WHITE PAPER



AI-FIRST SOC MODERNISATION: AN INFOSYS THOUGHT LEADERSHIP BLUEPRINT, BUILT WITH MICROSOFT SECURITY AND MICROSOFT SENTINEL

BUILDING SCALABLE, INTELLIGENT, AND RESILIENT SECURITY OPERATIONS FOR THE AI ERA

Infosys
Navigate your next

Executive Summary

Security Operations Centres (SOCs) are shifting from reactive monitoring and manual triage toward intelligence-led, cloud-native, and AI-assisted operating models. Enterprises are facing rising alert volumes, fragmented telemetry, hybrid and multi-cloud complexity, analyst fatigue, compliance pressure, and growing pressure to detect and respond faster.

Infosys enables SOC modernisation as an enterprise transformation, not a tooling upgrade. It effectively means working across people, process, technology, governance, and operating model, along with security advisory, SOC maturity assessment, telemetry rationalisation, SIEM (Security Information and Event Management) modernisation, detection engineering, automation, managed security operations, analyst enablement, and continuous optimisation.

Microsoft Security provides the foundation of technology for this transformation. Microsoft Sentinel serves as the cloud-native SIEM/SOAR (Security Orchestration, Automation, and Response) foundation for centralised detection, investigation, threat hunting, analytics, automation, and response, across Microsoft, non-Microsoft, hybrid, multi-cloud, and third-party environments. Around it, Microsoft Defender XDR (Extended Detection and Response), Entra, Purview, Security Copilot, Logic Apps, Threat Intelligence, Microsoft Fabric, and the Sentinel Data Lake cover identity, data governance, AI-assisted response, and automation, strengthening the end-to-end SOC modernisation ecosystem. Section 5 walks through what each one does.

Infosys Cyber Next complements this modernisation journey with accelerators for posture visibility, AI-assisted workflows, reusable playbooks, exposure-led prioritisation, connector acceleration, and continuous SOC evolution. Together, Infosys expertise, Microsoft Security capabilities, and Cyber Next accelerators help enterprises build a scalable, resilient, AI-first SOC aligned to business risk and operational maturity.

The Shifting SOC Operating Model

Traditional SOC operations were largely reactive and dependent on manual threat hunting, fragmented tools, rule-based detection, and analyst-driven triage. As threats grow more sophisticated and AI-enabled attacks accelerate, that model becomes harder to scale.

SOC modernisation helps organisations move from fragmented, reactive operations to an intelligence-led model built on unified visibility, automation, AI-assisted response, threat intelligence, strong governance, and continuous posture improvement.

The modern SOC's role is expanding too. It is no longer limited to alert monitoring and incident response. It has to bring together identity, endpoint, email, cloud, SaaS, network, data, threat intelligence, compliance, and business risk context, so security leaders can prioritise what matters most.



External Document © 2026 Infosys Limited

Enterprise Challenges Driving SOC Modernisation

Enterprises are modernising SOC operations to address structural challenges that limit visibility, slow investigation, increase analyst workload, and reduce confidence in detection and response outcomes.

Traditional SOC operations rely heavily on manual threat hunting, which often leads to alert fatigue. A 2025 BCG study found that although nearly all organisations are now aware of AI-driven risk, only a limited number are responding with the urgency required: around 60 per cent of leaders believe they have already experienced an AI-driven attack; yet merely seven per cent of organisations have implemented AI-powered defences, although 88 per cent are planning to.

SOC modernisation replaces reactive, manual effort with automated, AI-driven defences, so organisations can secure a wider and more sophisticated threat surface proactively rather than catching up after the fact.

