SECURITY MATTERS

ForeScout's CounterACT® Integration with SecurityMatters' SilentDefense

Create and maintain the most comprehensive inventory of IT and OT assets and related vulnerabilities

Highlights

- The integration of ForeScout's and SecurityMatters' products brings back the lost visibility and control to ICS asset owners and restores confidence across OT and IT networks.
- Risk & Vulnerabilities are strongly reduced through the combination of best of breed visibility for IT networks with the most comprehensive passive fingerprinting of OT infrastructure.
- Communication and processes between IT and OT stakeholders is improved and automated via a common and complete view of the asset inventory and of the vulnerabilities

ForeScout®

The Challenge

In the last 15 years, industrial networks have undergone significant changes in the way they are designed and managed. Legacy systems and protocols have been largely substituted by commercial-off-the-shelf (COTS) systems and standard communication technologies. This has led to relevant gains in connectivity, productivity and business analysis capabilities, but it has also introduced new risks.

Firstly, the increased complexity, dynamicity and heterogeneity of industrial networks has made it harder, if not impossible, for engineers and security analysts to keep track of the current configuration and security status of network devices and components. Secondly, the increased connectivity and the use of COTS technologies has made industrial networks more permeable to external threats, and more subject to vulnerabilities until now common only within IT networks.

The integration of ForeScout's and SecurityMatters' products brings back the lost visibility and control to industrial operators and restores security confidence across operational and IT networks. It combines the best of breed visibility and management capabilities for IT networks with the most comprehensive passive fingerprinting of OT infrastructure, thereby delivering maximum results without any disruption to the production process.

CounterACT®

ForeScout offers the ability to see devices the instant they connect to the network, across all network levels, classifying and determining their function, ownership, location and security hygiene level. This visibility is essential for improving your endpoint compliance posture, tracking assets and defining your security and enforcement policies. Devices, ports and connections are continuously monitored using passive techniques without imposing risk to operations. With this real-time intelligence, incident responders can use a broad range of actions to address risk and potential threats. For example, Windows-based devices are being continuously monitored and missing Windows updates can be immediately detected.

ForeScout integrates with a broad set of leading network, security and IT management solutions, orchestrating multivendor security and allowing:

- Shared context and control intelligence among systems to alert and enforce unified network security policy
- Reduce vulnerability windows by automating system-wide threat response
- Gain higher return on investment from your existing security tools while saving time through workflow automation

SilentDefense

SilentDefense is the most advanced and mature real-time network monitoring and intelligence platform for industrial control systems (ICS) networks. It leverages deep packet inspection and patented technology to passively analyze industrial protocol communications and automatically generate a full asset inventory and a complete communications fingerprinting of Purdue Level 2 and Level 1 devices. The inventory includes device details such as OS version, open ports, device vendor and model, firmware version, serial number, I/O modules and vulnerabilities for all major ICS vendors and 35+ industrial protocols.

In addition to its inventory capabilities, SilentDefense features a vast Industrial Threat Library for out-of-the-box detection of cyber security and operational threats such as connectivity issues, device malfunction and misconfiguration, dangerous process operations, use of insecure protocols and default credentials and exploit attempts. These capabilities as well as its advanced anomaly detection engines can be selectively enabled by the user, to achieve full protection of the network and effective response to existing and emerging threats to OT networks.

