The Future of Cyber Defense

"Redefining Next-Generation Security Operations"

Presentation by **Leonie Baranowski, Himanshu Chaudhary & Vishal Sharma**

22 April 2026

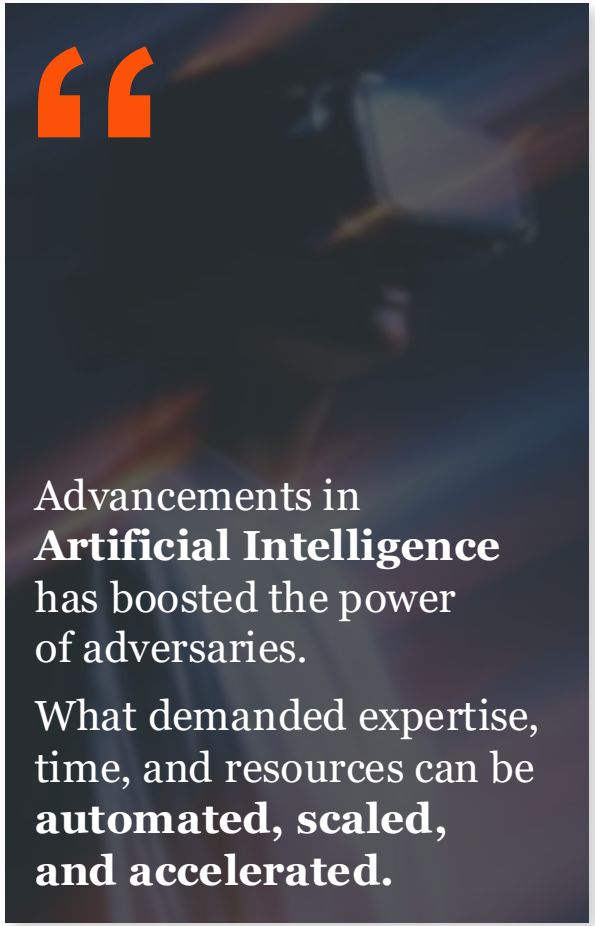
Your Speakers Today

Leonie Baranowski
Cyber Business Development Lead, PwC Germany
+49 171 5393229
leonie.baranowski@pwc.com

Himanshu Chaudhary
Cyber Defense Lead, PwC Germany
+49 1517 3059047
himanshu.chaudhary@pwc.com

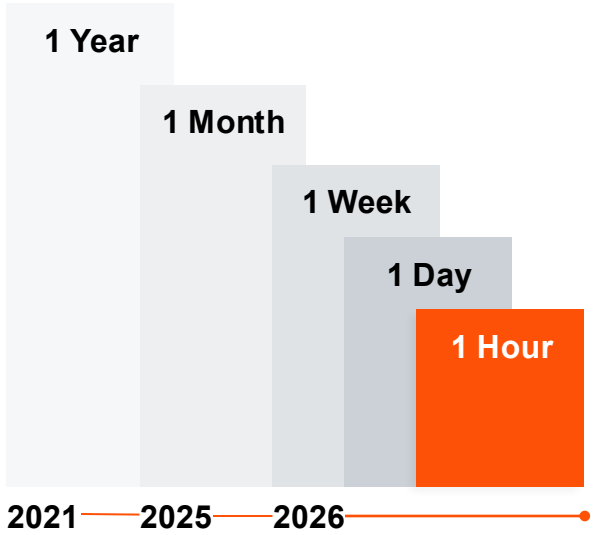
Vishal Sharma
Cyber Defense Lead, PwC Germany
+49 1517 2931922
vishal.s.sharma@pwc.com

AI is Changing the Rules of Cyber Defense – The Threat has Evolved



AI enables mature attackers to rapidly analyze CVEs, auto-generate exploits, and deploy at scale before patches are triaged, **massively increasing** the number of attacks taking place.

Time Needed To Exploit Zero Day Vulnerabilities*



*https://zerodayclock.com/

The New Accelerated, Adaptive, and Personalized Attack Lifecycle

200 x
Recon Speed through AI Assistance

Spear phishing
Campaigns are now generated at scale with personalized content.