SOC Modernisation Pressure Points

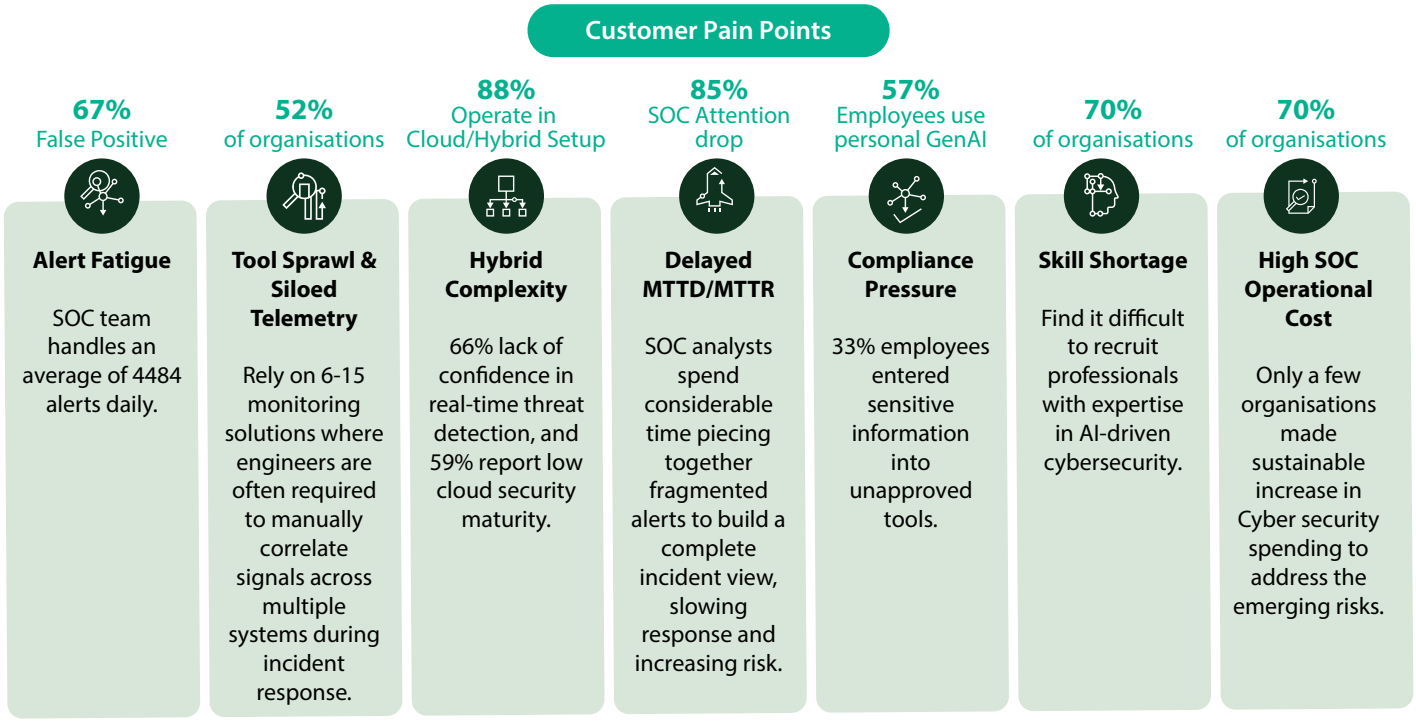


Fig. 1: Customer pain points across alert volume, tooling, cloud complexity, compliance, skills, and cost

Challenge	Business/SOC Impact
Alert fatigue and false positives	High alert volumes make it difficult for analysts to identify real threats, increasing the risk of missed compromises and delayed investigation.
Tool sprawl and siloed telemetry	Fragmented security tools create visibility gaps and require manual correlation across systems during incident response.
Skills shortage	Limited availability of experienced SOC analysts makes it difficult to manage increasing threat complexity and AI-driven attack patterns.
Delayed MTTD/MTTR (MTTD: Mean Time to Detect; MTTR: Mean Time to Respond)	Manual processes and limited data correlation slow detection, investigation, and response.
Cloud and hybrid complexity	Hybrid and multi-cloud environments make consistent monitoring, controls, and real-time detection more difficult.
Compliance pressure	Regulatory expectations require continuous monitoring, stronger reporting, governance, and evidence-based controls.
High SOC operational cost	Infrastructure, licensing, and workforce expenses create inefficiencies in traditional SOC operating models.

External Document © 2026 Infosys Limited

Why SOC Modernisation Is Needed

- Unified visibility across hybrid, multi-cloud, Microsoft, and non-Microsoft environments
- AI-assisted triage and intelligent correlation to reduce noise and improve detection accuracy
- Automation and SOAR-led response to reduce manual effort and accelerate remediation
- Improved MTTD and MTTR through real-time analytics, integrated workflows, and response playbooks
- Cloud-native scalability without heavy infrastructure dependency
- Governance, compliance, and evidence-based monitoring aligned with regulatory expectations
- Proactive resilience through threat intelligence, advanced hunting, continuous tuning, and posture improvement

Market Trends Shaping the AI-First SOC

Security operations are being reshaped by AI-enabled threats, fragmented telemetry, hybrid cloud complexity, identity and data risk, and rising expectations for faster response. These shifts are pushing SOC modernisation beyond simple tool replacement, towards an intelligence-led operating model built on visibility, automation, threat context, and continuous improvement.

