SHIELDWORKZ

Competitive Landscape IT, OT and IoT Cybersecurity Platform Providers

Mandate	Shieldworkz	Competitive Solution	Shieldworkz - Competitive Advantages
Solution, Focus and Modules	Suite – Vulnerability Management (Device Discovery and Risk Assessment) Advanced Threat Detection Micro Segmentation Threat Intelligence	No single solution that can cover end-to-end security requirement for OT & IoT Security	• Shieldworkz Solution is a market leading solution provider of OT & IoT Cybersecurity with diverse deployments securing more than 18 million devices around the world. • The solution is deployed across large global organizations including Tier 1 Telecom operators (including Telefonica, Etisalat, Tier 1 Singapore Operator), IoT MVNO (POD Group etc.), Manufacturing Plants (Mabe, Schaeffler), Oil & Gas infrastructures (KIPIC), Educational Institutions (NTU), Global SIs (Fujitsu APAC) among others. • One of the key differentiators is the solution platform (Security Suite) is modular and it can expand its detection capabilities for Cybersecurity through any addon modules (OT Security, IoT Security and 5G Security)

Solution, Focus and Modules	Suite – Vulnerability Management (Device Discovery and Risk Assessment) Advanced Threat Detection Micro Segmentation Threat Intelligence	No single solution that can cover end-to-end security requirement for OT & IoT Security	Wide coverage for protocols such as IEC61850-8-1 (GOOSE & MMS), IEC60870-5-101(Serial), IEC60870-5-104 (IP), Modbus/TCP, EtherNet/IP, DNP3.0, IEC62351, IEC 61850-9 protocols, or SV (Sampled Values) and effectively uses its advance machine learning tecniques that are both supervised and unsupervised in order to identify the attack patterns. • Collection of source data from Network Switches and Edge Cloud Environments • Alarm management & Custom Playbooks tailored for Security Investigation
Level of Automation and Control using Advanced detection techniques	Yes	This functionality is not available in other similar products in the market	• Shieldworkz Solution provides correlations across multiple attack strains, which helps customers to meet their key business requirements like detection Advance Persistent Threats and help mitigate the attacks with automated workflows (playbooks) • The unified management (HUB) provides complete control to the admin while allowing an option to automate certain functions. • The unified management is designed to reduce manual review or intervention, automate detection and response, and provide deeper insight into security on the substation network and the control centre.
Performance and Time to Detection	Proactive and Scalable	Reactive	• Shieldworkz has proactive approach to detect security events with signature-based inspection of network packets (PCAPs) and maintain all stages of events for early and near real time detection. • Reduced time to detection helps in containing the damage, reduced loss, improved QOS, Improved reaction time to new threats. • Shieldworkz is proven to scale in very large and complex networks (like Telefonica).

Multi-layered Protection	Three Layers of Detection	Single Layer of Protection	• The solution works with a modern understanding of the types of Advanced Attacks and their impact • Threat Detection in OT & IoT environments is complex and challenging due to its complicated network structure; Shieldworkz offers protection at multiple levels as it has 3 layers of detection namely, Signatures, Heuristics and Anomaly (Advanced Machine Learning and AI) in comparison to other products which uses only static rules coupled with some elements of basic machine learning.
Ease of Deployment and Integration	Easy to deploy	Complex	• Setting up, maintaining, and constantly updating the solution is essential and fundamental for Security Solutions. All Shieldworkz solutions work on a unified management called Shieldworkz Hub. This allows to integrate with any of our solution modules such as the OT Security, IoT Security or 5G Security seamlessly. • Shieldworkz allows provisioning to setup behavioural rules in the engine, through its unified management (HUB) console. • Shieldworkz provides easy non-intrusive integration into the network allowing near real-time threat detection and mitigation.
Security and Compliance Standards	Maximum Compliance	Limited Compliance	• Shieldworkz adheres to all standard guidelines defined by GSMA on IoT Security, NERC CIP, IEC 62443, IEC 61850, NIST etc for OT Security. We have the complete list on the technical proposal.
Real-time alerts and notifications	Yes	No	• As Shieldworkz monitors network data all alerts can be triggered near real time, this enables the user to effectively contain attacks before incurring huge losses. It effectively limits Attack cases and cuts down losses
Pricing Model and Value	Flexible Pricing	CAPEX Pricing Model	• Shieldworkz allows flexible pricing models (CAPEX, CAPEX + Yearly OPEX, OPEX etc.) for volume based, module based. Shieldworkz helps balance the customers current business needs and what you can use in the solution

Customer Support	Highly Skilled Support Team with High CSAT Score	Limited Support	• Shieldworkz provides varied levels of solution support and managed services from the India centric R&D and SOC. The world class support is built on knowledge base of IoT and OT Security.
AI and Machine Learning	Deep Learning Enabled	Basic Machine Learning	• Shieldworkz solution has inbuilt deep learning capabilities that automatically monitors, analyses, and improves its Threat Detection over time.
Ability to process data from multiple sources	Log and flow data ingestion to find security breaches	Limited coverage	• Network flow logs using netflow and sFlow, Firewall logs, Anti APT System Logs, IoT Sensor logs, IIoT Sensor Logs, OT Visibility Logs, SCADA / Historian data, Database & Kernel Logs
Handling false positives and Threat Intelligence	Organic	None	• Shieldworkz has one of the largest honeypot network and security intelligence in the world which collects signatures, heuristics, and patterns of attacks from various attackers in their attempts to intrude unknowingly into its decoy systems. With this unique strength, it has an unparalleled ability to identify & detect new and evolving threats before any other solution can identify. This comprehensive threat intelligence reduces possibility of any false positives significantly, almost negligble. • It also provides automatic updates of Threat intelligence with real-time threat intelligence feeds on Hotlist or Blacklist URLs, IPs etc. • Other platforms or solutions (which claim machine learning based detection techniques) have very high false positive.
Detection Capabilities	Ability to detect multiple Attack types	Requires multiple solutions (including 3rd party in some cases) to be put together to match the Shieldworkz's full Detection Capabilities	• Advanced Malware Detection, Zero Day Security Detection, Anomaly Detection and Many more

Secure Your Industrial Future

Talk to us today!

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.