<5 Mins
Between phishing click and credential theft.

Automated spear-phishing coupled with large-scale recon and working exploits, AI-driven attack paths pose an unavoidable threat.

Claude Mythos

When the Model becomes the Attacker,
Released April 2026

Autonomous Exploitation, No Human Supervision Required

Incredible Speed, Outpacing Human Defense

Anthropic's most advanced offensive-capable model that discovered previously overlooked bugs across operating systems, applications, and cryptographic libraries, the backbone and spine of all technical capabilities, highlighting the need for heightened defensive operations to maintain the current infrastructure.

What breaks first inside the cyber organisation

AI-augmented attacks do not just hit the perimeter – they strain the cyber organisation itself: its assumptions, its cadence,its people.

Source: CSA / SANS Mythos-ready briefing, April 2026 — risk register and CISO key takeaways.

Patch backlog explosion

Glasswing-style coordinated disclosures arrive in waves. Patch ops cannot absorb 40-vendor synchronised cycles.

CVE & threat intel cannot keep pace

AI-discovered zero-days outrun the CVE/KEV system. Detection content built on lagging intel is structurally late.

Simultaneous critical incidents

Multiple high-severity incidents in the same week is the new normal. Pre-authorised playbooks become survival, not maturity.

AI-grade phishing & social engineering

Industrial-scale, hyper-personalised campaigns. Awareness training alone is no longer a sufficient control.

Citizen coders & shadow agents

Agentic coding tools proliferate to non-developers. New asset classes appear daily — outside CMDB, outside scope.

Burnout as a strategic risk

Workload rises exponentially against flat headcount. Loss of senior expertise is unrecoverable on relevant timescales.

What is a SOC ?

A Security Operations Center is a centralized function that continuously monitors, detects, analyzes, and responds to cybersecurity threats across an organization's entire IT environment. It serves as the nerve center of an organization's cyber defense, combining people, processes, and technology to protect critical business assets around the clock.

SOC Core Capabilities

Log Collection	
CATEGORY	**SOURCES**
Network	Firewalls, IDS/IPS, NetFlow, DNS logs, Proxy logs, VPN logs
Endpoint	EDR, Antivirus, OS event logs, Host-based IDS
Cloud	Cloud trail logs, SaaS activity logs, CASB, Container logs
Identity	Active Directory, IAM, MFA logs, Privileged Access Management
Email	Email gateway logs, Anti-phishing tools, DLP alerts
Application	Web application firewalls, Application logs, Database activity logs
External	Threat intelligence feeds, OSINT, Dark web monitoring, Vulnerability scanners
Compliance	DLP alerts, Audit logs, Configuration management, Policy violation alerts

Detection

Building custom detection rules, correlation logic, and behavioral analytics within the SIEM **to identify threats** like lateral movement, privilege escalation, and data exfiltration.

Response

Executing **automated SOAR playbooks** that **enrich alerts** with threat intelligence, contain threats by **isolating endpoints or blocking IPs**, and **respond in seconds.**

Models Comparison

FACTOR	IN-HOUSE	OUTSOURCED	HYBRID
Cost	High	Low-Medium	Medium
Control	Full	Limited	Shared
Business Context	Deep	Shallow	Moderate
Scalability	Difficult	Easy	Flexible
Time to Deploy	Months	Weeks	Weeks-Months
Talent Dependency	Critical	Provider	Balanced
24/7 Coverage	Expensive	Included	Shared
Customization	Full	Limited	Moderate

The SOC exists to protect the organization by:

- **Monitoring :** Continuous 24/7 surveillance of the organization's digital environment
- **Detection:** Identifying threats, anomalies, and suspicious activities in real time
- **Investigation:** Analyzing and triaging security events to determine severity and scope
- **Response:** Containing, mitigating, and remediating confirmed security incidents
- **Recovery:** Restoring normal operations and applying lessons learned to strengthen defenses

Challenges with Traditional SOC

Traditional SOCs were often built to **satisfy compliance requirements rather than to actively defend against real threats.** Over time, this compliance-driven approach created **critical gaps across people, processes, and technology** resulting in **limited visibility, weak detection,** stale use cases, and poor data quality.