What Leading Organisations Do Differently

Market Force	What's Changing	SOC Implication
AI-led threat environment	Agentic AI adoption is increasing across users and developers, creating new attack surfaces and governance challenges.	SOCs need AI-assisted triage, automated enrichment, stronger monitoring, and governed response workflows.
Shadow AI and expanding attack surface	Employees are increasingly using personal GenAI tools, increasing the risk of sensitive information entering unapproved platforms.	SOCs must integrate XDR, data protection, identity risk, and governance signals to detect and manage emerging exposure.
Hybrid and multi-cloud complexity	Enterprises operate across on-premises, cloud, SaaS, third-party, and non-Microsoft environments, making centralised visibility harder.	Cloud-native SIEM/SOAR becomes essential for scalable ingestion, detection, hunting, investigation, and response.
Identity and data as SOC signals	AI agents and machine actors introduce new identity and access management (IAM) challenges, including credential automation and policy-driven authorisation.	Zero Trust, Conditional Access, identity risk, and data classification and governance must become part of SOC workflows.
Future-ready cyber resilience	Threat intelligence, exposure management, and quantum-readiness are becoming long-term SOC priorities.	SOC modernisation should include proactive threat anticipation, crypto-agility planning, and continuous risk reduction.

Market Signals Reinforcing SOC Modernisation

Gartner: Agentic AI adoption is creating new attack surfaces and identity governance challenges for SOC teams. Gartner-related research also finds that 57 per cent of employees use personal GenAI accounts for work, and 33 per cent enter sensitive information into unapproved tools. Separately, a Forrester Total Economic Impact study commissioned by Microsoft found Sentinel adoption delivered a 234 per cent ROI, supporting the case for cloud-native SIEM/SOAR modernisation. Industry cloud security studies show hybrid and multi-cloud environments continuing to increase visibility, telemetry, and response complexity. On the horizon, Gartner projects that quantum computing could make current asymmetric encryption methods ineffective by 2030, making crypto-agility a long-term SOC priority; Microsoft frames the corresponding quantum-safe migration as a multi-year transformation that needs early planning.

Microsoft Sentinel provides the cloud-native SIEM/SOAR foundation for this modernisation journey, while Infosys brings the advisory, migration, detection engineering, automation, governance, and managed operations capabilities needed to turn platform capability into enterprise-scale SOC outcomes.

External Document © 2026 Infosys Limited

Microsoft Security and Sentinel as the Technology Foundation

Microsoft Security provides a cloud-native technology foundation for modern SOC transformation. Microsoft Sentinel, Microsoft's cloud-native SIEM and SOAR platform, acts as the backbone for centralised monitoring, detection, investigation, hunting, automation, and response, across hybrid, multi-cloud, Microsoft, and third-party environments.

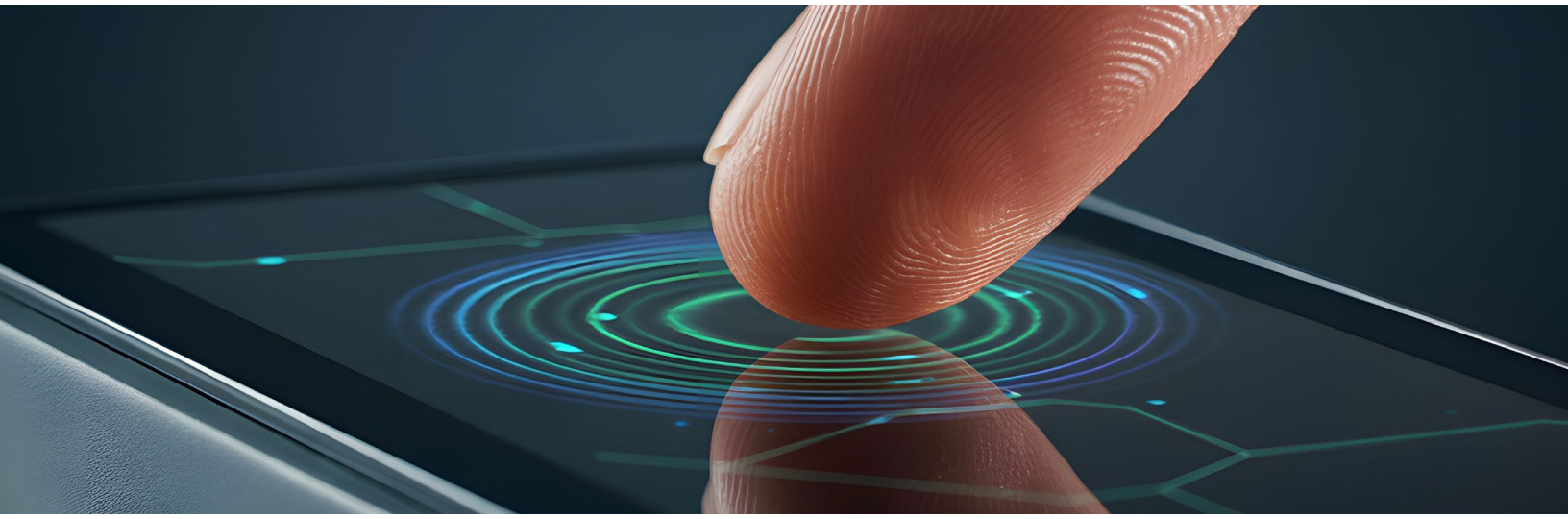
The broader Microsoft Security stack strengthens this foundation through XDR, identity protection, data security, governance, generative AI assistance, threat intelligence, automation, and scalable security data management.

