



# AI-Enabled Autonomous Cyber Defence Centre (CDC)

## Stay resilient with AI-powered detection, response, and defense against advanced cyberattacks.

**“By 2028, over 80% of SOC operations will integrate AI-driven automation to reduce response times.” ~ Gartner**

### Product Overview

Modern cyber threats move faster than traditional security can handle, overwhelming teams and bypassing existing controls.

The **AI-Enabled Autonomous Cyber Defence Centre (CDC)** by stc Bahrain delivers real-time protection using advanced AI, integrated security, and automated response.

Unlike traditional SOCs, the CDC works as an intelligent system that detects, investigates, and responds to threats automatically across your entire environment.

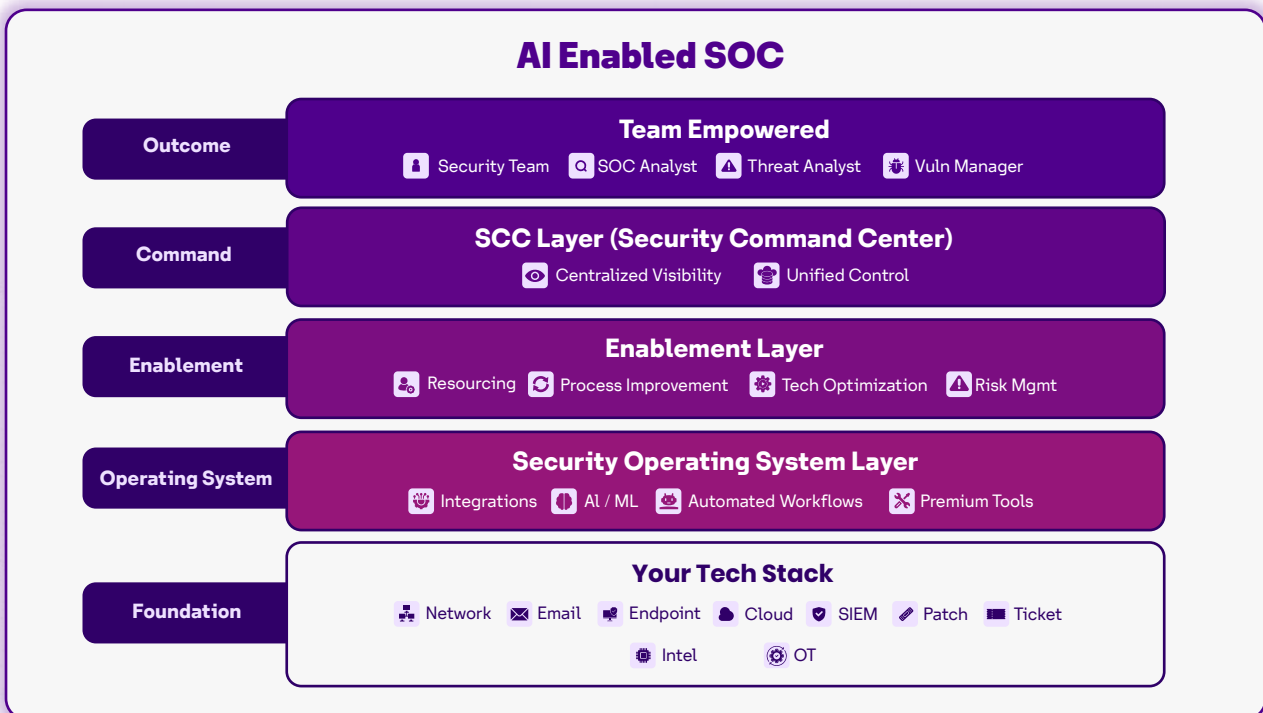
With unified visibility across network, cloud, endpoints, and identity, the CDC helps organizations reduce risk, respond faster, and stay compliant — with less operational effort.

### Customer Challenges

- **Alert Overload & False Positives:** Security teams are overwhelmed with thousands of alerts daily, making it difficult to identify real threats.
- **Fragmented Security Tooling:** Multiple disconnected tools create visibility gaps and slow investigations.
- **Slow Investigation & Response:** Manual processes take 30–90 minutes per alert, increasing exposure to attacks.
- **Talent Scarcity & High Costs:** Building and maintaining 24/7 security operations is resource-intensive and costly.

### Our Solution

- **AI-Powered Autonomous Detection & Response:** Automatically identifies, prioritizes, and responds to threats in real time.
- **Unified Security Ecosystem:** Correlates data across SIEM, EDR, XDR, cloud, identity, and email security.
- **Automated Investigation & Decisioning:** Delivers complete analysis, risk scoring, and recommended actions within minutes.
- **24/7 Expert Oversight:** Combines AI automation with stc cybersecurity experts for continuous protection.





## Key Features

- **AI-Driven Threat Detection:** Processes large volumes of security data to identify real threats with high accuracy.
- **Automated Threat Response (ATR):** Executes predefined response actions to contain threats instantly.
- **Unified Visibility (Single Pane of Glass):** Centralized monitoring across all environments — on-prem, cloud, and hybrid.
- **Threat Intelligence Integration:** Leverages global and regional intelligence feeds, including dark web monitoring.
- **Cross-Platform Correlation:** Combines signals from multiple security layers for contextual threat detection.
- **Real-Time Analytics & Dashboards:** Provides actionable insights, reporting, and executive-level visibility.

## Business Benefits

- **Faster Detection & Response:** Reduce investigation time from hours to minutes.
- **Improved Security Posture:** Proactively detect and mitigate advanced cyber threats.
- **Reduced Operational Burden:** Operate as an extension of your team without hiring additional resources.
- **Cost Optimization:** Lower total cost of ownership by consolidating tools and reducing manual effort.
- **Compliance & Governance Ready:** Supports regulatory requirements including CBB, PDPL, ISO 27001, and global standards.
- **Enhanced Business Resilience:** Minimize downtime and protect critical business operations.

## stc Edge

- **Regional Expertise:** Deep understanding of Bahrain's regulatory environment and threat landscape.
- **AI-First Cybersecurity Approach:** Purpose-built platform for autonomous detection, investigation, and response.
- **End-to-End Cybersecurity Coverage:** From prevention and detection to response and recovery.
- **Integrated Security Ecosystem:** Seamlessly connects with stc's broader cybersecurity portfolio.
- **24/7 Expert Support:** Continuous monitoring and support from certified cybersecurity professionals.

## Service Snapshot

Category	Details
Delivery Model	AI-enabled, cloud-based and hybrid Security Operations platform
Support	24/7 monitoring with AI automation and expert oversight
Core Capabilities	Threat detection, investigation, automated response, threat intelligence
Coverage	Endpoints, network, cloud, identity, applications, email
Industries Served	Banking, Government, Telecom, Energy, Healthcare, Retail, Enterprises
Key Technologies	SIEM, EDR/XDR, AI analytics, automated response, threat intelligence

## SLA Highlights

- 24/7 Monitoring & Response
- Investigation Time: Minutes (AI-driven)
- High Alert Accuracy & Noise Reduction
- Automated Incident Response Capabilities
- Compliance Reporting & Audit Readiness

## Take the Next Step

Strengthen your cybersecurity posture with **AI-powered autonomous defence.**

Contact stc Bahrain's Cybersecurity Team to deploy the

**AI-Enabled Autonomous Cyber Defence Centre (CDC).**