Strategic Mindset

Used Only for Compliance

The SOC was built to satisfy regulatory and audit requirements rather than actively detecting and responding to real cyber threats effectively.

People

Skilled Resource Shortage & High Turnover

Scarcity of qualified security analysts and high staff turnover create knowledge gaps, inconsistent operations, and constant recruitment and training burden.

Processes

Lack of Continuous Validation

Detection rules are never tested against real attack scenarios, leaving the SOC operation on assumptions rather than proven detection effectiveness.

Lack of Continuous Enhancement

Use cases and playbooks remain static after deployment, never updated to reflect evolving threats, causing detection capabilities to degrade.

Technology

Lack of Coverage

The SOC fails to monitor the client's full landscape cloud, OT, IoT, endpoints, and third parties.

Lack of Detection Capabilities

Use cases and playbooks remain static after deployment, never updated to match evolving threats and techniques.

Impact

Tool SPOC

Each tool to have its own SPOC/ Go-to-person

Operational Instability

Inconsistent investigations, longer response times, and missed incidents.

Unverified Detection Logic

High false positives/negatives, reducing analyst trust and increasing chances of evasion.

Detection Capability Decay

Failing to adapt to evolving TTPs causing gradual erosion in detection efficiency.

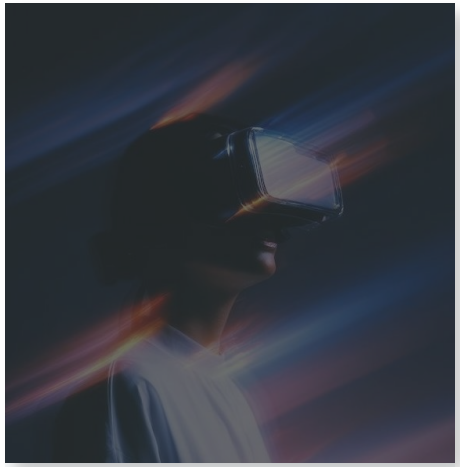
Blind Spots

Incomplete visibility enables attacker persistence and lateral movement.

Advanced Threats

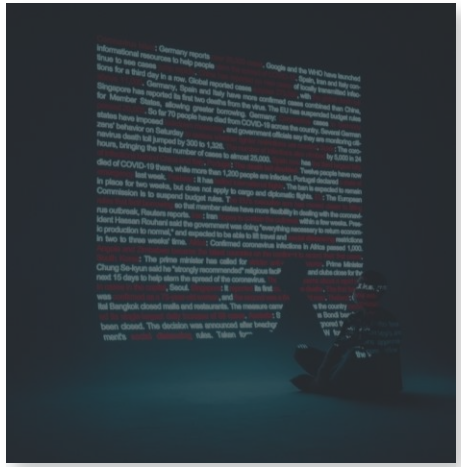
Modern attack techniques go through without detection, resulting in higher breach impact.

Five things every CISO must act on now



AI has already broken the offense – defense balance

Mythos-class models autonomously discover, weaponize and chain vulnerabilities at machine speed. The shift is structural — not a spike.

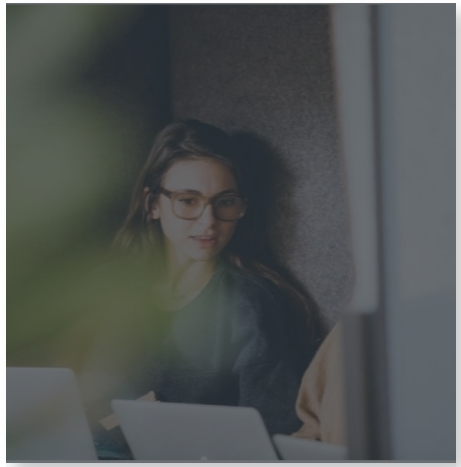


The traditional SOC will not survive in its current form

Compliance-led, alert-centric, human-paced operations cannot absorb the volume, speed and complexity of AI-augmented attacks.