Foundation Area	Microsoft Capability	SOC Modernisation Relevance
Cloud-native SIEM/SOAR	Microsoft Sentinel	Centralised detection, investigation, hunting, automation, response, UEBA (User and Entity Behaviour Analytics), threat intelligence, and scalable analytics
Extended detection and response	Microsoft Defender XDR	Correlated incidents across endpoints, identities, email, cloud apps, and workloads
Identity security	Microsoft Entra	Strong authentication, conditional access, identity protection, and least-privilege controls
Data security and governance	Microsoft Purview	Sensitive data classification, protection, monitoring, compliance, insider risk, and responsible AI governance
Generative AI for SecOps	Microsoft Security Copilot	Incident summarisation, investigation acceleration, insight generation, and analyst productivity
Automation and orchestration	Logic Apps and Sentinel Playbooks	Repeatable enrichment, notification, containment, remediation, and response orchestration
Threat context	Microsoft Threat Intelligence	Prioritised detection, investigation enrichment, and proactive response to emerging threats
Scalable security data platform	Microsoft Fabric and Sentinel Data Lake capabilities	Security data centralisation, longer retention, analytics, and future AI-led SOC use-cases

Infosys Perspective: SOC Modernisation at Enterprise Scale

Infosys treats SOC modernisation as an operating-model transformation. Platform modernisation matters, but its value shows only when an organisation also modernises its telemetry strategy, use-case library, detection engineering practices, automation model, governance, skills, and continuous improvement cadence.

Infosys brings the transformation blueprint, delivery scale, migration experience, Cyber Defence Centre operations, detection engineering capability, playbook industrialisation, analyst enablement, and governance model needed to turn Microsoft Security capabilities into measurable SOC outcomes.



External Document © 2026 Infosys Limited

Infosys Approach to Enterprise SOC Modernisation

Infosys approaches SOC modernisation as an enterprise operating-model transformation, not only a technology implementation. The focus is helping organisations rationalise security telemetry, modernise SIEM capabilities, improve detection coverage, automate response, strengthen governance, and operate SOC capabilities at scale, using Microsoft Sentinel and the broader Microsoft Security stack.

