

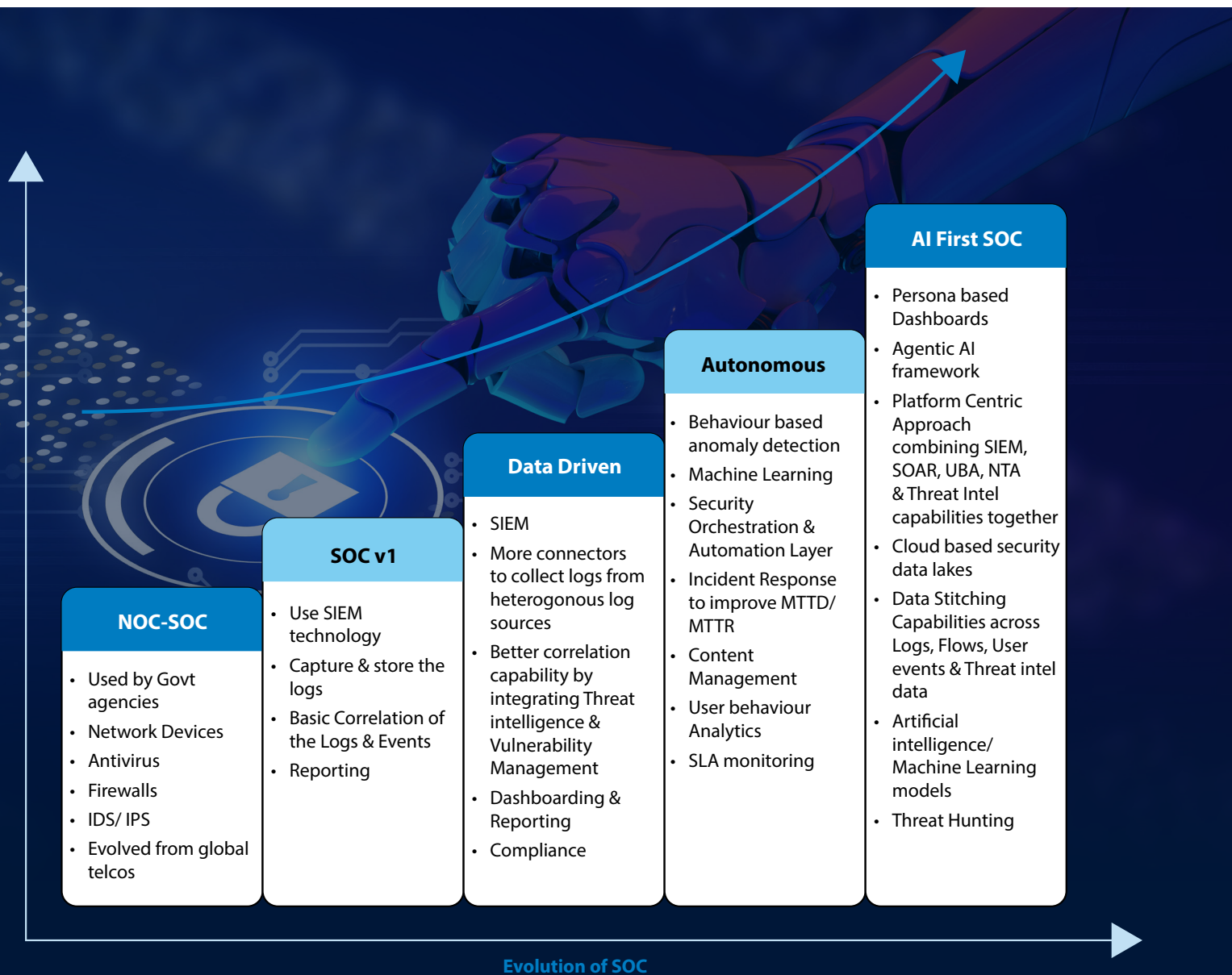
INFOSYS AI-FIRST SOC



Evolution of 5th Generation AI-First SOC

High volume of alerts and increasing sophistication of cyber threats need a paradigm shift in running enterprise Security Operations Center (SOC). A McKinsey report suggests that damage from cyberattacks could amount to about \$10.5 trillion annually by 2025—a 300 % increase from 2015 levels. Enterprises currently heavily rely on expensive, high in demand and difficult to retain human analysts.

AI for Cyber Defense emerges as a strategic imperative to address this growing threat. *Infosys Cyber AI aims to amplify the defender potential by processing and analyzing vast volumes of data.* AI enables organizations to pre-empt cyberattacks, minimizing potential disruptions and discovering critical assets. By automating routine tasks and augmenting human expertise, it frees up valuable resources for strategic decision-making and innovation. Infosys Cyber AI aims to build resilient digital infrastructure core, platform centric services and AI-first SOC which enables enterprises to remain effective against evolving threat landscapes.