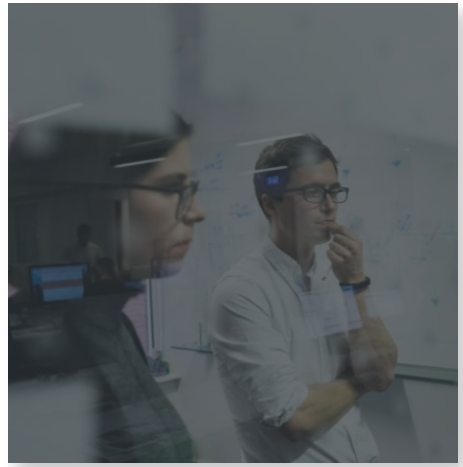
The cyber organization itself is being disrupted

Patch backlogs, CVE cadence, risk metrics, supply chain, analyst capacity — every assumption underneath your program is now under pressure.



Boards and regulators are already moving

ECB, BoE, BaFin and DORA scrutiny is reframing cyber resilience around exposure reduction, control validation and AI-grade response.

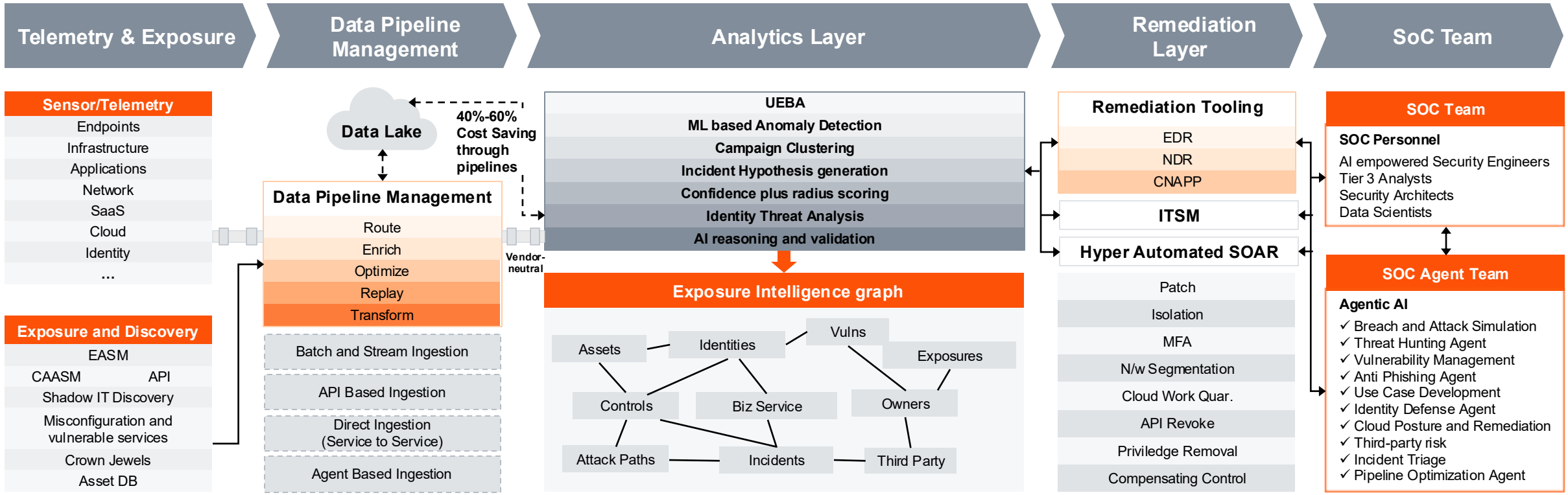


This is a 90-day decision, not a five-year roadmap

Aggressive plan, named owners, measurable outcomes. Status quo is the most expensive option on the table.

Sources: CSA / SANS, “The AI Vulnerability Storm — Building a Mythos-ready Security Program”, April 2026; ECB / BoE / BaFin supervisory communications, 2026.