Modern SOC Capability	Infosys Approach	Key Microsoft Anchors and Value
Better threat detection and faster response	Integrate UEBA-driven insights into Cyber Defence Centre operations for continuous monitoring, intelligent triage, alert-noise reduction, and automated containment and remediation	Microsoft Sentinel UEBA, Analytics Rules, SOAR, Logic Apps Playbooks: faster detection, fewer false positives, improved MTTD/MTTR
Intelligent, data-driven decisions	Enable governed ingestion, faster connector onboarding, scalable integration, contextual enrichment, rule tuning, and AI-assisted playbook generation	Sentinel Data Connectors, Analytics Rules, UEBA, SOAR, Logic Apps, Threat Intelligence: better signal quality and prioritised response
Structured SIEM migration	Support phased migration from legacy SIEM platforms through the 4D framework, Discover (map existing tools and data), Design (plan the target architecture), Deliver (migrate and build detections), and Defend (validate and operate), with use-case mapping, KQL (Kusto Query Language) optimisation, and alignment to MITRE ATT&CK, the industry-standard catalogue of attacker tactics and techniques	Sentinel, KQL, Data Connectors, Analytics Rules, UEBA, SOAR, Threat Intelligence, MITRE-aligned content: lower migration risk and improved coverage
Future-ready cybersecurity platform	Combine posture visibility, intelligent protection, proactive prevention, responsible AI governance, standardised playbooks, and Zero Trust-aligned controls	Microsoft Security stack, Sentinel, Fabric, Sentinel Data Lake, Purview, Zero Trust, AI agents, SOAR, DLP (Data Loss Prevention), SASE (Secure Access Service Edge), third-party platforms: unified and governed cyber defence
Continuous SOC innovation	Drive continuous improvement through Microsoft collaboration, reference architectures, migration accelerators, Sentinel-led maturity frameworks, MDASH (Microsoft's multi-model agentic scanning harness, which discovers and validates exploitable code vulnerabilities)-led exposure management, Security Copilot, Topaz Fabric agents (AI agents from Infosys's own Topaz Fabric platform, which powers Cyber Next automation), and analyst enablement	Sentinel, Security Copilot, Defender capabilities, Threat Intelligence, SOAR, Topaz Fabric agents, vulnerability and exposure integrations: a scalable, self-evolving SOC

A modern SOC needs governed telemetry, high-quality detections, automation, exposure-aware prioritisation, and a continuous improvement model that balances AI assistance with human expertise, not platform migration alone.



External Document © 2026 Infosys Limited

Cyber Next as a 3P Accelerator Layer

Infosys Cyber Next supports SOC modernisation across three accelerator dimensions: Posture, Protect, and Prevent. Within the broader Infosys SOC modernisation approach, it helps improve visibility, strengthen protection workflows, and enable proactive prevention across Microsoft and non-Microsoft security environments.

Posture	Protect	Prevent
Observability | Exposure insights | Risk prioritisation	Detection | Triage | Investigation | Response	Playbooks | Hunting | Remediation | Recurrence reduction

Cyber Next Dimension	Role in SOC Modernisation	Customer Value
Posture	Enables CISO (Chief Information Security Officer)-level observability, exposure insights, security context, control-gap visibility, and risk prioritisation across Microsoft and non-Microsoft environments	Improved visibility into business risk, prioritised remediation, and stronger posture management
Protect	Supports AI-assisted triage, detection engineering, incident enrichment, managed SOC workflows, and integrated investigation across Microsoft Sentinel, Defender XDR, and third-party tools	Faster detection, improved analyst efficiency, reduced alert noise, and stronger operational resilience
Prevent	Enables reusable playbooks, automated response patterns, proactive threat hunting, exposure-led remediation, and governance-led controls	Fewer repeat incidents, faster containment, proactive defence, and measurable SOC maturity improvement.

Infosys modernisation and managed SOC services put the 3P model into practice through SIEM migration, automation, governance, analyst enablement, and continuous improvement.

