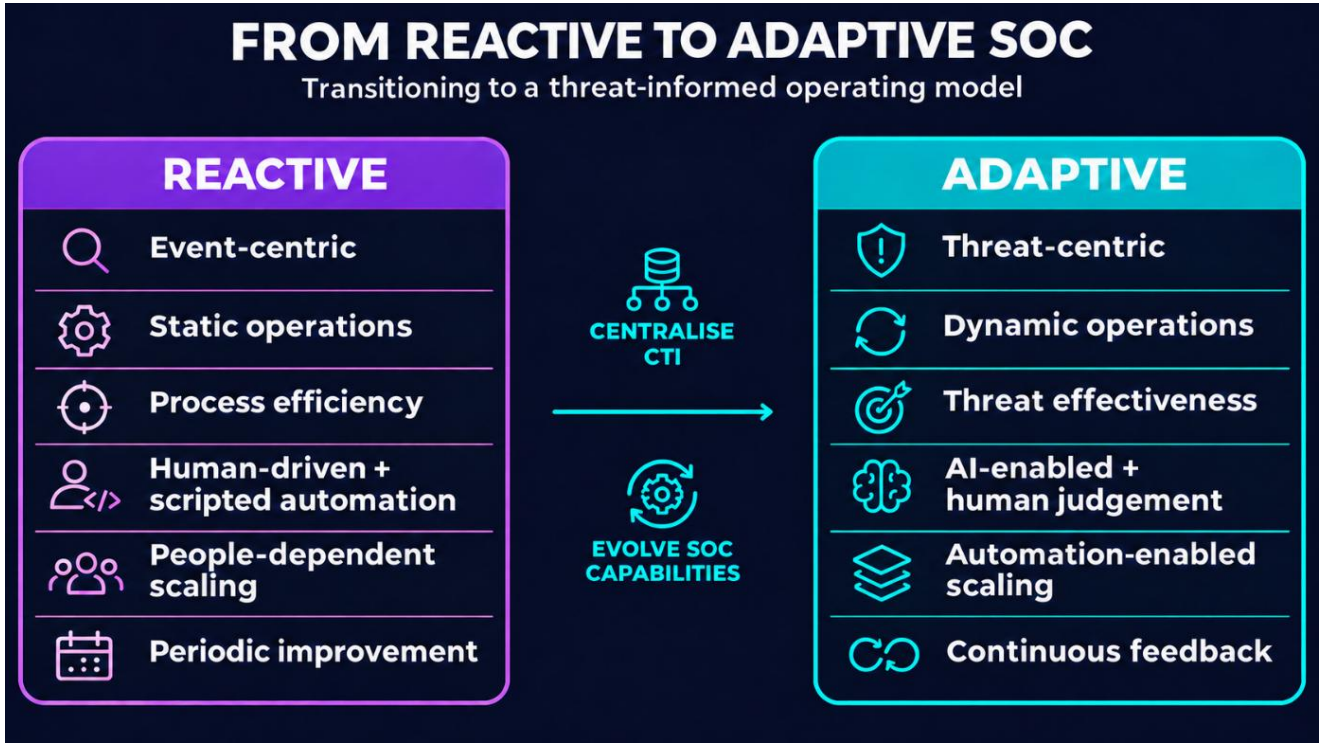
TRANSITIONING TO AN ADAPTIVE OPERATING MODEL

Adaptive security operations

Capabilities

The dynamic SOC:

- Revolves around integrated CTI
- Moves from events to threats
- Maturity shifts from process focus to threat relevance
- Higher levels of automation



