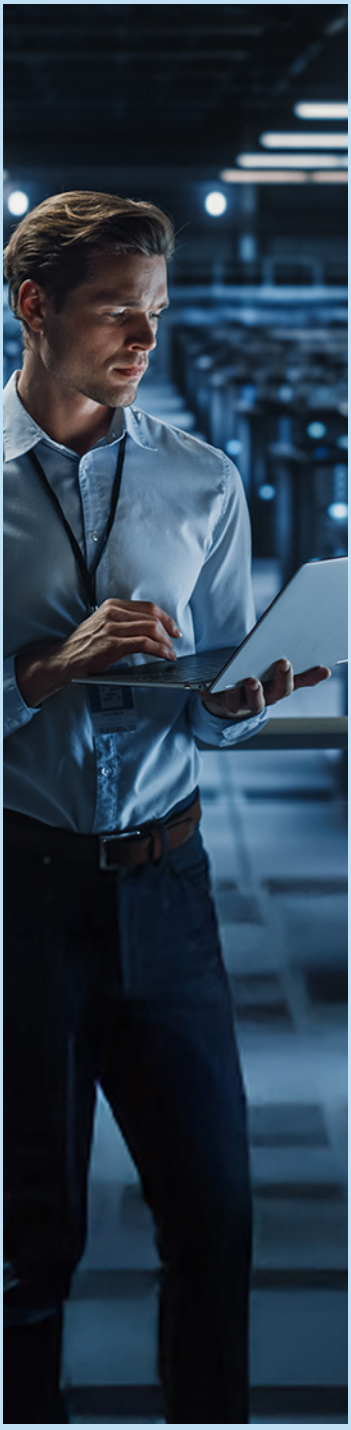
Infosys topaz

VIEW POINT



INFOSYS CYBERSECURITY DATA LAKE

databricks

Infosys®
Navigate your next

Cyber Security Drivers

The consumer privacy regulations are rapidly expanding, with privacy rights expected to cover 5 billion people. Governments around the world have passed legislation to regulate ransomware payments and strengthen data protection measures. As these Government privacy policies continue to evolve, the organizations face increasing pressure to enhance their cybersecurity capabilities and ensure compliance with a complex global regulatory landscape.

Beyond regulatory pressures, several technology and business trends are accelerating the need for stronger cybersecurity measures. The widespread adoption of cloud computing and the rise of hybrid work models are fueling demand for Secure Service Edge (SSE) solutions. Emerging technologies such as AI-driven bots and digital twins introduce new vulnerabilities, expanding the attack surface. At the same time, cyber threats have become increasingly sophisticated, with malicious actors weaponizing their attacks. As a result, cybersecurity has become a top boardroom priority—rising from 58% to 88% of boards now view it as a critical business risk.

Market Unmet needs

The analysis of the current Cyber Security tools in the market highlight the below unmet needs - The current Security tools in the market do not scale to handle large data, they don't have ability to integrate data.

Many tools do not support a variety of data (SASE, EDR, XDR). They don't provide business context for the security analysis.

There is no/less actionable personified security insights. There is less automated security foresights & scope.

Solution objective

Cyber Security Data Lake Solution powered by modern data platforms aims to provide unified, contextual, governed and automated data security insights to increase visibility, predict and control incidents and accelerate realization of cyber security by 40%.

By leveraging advanced analytics capabilities, this solution empowers CISO & CDO through pro-active detection and remediation of threats. It integrates with extended ecosystem to optimize cost and time ensuring compliance, scalability and intelligence for data operations.

Key Features

Key features of the Cyber Security Data Lake solution include

- **Unified security data foundation**: Diverse and large volume of security data sourced into governed and unified data platform.
- **Integrated data and security operations:** Near real time detection and response for security incidents.
- **Scalable data and processing:** Support to high volume and frequent data ingestion and processing.
- **AI-driven security and cognitive security decisioning:** Leverage AI & cognitive decisioning to predict, detect and remediate security threats.

The databricks data Intelligence platform is an optimal fit for the solution, offering a scalable delta lake for unified data, powerful processing capabilities, and the Mosaic AI framework to enable cognitive decisioning.

Solution blueprint with Databricks Data Platform

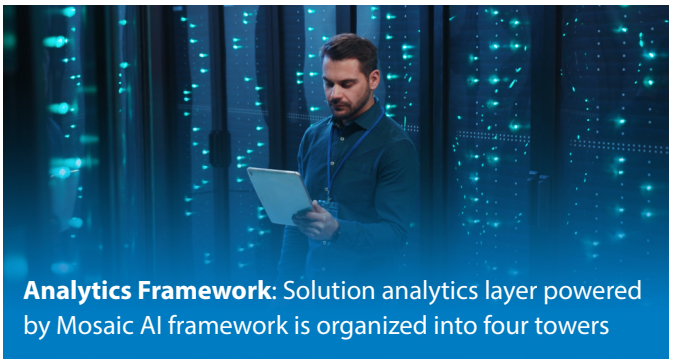
Cyber security data lake solution provides scalable and governed architecture with databricks data platform, blueprint consists of following components:

Data Ingestion & processing: High volume and velocity data from multiple cybersecurity data sources such as

Network logs, fraud alerts, IT operations, supply chain events,

Security breach reporting, social engineering indicators, and other threat intelligence feeds.