Reference Architecture

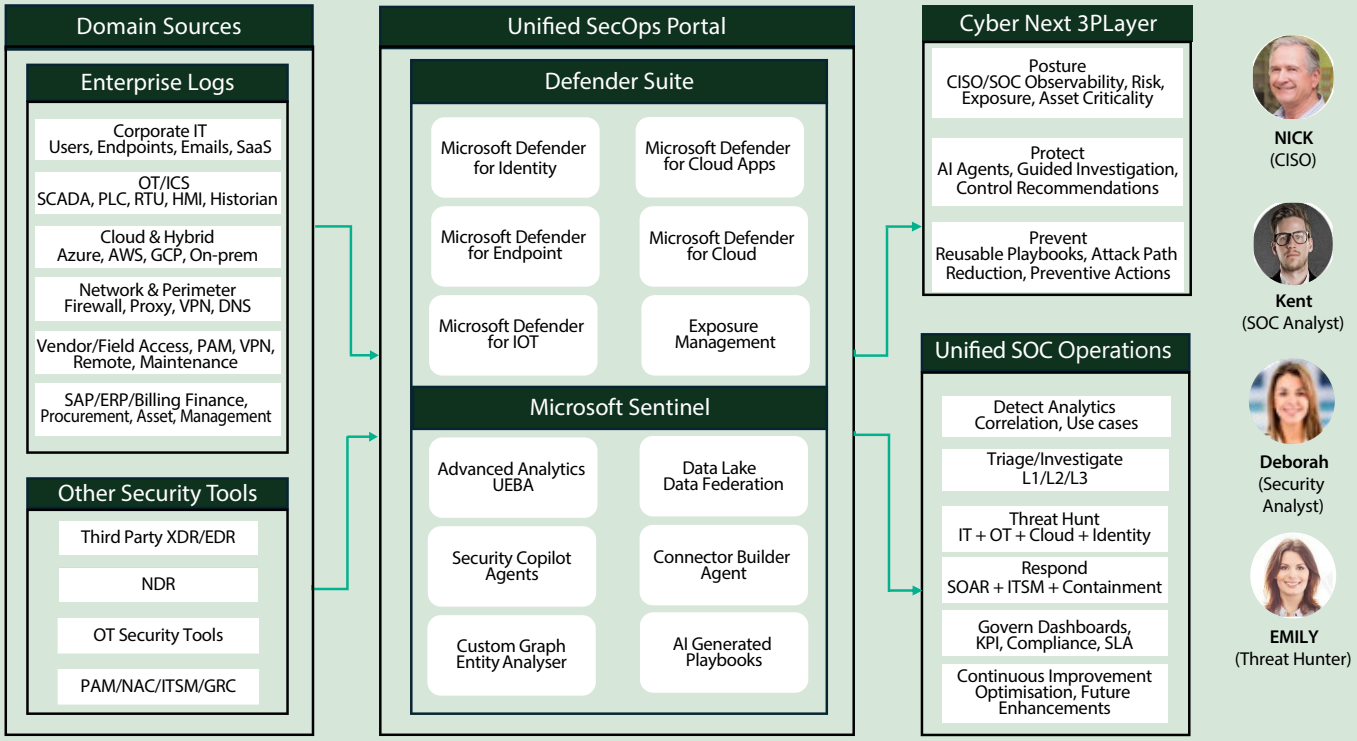


Fig. 2: Domain sources, the unified SecOps portal, and Cyber Next's 3P layer, from raw telemetry through to governed SOC operations

External Document © 2026 Infosys Limited

Infosys 5-Step SOC Modernisation Framework

SOC modernisation needs a phased roadmap that balances business risk, operating-model maturity, telemetry readiness, detection coverage, automation potential, governance, and continuous improvement, not just tool deployment.

5-Step SOC Modernisation Framework

Automate with AI & Playbooks
Deploy SOAR, automate repetitive tasks, introduce AI-driven triage, enrichment, and response workflows

Operate and Continuously Optimise
Establish 24×7 operations, track KPIs (MTTD, MTTR), continuously tune detections, expand automation, and onboard new data



Modernise SIEM
Implement cloud-native SIEM, migrate and optimise use-cases, align detections with threat frameworks, enrich with threat intelligence

Assess Maturity
Evaluate current SOC across data, tools, detections, processes, and skills; identify gaps in visibility, coverage, and response

Rationalise Tools and Data
Consolidate overlapping tools, eliminate silos, onboard key data sources, and standardise data ingestion

Fig. 3: The five-step path from assessing maturity through to continuous optimisation

Step	Key Actions	Customer Decision	Expected Outcome
Assess maturity	Evaluate current SOC across data, tools, detections, processes, skills, and governance; identify visibility, coverage, and response gaps	Define current maturity level and prioritise transformation areas based on risk and business impact	Clear baseline and prioritised modernisation roadmap
Rationalise tools and data	Consolidate overlapping tools, eliminate silos, onboard key data sources, standardise ingestion, and define retention strategy	Decide target architecture, consolidation approach, and data strategy	Reduced complexity, improved visibility, and lower operational cost
Modernise SIEM and detections	Implement cloud-native SIEM, migrate and optimise use-cases, map detections to frameworks, enrich with threat intelligence, and tune rules	Choose phased or full migration and prioritise high-value detection use-cases	Improved detection accuracy, better coverage, and faster onboarding
Automate with AI and playbooks	Deploy SOAR, automate repetitive tasks, introduce AI-assisted triage, enrichment, and response workflows	Identify high-impact automation use-cases and define a responsible AI adoption level	Reduced manual effort, faster response, and consistent incident handling
Operate and continuously optimise	Establish 24×7 operations, track KPIs, tune detections, expand automation, onboard new data, and review governance	Define operating model, internal, MDR (Managed Detection and Response), or hybrid, and a continuous improvement strategy	Scalable, continuously improving SOC with stronger resilience

External Document © 2026 Infosys Limited

From AI-Assisted to AI-Led SOC Operations

As SOCs mature, the next phase of transformation is the shift from AI-assisted operations to AI-led security. Today, AI mainly supports analysts by automating repetitive tasks like alert triage, enrichment, summarisation, and investigation. Over time, organisations will move toward agentic AI models, where AI systems can correlate data, recommend actions, and initiate controlled response workflows with human oversight.