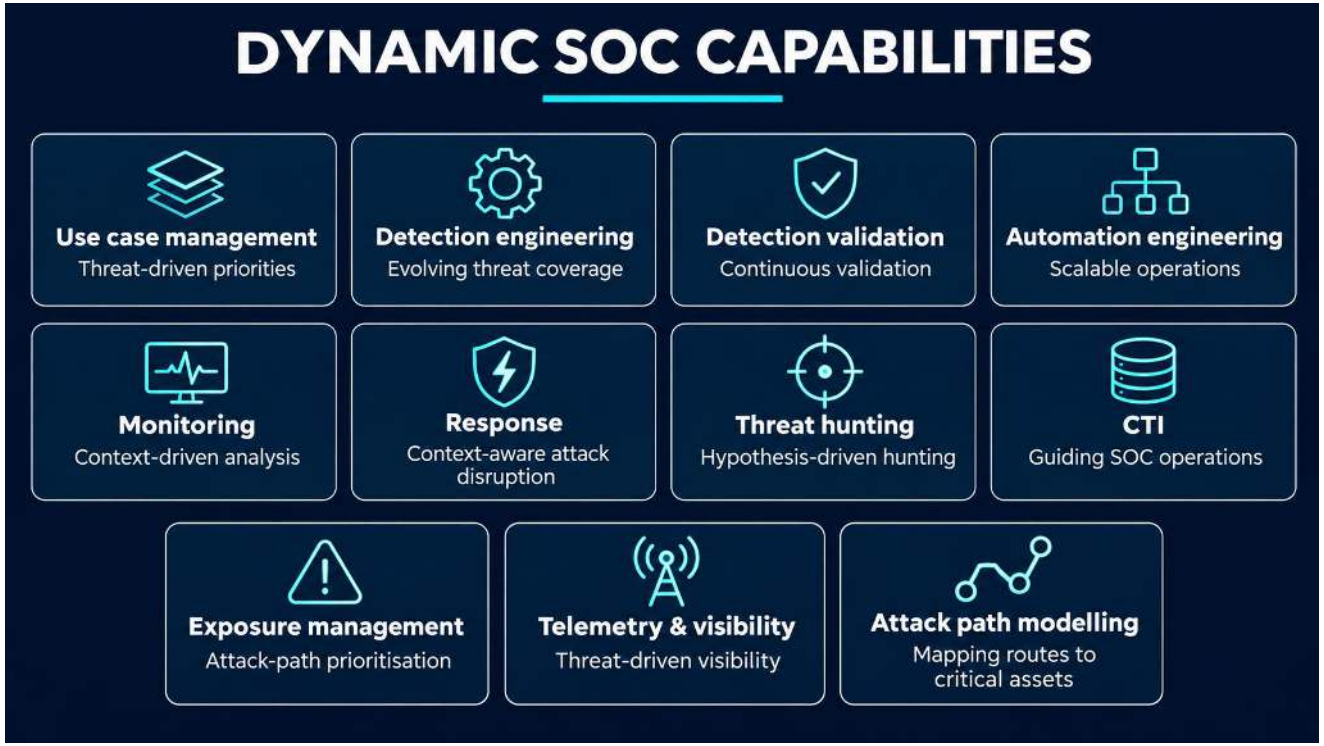
Reactive operations are driven primarily by observed events;
Adaptive operations are continuously shaped by relevant threats

Dynamic security operations

Capabilities

Capabilities evolve:

- Vulnerability management becomes exposure management
- Attack paths are proactively determine and integrated into monitoring and response
- Prioritisation of responses and activities is determine by what is relevant, not what comes first