Security Operations Centers have evolved from traditional network operation centers, which aimed to provide continuous monitoring of network devices. The second-generation SOC started leveraging SIEM Technology to correlate logs and events across multiple sources of threat intelligence. As threats became increasingly sophisticated, enterprises started moving towards an autonomous Security Operations Centers (SOCs) that focused on data driven decision making and automation.

The next stage of evolution in enterprise SOC is AI-First SOC. The Infosys AI-First SOC built with resilience at the core of all SOC operations, powered by platform centric services to innovate at scale and powered by AI to amplify defender potential. Infosys has partnered with Palo Alto Networks to build a unified Infosys AI-First SOC leveraging capabilities of Infosys Cyber AI, power of cloud native XSIAM platform and Infosys Cyber Next platform.

How can Infosys AI-First SOC help enterprises?

Rise of digital transformation and adoption of AI have widened the attack surface. Cybersecurity Ventures predicts that global cybercrime costs are projected to reach \$10.5 trillion annually by 2025. The complexities of modern systems, high costs of maintaining multiple security solutions, lengthy procurement cycles, a shortage of skilled professionals, and integration challenges necessitates a holistic approach to SOC operations.

Key challenges faced by enterprise SOC:




Volume

SOC analysts are grappling with an overwhelming influx of data, often leading to high stress and burnout. The sheer volume of information, coupled with poor engineering and a high rate of false positives, making it a challenge to identify actual threats. The burden of investigating numerous alerts from disconnected endpoints can lead to inaccurate assessments and compromised security.



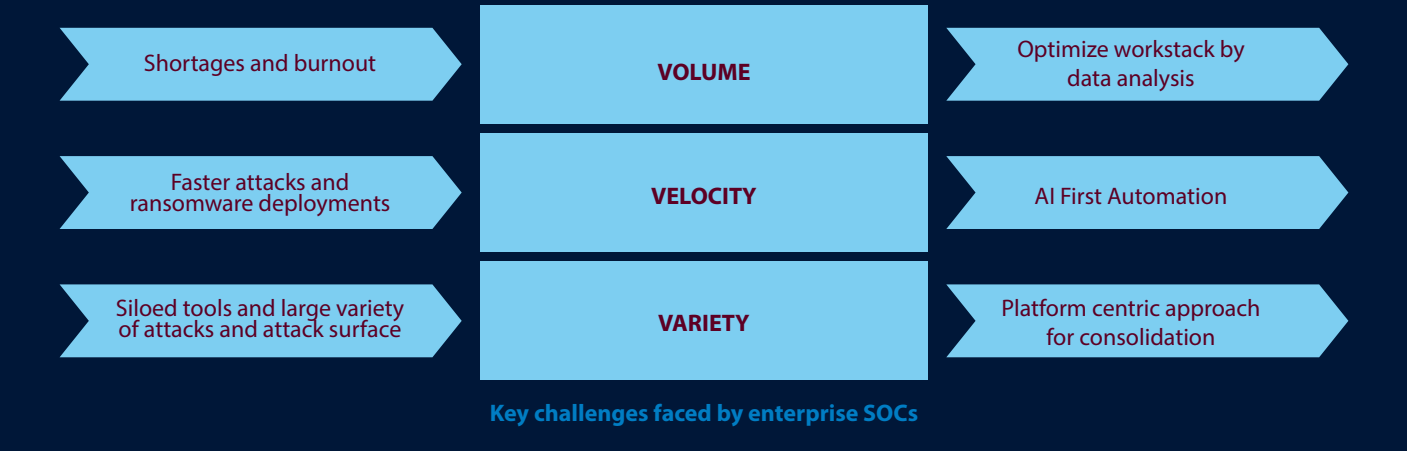
Velocity

Comprehending the velocity of cyber attacks is critical for an enterprise to respond and recover with minimal impact. The pace of attacks is crucial and has a cascading business impact. Cybercriminals equipped with Gen AI based weaponry are now deploying ransomware within 24 hours. which used to take more than 4-5 days.



Variety

Siloed tools and data feeds hinder threat detection and delay incident response. Complex organizational structures, like decentralized operations and independent cybersecurity teams, exacerbate this issue. Variety of threats can often create alert fatigue, and manual correlation can create hinderance for SOC analysts.



Infosys AI-First SOC - Smarter, Faster and Safer!