AI-Led SOC Maturity Progression

Maturity Stage	Description	Human Role
AI-assisted SOC	AI supports incident summarisation, enrichment, triage, and investigation acceleration	Analysts validate insights and drive response
AI-augmented SOC	AI recommends prioritisation, response actions, playbooks, and exposure-led remediation	Analysts approve, tune, and govern response
AI-led SOC	Agentic workflows coordinate detection, response, governance, and continuous improvement across tools and data platforms	Humans provide oversight, exception handling, threat hunting, and decision governance

AI-led SOC operations need mature telemetry, detections, automation, governance, and operating-model foundations to run safely. Enterprises should begin modernising now to prepare for scalable, accountable, AI-first security operations.

SOC Modernisation Readiness Checklist

The readiness checklist gives a practical way to assess current maturity, identify modernisation priorities, and define a phased roadmap.

SOC Modernisation Readiness Checklist

Data and Telemetry
Ensure comprehensive, high-quality, and normalised telemetry across all critical environments for end-to-end visibility

SIEM /Tool Rationalisation
Consolidate fragmented security tools into a unified SIEM/XDR platform to reduce complexity and improve visibility

Detection Engineering Maturity
Develop and continuously refine intelligence-driven detections aligned with threat frameworks for higher accuracy and coverage



Automation and Playbook
Implement standardised and AI-driven playbooks to automate triage, investigation, and response at scale

Analyst Skills and Operating Model
Build a skilled workforce and a well-defined operating model to effectively leverage modern SOC technologies and processes

Governance, Compliance and Responsible AI
Establish strong governance and Responsible AI controls to ensure secure, compliant, and trustworthy operations

Cost, Risk, and Business Alignment
Align SOC investments with business priorities and risk appetite while optimising cost and demonstrating measurable value

Fig. 4: Six readiness dimensions, from data and telemetry through to governance and business alignment

External Document © 2026 Infosys Limited

Data and Telemetry Readiness

- Are all essential data sources onboarded across identity, endpoint, cloud, network, SaaS, and data?
- Is data normalised, enriched, and mapped to a common schema?
- Do you have visibility across hybrid and multi-cloud environments?

SIEM/Tool Rationalisation Readiness

- Are security tools consolidated to reduce duplication and silos?
- Is there a unified SIEM/XDR platform strategy?
- Are legacy SIEM dependencies identified for phased migration?

Detection Engineering Maturity

- Are detections aligned to frameworks such as MITRE ATT&CK?
- Is there a process for continuous rule tuning and validation?
- Are detections enriched with threat intelligence and business context?

Automation and Playbook Readiness

- Are repetitive SOC tasks automated through playbooks or runbooks?
- Is there integration across tools for end-to-end response?
- Are AI-assisted or adaptive playbooks used for faster response?

Analyst Skills and Operating Model Readiness

- Do analysts have skills in modern SIEM, XDR, cloud, and AI-assisted security operations?
- Is there a defined SOC operating model, such as 24×7, MDR, or hybrid?
- Are continuous training and upskilling programmes in place?

Governance, Compliance, and Responsible AI Readiness

- Are controls aligned with regulatory and compliance expectations?
- Is there governance for data access, monitoring, reporting, and evidence management?
- Are Responsible AI guardrails defined for privacy, data protection, and human oversight?

Cost, Risk, and Business Alignment

- Is SOC investment aligned with business priorities and risk appetite?
- Are cost optimisation levers such as retention, licensing, and ingestion strategy defined?
- Are KPIs such as MTTD, MTTR, coverage, false-positive rate, automation rate, and ROI defined?



External Document © 2026 Infosys Limited

Conclusion

SOC modernisation is no longer optional. Rising alert volumes, increasing attack sophistication, hybrid complexity, AI-enabled threat patterns, and analyst fatigue are making traditional, manual SOC operations unsustainable.

