

Cyber Security Asset Detection

You can't effectively manage what you can't effectively see or control



Cyber Security Asset Detection, why now?

- The merging of IT and OT due to digital transformation
- The working from home movement creating more risk to the network environment
- Having a complete asset inventory, which is critical for effective security
- More devices becoming 'un-agentable' and a greater number of unsanctioned devices accessing your network
- Improve the risk posture of all devices, providing you with one source of truth
- Device identification and tracking via crowd sourced, cloud based device behaviour knowledgebase, which tracks 1 billion + devices daily
- Ability to query and identify specific devices, building reports and insights simply and easily

The Challenge

Cyber security asset management and detection is a major challenge for all companies. The IT and OT convergence has resulted in new demands on CIOs and CISOs, who are now tasked with protecting the entire business ecosystem. There has been an explosion of IoT and unmanaged devices on networks, along with challenges of managed devices and the cloud environment. Organisations are struggling to have an accurate and detailed inventory of every asset in their environment.

Area of Focus - Cyber Resilience

C-STEM CrowdSMART agentless device security services offer consultancy, design, engineering and the complementary phased introduction of best of breed technology, which is proven to impact business outcomes in digital transformation. Whether there is a need to overcome challenges in one or multiple areas, C-STEM can provide the right solution designed to complement existing systems and tools, reduce time, effort and cost effectively bridge the gaps. Five real world scenarios are:

Asset Inventory

Ability to automatically discover every connected device in the environment — managed and unmanaged, wired and wireless, on or off your network.

Risk Management

Discover the risk of every device. Armis generate a risk score for every device on your environment.

Threat Detection and Response

Ability to safely determine whether any existing devices are vulnerable to ransomware attacks, allowing security teams to take proactive measures to protect these devices from attack.

Efficient Auditing

Platform gathers equipment utilisation information across the entire enterprise, giving intelligence about device usage, hours of operation and underutilisation.

More value from your existing investments

Integrate with your existing security tools, letting you leverage existing investments to achieve greater value and more automated response.

Hassle Free Engagement

To assist with qualifying a complementary fit, C-STEM has evolved a 3 stage collaborative process to empower business leaders and heads of IT with a minimum to no disruption risk free efficient evaluation. This includes:

Qualifying existing technologies & services; accurately scoping and defining success criteria; assessment, testing & evidence based reporting.

“Making digital transformation safe for the enterprise”

The Solution powered by



- ✓ 100% Agentless, passive, comprehensive continuous security monitoring
- ✓ Flexible and seamless asset inventory solution
- ✓ Frictionless deployment
- ✓ Automated response and remediation
- ✓ Eliminates fragmentation and complexity
- ✓ Automate security and policy enforcement
- ✓ Rapid deployment
- ✓ Integrates with existing security solutions including Network infrastructure, Firewalls, NAC, SIEM, ITAM & CMDB, Vulnerability scanners
- ✓ Complementary professional services
- ✓ Reduced demands on time and resource



Kick start the acceleration of your digital transformation journey with our hassle free assessment, gap analysis and risk report