Infosys AI-First SOC enables enterprises by harnessing the power of AI and automation to simplify security operations, stop threats at scale, and accelerate incident remediation. Reduce risk and operational complexity by converging multiple products into a single, coherent platform purpose-built for security operations.

Infosys AI-First SOC, a strategic business enabler delivers significant value to our customers by providing a unified view of security posture of the enterprise, sustaining and accelerating manual tasks through AI based automation, enriching data driven decisions, amplifying defender potential and establishing security, privacy and responsible guardrails for AI.



Key Outcomes of Infosys AI-First SOC



Unified persona driven AI-First platform - Our AI-powered platform offers a unified view with actionable insights tailored for each persona of the security team, eliminating the need for multiple tools.



Amplifying defender potential through threat hunting and threat intel - AI-First SOC provides security practitioners Gen-AI assistance to amplify their defender capabilities and shift to proactive security with best-in-class threat intel powered by Unit 42 Threat Intelligence from Palo Alto.



Built-in security, privacy and responsible guardrails for AI - Our human-centric approach ensures transparent and accountable AI decisions, fostering trust. Our AI-First SOC is designed to augment your existing SOC team and improve the adoption of AI for cyber defense.



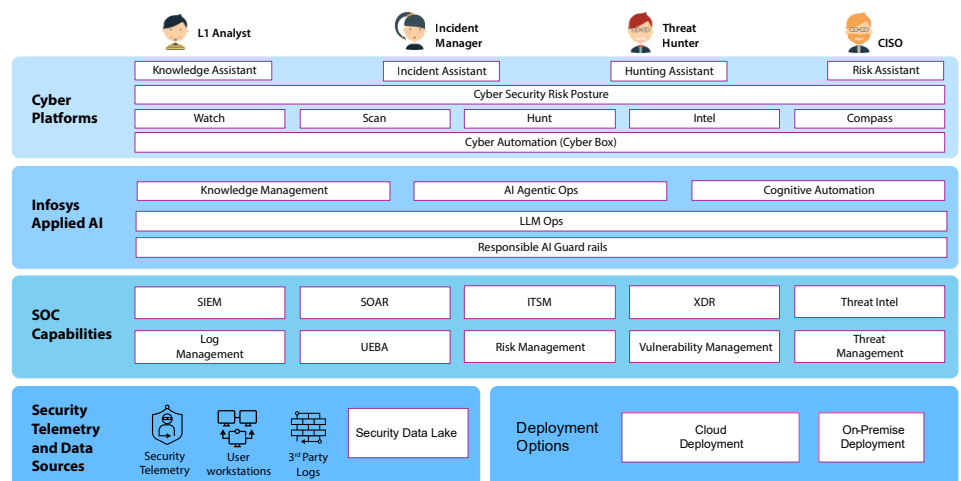
Enriched data driven decisions - With broad integration support, we easily connect to various data sources, minimizing engineering efforts. AI-First SOC can ingest more data sources while simultaneously improving response times from days to minutes, enabling faster identification and mitigation of threats. Data driven decisions helps the security team to reduce the mean time to repair (MTTR), reduce number of incidents requiring manual investigation and improve the overall security posture.



Sustain and accelerate through hyper automation - Infosys AI-First SOC automates manual tasks, significantly reducing response times and improving incident management efficiency. With customizable automations, you can tailor our platform to your specific needs. Our alert-specific playbooks automatically execute security tasks and address risks, even before an analyst intervenes. The platform learns from analyst actions, providing recommendations for future automations, continuously enhancing its ability to resolve incidents efficiently and accurately.

Driving Business Value with Infosys AI-First SOC

With Infosys AI-First SOC platform powered by Infosys Topaz, enterprises can protect their assets, reputation, and customer trust in an increasingly complex and challenging threat landscape thereby maintaining their competitive edge. AI-enhanced SOC platforms offer the agility, efficiency, and foresight necessary to navigate this landscape, ensuring long-term business resilience and growth.



The future of AI powered Security Operations Centers (SOCs) is one of the biggest challenges faced by enterprises today. AI, big data analytics, and advanced automation are enabling algorithms to take on cyber defense tasks that typically require human intervention. Opinions on AI's role in security are divided; some believe it will eliminate security team members, while others argue it will enhance intelligent threat detection capabilities.

Infosys' AI-First SOC is critical for building effective cyber defenses, as it has proven successful in reducing false positives, scanning large volumes of data to identify patterns, and providing generative AI-based assistance for personnel within the SOC. While AI is poised to radically transform security operations and the roles within them, its larger impact lies in collaboration—enhancing and amplifying the capabilities of defenders rather than replacing them.

For more information, contact askus@infosys.com

Infosys[®]
Navigate your next

© 2025 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.