Infosys, working with Microsoft, helps enterprises turn SOC modernisation strategy into execution: combining Microsoft Sentinel and the broader Microsoft Security stack with advisory, SIEM modernisation, detection engineering, automation, managed operations, governance, and continuous improvement capabilities.

Cyber Next further accelerates this journey across Posture, Protect, and Prevent, helping enterprises improve visibility, strengthen protection workflows, and enable proactive prevention, while keeping Microsoft Sentinel as the platform foundation.

The path to an AI-first SOC begins with disciplined modernisation today. Enterprises should start with a structured SOC assessment and roadmap to identify current-state gaps, prioritise high-value use-cases, rationalise telemetry, modernise SIEM capabilities, and establish the operating foundations that scalable, resilient, governed, AI-led security operations need.

References

1. BCG. AI Raising the Stakes in Cybersecurity. https://www.bcg.com/publications/2025/ai-raising-stakes-in-cybersecurity
2. IBM. Alert Fatigue Reduction with AI Agents. https://www.ibm.com/think/insights/alert-fatigue-reduction-with-ai-agents
3. IBM. Future IT Operations: Unifying Applications and Infrastructure. https://www.ibm.com/think/insights/future-it-operations-unifying-applications-infrastructure
4. Cribl. Microsoft Sentinel SIEM Integration. https://docs.cribl.io/stream/usecase-azure-sentinel/
5. Forrester Consulting / Palo Alto Networks. Total Economic Impact of Cortex XSIAM. https://tei.forrester.com/go/PaloAltoNetworks/CortexXSIAM/index.html?lang=en-us
6. Virtualization Review. Report: Cloud Complexity Outpaces Security Defenses as Multi-Cloud Becomes the Norm. https://virtualizationreview.com/articles/2026/01/27/report-cloud-complexity-outpaces-security-defenses-as-multi-cloud-becomes-the-norm.aspx
7. Gartner. Gartner Identifies the Top Cybersecurity Trends for 2026. https://www.gartner.com/en/newsroom/press-releases/2026-02-05-gartner-identifies-the-top-cybersecurity-trends-for-2026
8. Fortinet 2026 Cloud Security Report 2026-fortinet-cloud-security-report.pdf
9. Microsoft Learn. Microsoft Sentinel Overview. https://learn.microsoft.com/en-us/azure/sentinel/overview
10. Microsoft Learn. Microsoft Sentinel in the Microsoft Defender Portal. https://learn.microsoft.com/en-us/azure/sentinel/microsoft-sentinel-defender-portal
11. Microsoft Security Blog. Microsoft Sentinel Delivered 234% ROI According to New Forrester Study. https://www.microsoft.com/en-us/security/blog/2024/03/19/microsoft-sentinel-delivered-234-roi-according-to-new-forrester-study/
12. Microsoft Learn. Security Copilot Included Experiences. https://learn.microsoft.com/en-us/copilot/security/security-copilot-inclusion
13. Microsoft Learn. Microsoft Sentinel UEBA. https://learn.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics
14. Microsoft Learn. Microsoft Sentinel Migration. https://learn.microsoft.com/en-us/azure/sentinel/migration
15. Microsoft Learn. Microsoft Sentinel Threat Detection. https://learn.microsoft.com/en-us/azure/sentinel/threat-detection
16. Microsoft Learn. Microsoft Sentinel Roles. https://learn.microsoft.com/en-us/azure/sentinel/roles
17. Microsoft Tech Community. Microsoft Sentinel: SOAR Through the SIEM, Begin with the Basics. https://techcommunity.microsoft.com/blog/fasttrackforazureblog/microsoft-sentinel---soar-through-the-siem-begin-with-the-basics/3990142

External Document © 2026 Infosys Limited

About the Authors



Aparna Bhargavi Challa
Senior Associate Consultant

Aparna Bhargavi Challa is a Product Manager with over six years of experience in the SaaS industry, leading initiatives in product strategy, innovation, and solution delivery. Expertise spans customer-centric product development, stakeholder alignment, and the execution of scalable digital solutions.



Meena Kumari Chatla
Senior Consultant

Meena Kumari Chatla is a Senior Consultant serving as a Sentinel Implementation Engineer, bringing more than a decade of expertise in security operations, software development, and quality assurance.

For more information, contact askus@infosys.com

Infosys
Navigate your next

© 2026 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.