Data is transformed, enriched and aggregated into Delta lake and governed through Unity catalog.



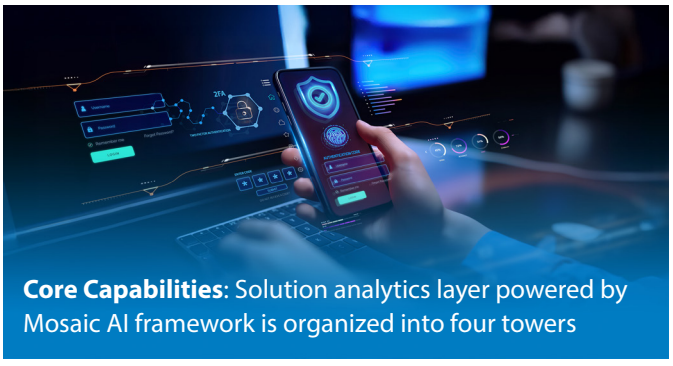
Analytics Framework: Solution analytics layer powered by Mosaic AI framework is organized into four towers

Threat Modeling: Data-centric, system-centric, threat-centric, and asset-centric models hosted on ML flow model registry and served through endpoint.

Prevention Modeling: Zero-threat design, security training, chaos engineering, and monitoring

Detection Modeling: Anomaly detection, event correlation, attack classification

Response Modeling: Incident management, eDiscovery, forensics, BCM information security, and backup/recovery.

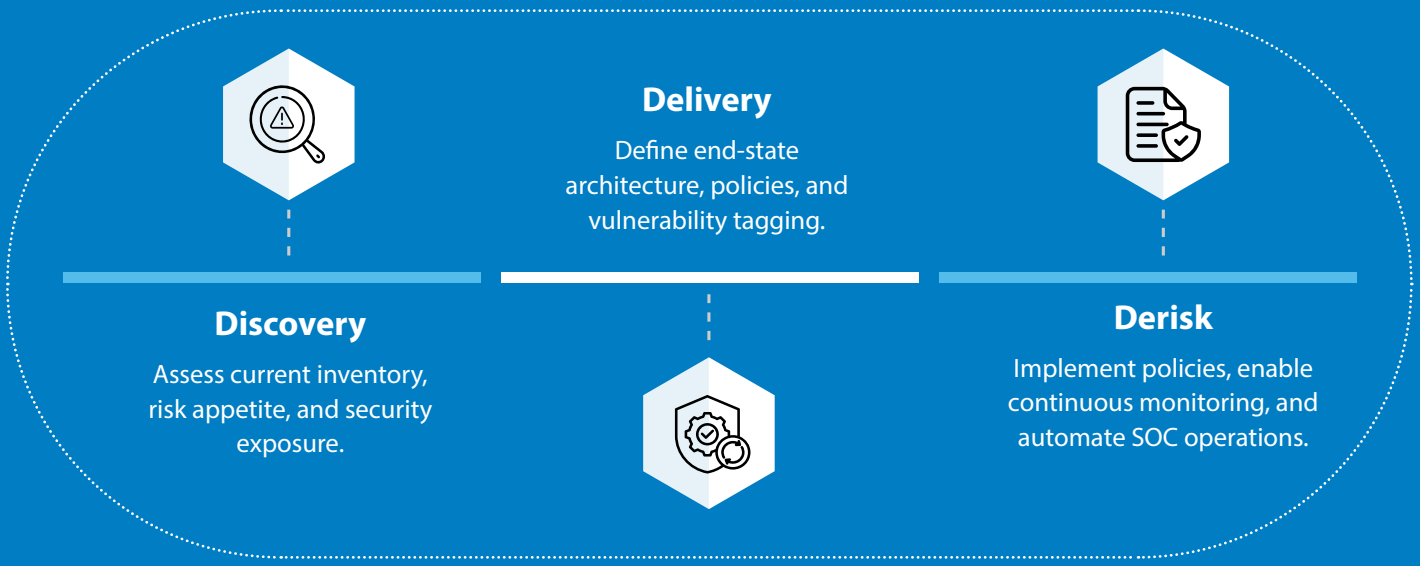


Core Capabilities: Solution analytics layer powered by Mosaic AI framework is organized into four towers

Solution integrates with Databricks asset bundle for resource provisioning and metadata management,

Monitoring and Diagnostics: Continuous health check and anomaly detections.

Solution follows 3 phase implementation approach, discover, deliver and derisk.



By implementing the Infosys Cybersecurity Data Lake Solution, enterprises can achieve significant automation of Security Operations Center (SOC) processes and reduce security incidents. Leveraging a unified data platform combined with advanced AI capabilities, the solution enables realization of critical cybersecurity use cases, delivering faster detection, response, and remediation aligned with modern security environments.

For more information, contact askus@infosys.com

Navigate your next