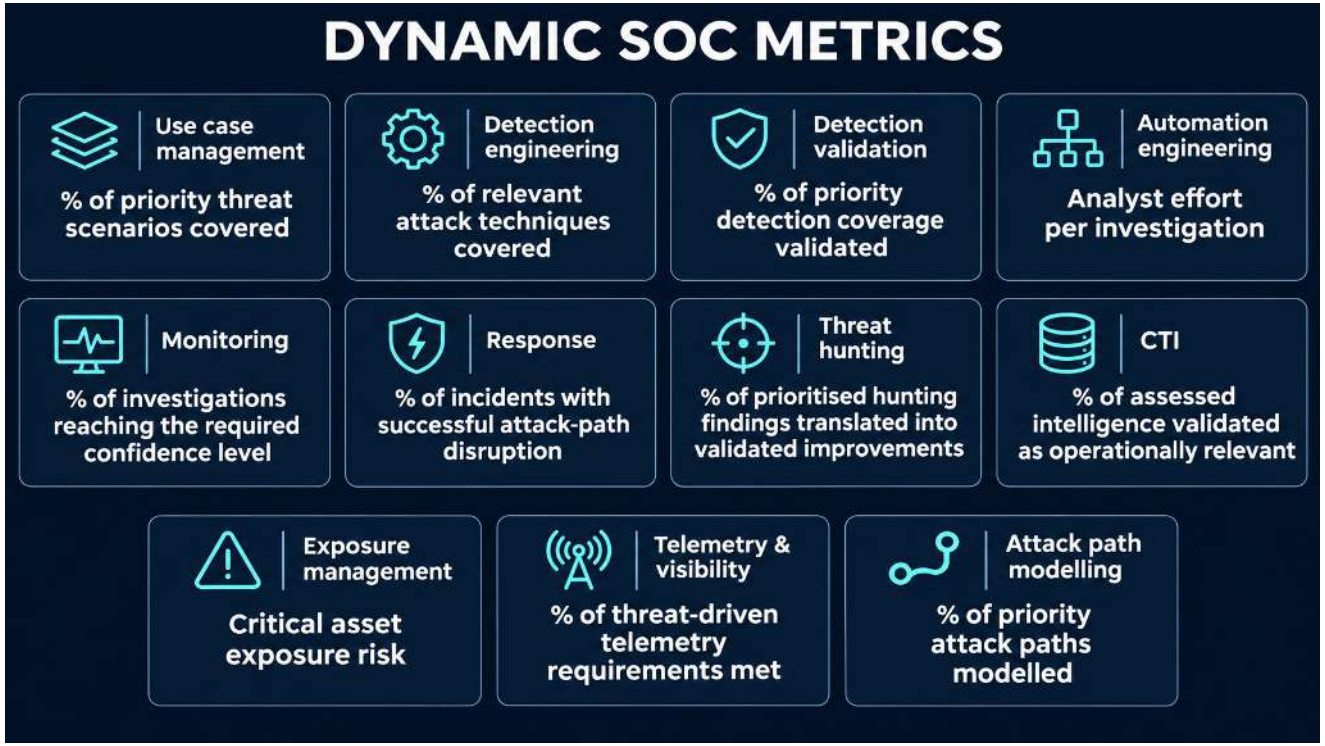


Dynamic security operations

Metrics

KPI focus changes:

- From optimisation of process to optimisation of threat relevance
- From MTTx to determining threat relevance
- From static to contextualised

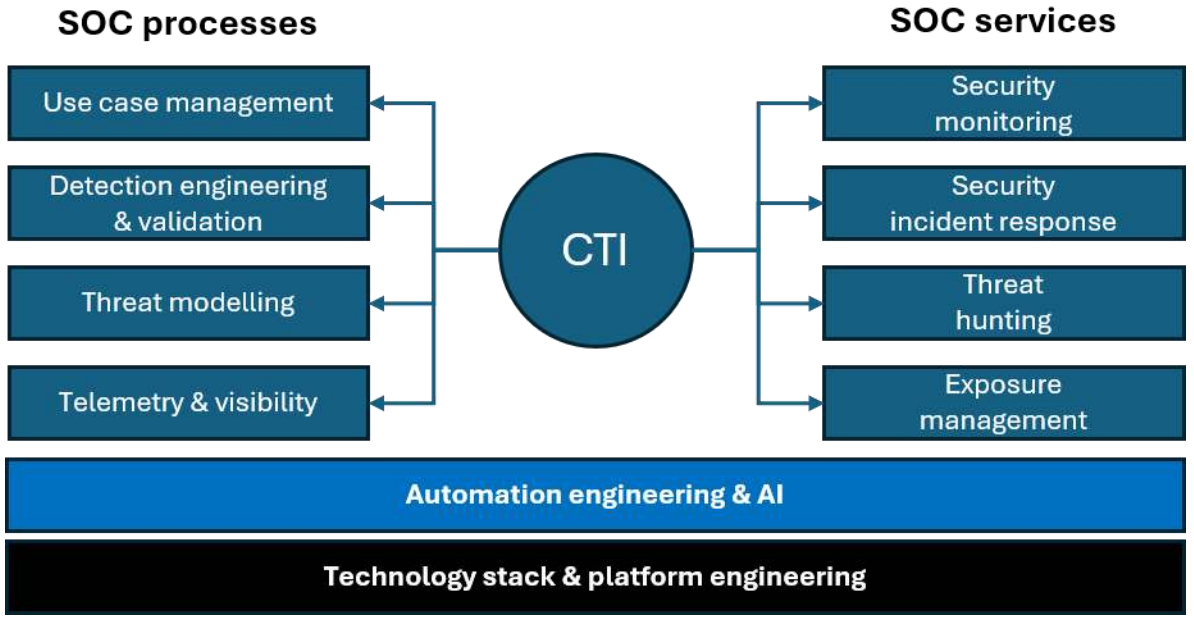


Dynamic security operations

Adaptive SOC operating model

The operating model shifts:

- CTI is central to security operations:
  - Contextualisation
  - Enrichtment
  - Direction
  - Prioritisation
- Automation engineering & AI as a horizontal layer supporting other capabilities
- Technology as an enablement layer
- Don’t forget the role of risk in this model:
  - Crown-jewel identification
  - Attack path prioritisation
  - Etc.



Summary

Key take-aways

- **SOC automation** is no longer optional
  - Attacks are accelerating through automation & AI
  - Vulnerable surfaces are expanding
  - Cyber defense (& SOC) automation are required to keep up
- **Many SOCs** do not have a defined way forward
  - The SAMM is a helpful resource to structure the approach on AI
  - Start with an AI adoption strategy, quantify progress

- **AI SOC** is not a goal, but a means to an end
- **An adaptive operating model** will leverage AI and automation in a bigger goal: matching adversary capabilities

Summary

SOC Maturity report

- The SOC maturity report is available on the SOC-CMM website
- The website also has a library of best practices and whitepapers

https://www.soc-cmm.com/



Rob van Os | Strategic SOC Advisor

rob@argos-csa.nl