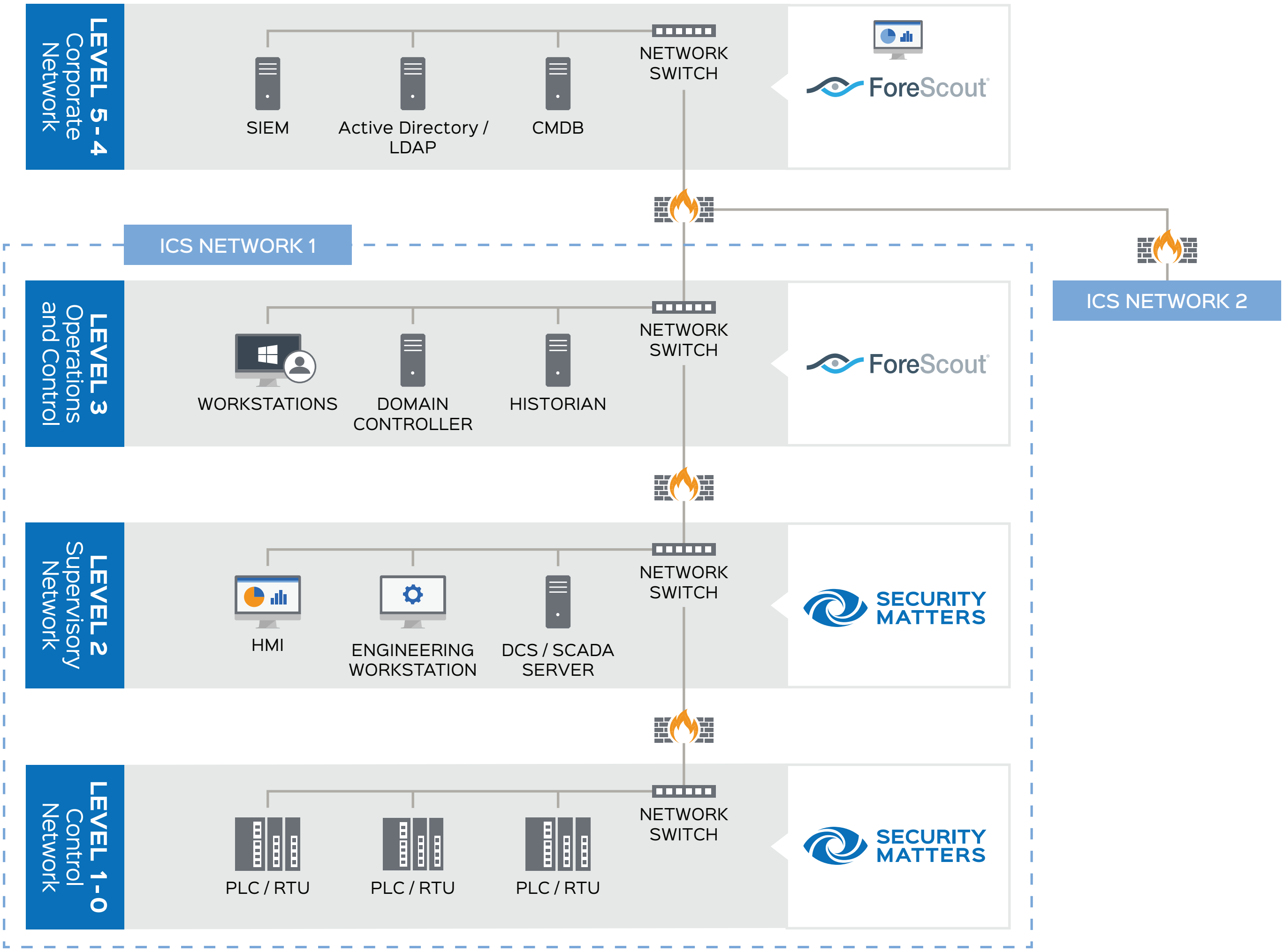
CounterACT® & SilentDefense

The integration of ForeScout and SecurityMatters' SilentDefense enables industrial organizations to automatically generate and maintain an integrated and always up-to-date inventory of their entire IT/OT infrastructure from the L5 to L1 devices, guaranteeing a smoother, quicker and cost effective integration of the OT infrastructure into existing IT security programs. The inventory contains critical device and network information that is required by CISOs and OT managers to preserve the security and productivity of the industrial network.

ForeScout and SilentDefense seamlessly integrate and consolidate the information independently collected and make it available to the user through ForeScout's console and policy engine, or by forwarding it to an external system such as Security Information and Event Management (SIEM) solutions, configuration management databases (CMDBs), asset management and governance, risk management and compliance (GRC) platforms.

Benefits of the Integration

- Full visibility over the network, its devices and components including IT and operations (OT)
- Assessment of device vulnerabilities and network security exposure
- Report of violation of company policies, such as the use of default credential and insecure protocols
- Prioritization of patching and hardening activities
- Detection of operational problems and cyber attacks at their earliest stage
- Reduction of planning and troubleshooting effort and costs
- Maximized efficiency of security and operational personnel



SECURITY MATTERS

SecurityMatters empowers critical infrastructure and manufacturing organizations with the ability to identify, analyze, and respond to industrial threats and flaws, minimizing troubleshooting costs and unexpected downtime. We leverage ICS-specific knowledge and understanding to provide visibility into critical assets and their activity, and detect operational problems and cyber security threats. Our revolutionary network monitoring platform has been successfully deployed by customers worldwide.

www.secmatters.com | info@secmatters.com