Annex A: Notable Offerings Showcased at Cybersecurity Summit 2025

Cybersecurity Innovations in AI

Name	Features	Benefits
AI-Enabled Threat Elimination and Response (AETHER)	Scans endpoints proactively, establishes security baselines, and delivers regular health check reports Deploys scanning agents for threat hunting, compromise assessment and benchmarking against industry security standards Supports incident response planning and provides ongoing incident handling reports	**Enables faster threat response**: Delivers comprehensive visibility into endpoint activity and instant alerts, helping SMEs detect and respond to threats in real-time **Improves confidence and decision-making**: Uses AI-driven behavioural analytics to reveal relevant threats, reducing guesswork and helping SMEs minimise cyber risk **Eliminates setup and operational effort:** Offered as a fully managed subscription service, eliminating the complexity of system ownership, ideal for resource-constrained SMEs
AGIL® Secure AI	Detects and mitigates adversarial AI attacks such as prompt injection, model evasion, and prompt leaking Automates security testing to identify vulnerabilities in AI and GenAI systems before deployment and production Evolves with emerging AI attack techniques to ensure up-to-date protection Performs root-cause analysis to trace incidents back to their source and accelerate resolution	**Protects AI and GenAI systems at every stage:** Embeds security at every stage of the AI lifecycle—from development to deployment to production—for end-to-end threat coverage **Prevents unknown threats:** Continuously evolves with the latest threat research to defend against known and emerging AI-specific attack vectors, ensuring long-term protection **Delivers real-time protection**: Identifies and neutralises threats before they disrupt AI operations, reducing risk exposure and potential operational downtime

		Builds trust and accountability: Implements automated security testing and compliance to AI security guidelines, strengthening stakeholder confidence in responsible AI adoption
Adaptive & Intelligent Cyber Monitoring of OT Systems (AICYMO)	Uses AI and machine learning to develop advanced threat detectors tailored for Operational Technology (OT) environments across manufacturing, energy and transportation industries, and more Correlates data from multiple OT sources to link anomalies and alerts, enabling smart categorising of potential issues	**Improves threat detection**: Utilises AI-driven models to uncover security threats that traditional OT monitoring may miss, significantly enhancing both visibility and detection accuracy in OT systems **Enables faster, more informed response:** Identifies threats across both physical and digital environments, providing unified IT-OT actionable insights for swift responses and risk mitigation **Boost investigation and forensic efficiency:** Differentiates IT events from system faults, allowing analysts to focus on root causes and accelerate investigation efforts
AI Cyber Analyst	Uses Agentic AI to act autonomously and support human analysts in real time in Security Operation Centres (SOCs) Automates and streamlines existing SOC workflows such as initial triage and improving threat insights Continuously learns from threat intelligence to automatically create new detection rules that stay ahead of emerging threats Integrates extensive data sources to correlate information and deliver precise, context-	**Boosts SOC efficiency:** Automates labour-intensive, repetitive tasks, reducing manual workload by more than 50%, freeing analysts to focus on high-value investigations and reducing alert fatigue **Enables faster, deeper investigations**: Empowers Tier 1 and 2 analysts to handle complex Tier 3-level analysis with AI-guided assistance, enabling Tier 3 analysts to focus on strategy **Improves decision quality and speed**: Delivers context-rich, AI-driven insights that support faster triage, root-cause analysis, and threat attribution

	aware recommendations for incident response	

Quantum-Ready Encryptor

Name	Features	Benefits
EtherCrypt	Delivers AES-256 high-assurance quantum-safe encryption for secure data transmission across Ethernet and Metro-Ethernet networks Supports full-duplex encryption at up to 10Gbps or 1Gbps, suitable for point-to-point, point-to-multipoint, and mesh network setups Built with future-ready architecture that supports Quantum Key Distribution (QKD) Designed with tamper resistance, active zeroisation, and emergency erasure for hardware-level security control Multi-speed port encryptor supporting network segregation and aggregation in a single device	**Protects high-value sensitive data:** Protects sensitive data in real-time with strong encryption, integrity assurance and anti-replay communication **Prepares networks for quantum threats:** Enables a smooth shift to quantum-resilient encryption through Post-Quantum Computing (PQC) and QKD support, ensuring long-term data security **Simplifies secure deployment:** Seamlessly integrates into existing network environments, reducing time and effort required for implementation **Delivers end-to-end network insight:** Remotely monitors deployed encryptors to provide comprehensive network visibility and enable faster issue detection and troubleshooting