Target Architecture for Cognitive SOC



Key Benefits

- Left Shift Architecture
- Micro Response at the edge
- Macro level detection and automated response
- Threat based and behavioral based detection and not symptom-based detection

Key Outcomes

- Reports
- Analytics
- Trends
- Dashboards
- Alerts
- Gap Analysis
- State Analysis

Design principles for future SOC

Left shift, edge response, central intelligence with Agentic orchestration

The attack & defense lifecycle

LEFT SHIFT

Reduce exposure before exploitation

ASM, hardening, patching, identity hygiene, AI-driven code review

EDGE RESPONSE

Contain at the point of impact

EDR / NDR / CNAPP enforce in milliseconds, micro-actions

CENTRAL INTELLIGENCE

Coordinate, learn, orchestrate

NG-SIEM, Analytics Layer, hunting, agent orchestration, macro response

The earlier you intervene, the cheaper the defense and the smaller the blast radius.

Our Four Phases to next generation Cyber Defense Maturity

SOC Assessment 01

- Review of the overall architecture to identify weaknesses, redundancies, and areas for optimization
- Coverage review of logs, monitoring and alerts for critical services
- Detection and incident-response maturity scoring
- In-depth analysis of the security infrastructure to uncover structural gaps in people, processes, and technology

Attack Surface Management 02

- Establish visibility across internal, external, cloud, identity, application, and third-party attack surface
- Identify exposed assets, misconfigurations, shadow IT, vulnerable services and unmanaged entry points
- Prioritized exposures based on exploitability, potential business impact, and attacker interest
- Create workflows to route prioritized findings into remediation activities

Threat Hunting 03

- Introduce threat hunting aligned to priority adversary behaviors, high-risk assets, and business-critical services
- Use hypotheses driven by threat intelligence, attack surface findings, and incident learning
- Validate whether existing detection, telemetry, and controls can identify relevant attacker activity
- Translate findings into concrete remediation actions across architectural gaps, coverage expansion and response flows

Maturing SOC into Next Generation Defense 04

- From reactive to proactive defense
- Strengthen detections with behavioral detections using ML
- Introduce end-to-end automation and orchestration while leveraging AI
- Introduce continuous validation
- Introduce virtual team members to support specialized tasks

How PwC Can Support: **Call to Action Offers**

Threat Hunting

Identify coverage gaps from logs and detection capabilities and quality perspective

SOC Assessment / Architecture Review

Evaluate SOC maturity and architecture to identify strengths, gaps, and improvement priorities

Incident Response Readiness

Assess preparedness to respond effectively to cyber incidents before a real crisis occurs

30 Minutes 1-to-1 Meeting

Focused one-on-one session with a PwC cyber defense expert on your priority topics

Cyber Defense Quarterly Community Exchanges

Peer discussions and expert insights, and ongoing forums for best practices and emerging cyber defense trends


Q&A

Thank you

pwc.com

Our Capabilities

Cyber Defense Target Strategy & Operating Model

From ad-hoc alerts to autonomous defense architecting an AI-ready SOC for tomorrow, today.

SOC Health & Coverage Assessment

Reveal the blind spots quantify your detection health with ATT&CK-driven, data-first analytics.

DORA Ready Cyber Defense

Turn regulation into resilience compliant by design, secure by default.

NIS Ready Cyber Defense

Turn regulation into resilience compliant by design, secure by default.

Use Case Foundry as a Service

Forging high-fidelity, AI-ready detections at scale from threat intel to production use cases on tap.

Cyber Defense Tech Capabilities Implementation

Orchestrating the next-gen cyber stack so every signal becomes actionable intelligence.

Managed Cyber Defense

24/7 threat hunting and response a next-gen SOC as an extension of your team.

SOC Engineer as a Service

Elite SOC engineering on demand infrastructure, playbooks, and pipelines as code.

Onboarding Factory

TBD

Cyber Defense Operations & Cost Optimization

Do more with fewer alerts precision-engineered SOC efficiency at scale.

AI Agents & Machine Learning Models

LLM-powered defense autonomous cyber agents with guardrails built-in.

Breach & Attack Simulation

Assume breach, prove resilience continuous purple-team in a digital twin of your estate.

Data Pipeline Management

Fueling AI-ready cyber analytics clean, normalized, and cost-optimized security data.