RAM²-Symantec Integration

As more companies adapt to Industry 4.0 standards , efficiency and innovation is achieved faster than ever before. However, advantages also bring an increase in the number of OT-specific security vulnerabilities and expand the attack surface of the OT network. This exposes the industry to new cyber security threats, putting operational continuity at risk.

OTORIO's RAM² mitigates these risks. RAM², an industrial SIEM & SOAR (Orchestration, Automation, and Response) platform integrates with Symantec's Critical System Protection (CSP) to deliver a comprehensive security solution that adds operational context to cybersecurity alerts, reduces industrial-specific threats, and improves the ROI of security tools making the Industry 4.0 journey safer.

Use Case Examples:

Vulnerable and rogue devices

By correlating Symantec's CSP events with asset inventory information, RAM² creates alerts about gaps in endpoint protection. When new assets are detected by RAM², it means that the host is not protected. This information is used to identify rogue devices and increases the need for mitigation. RAM² asseses risk assessment and prioritization based on asset vulnerabilities.

Malware outbreak

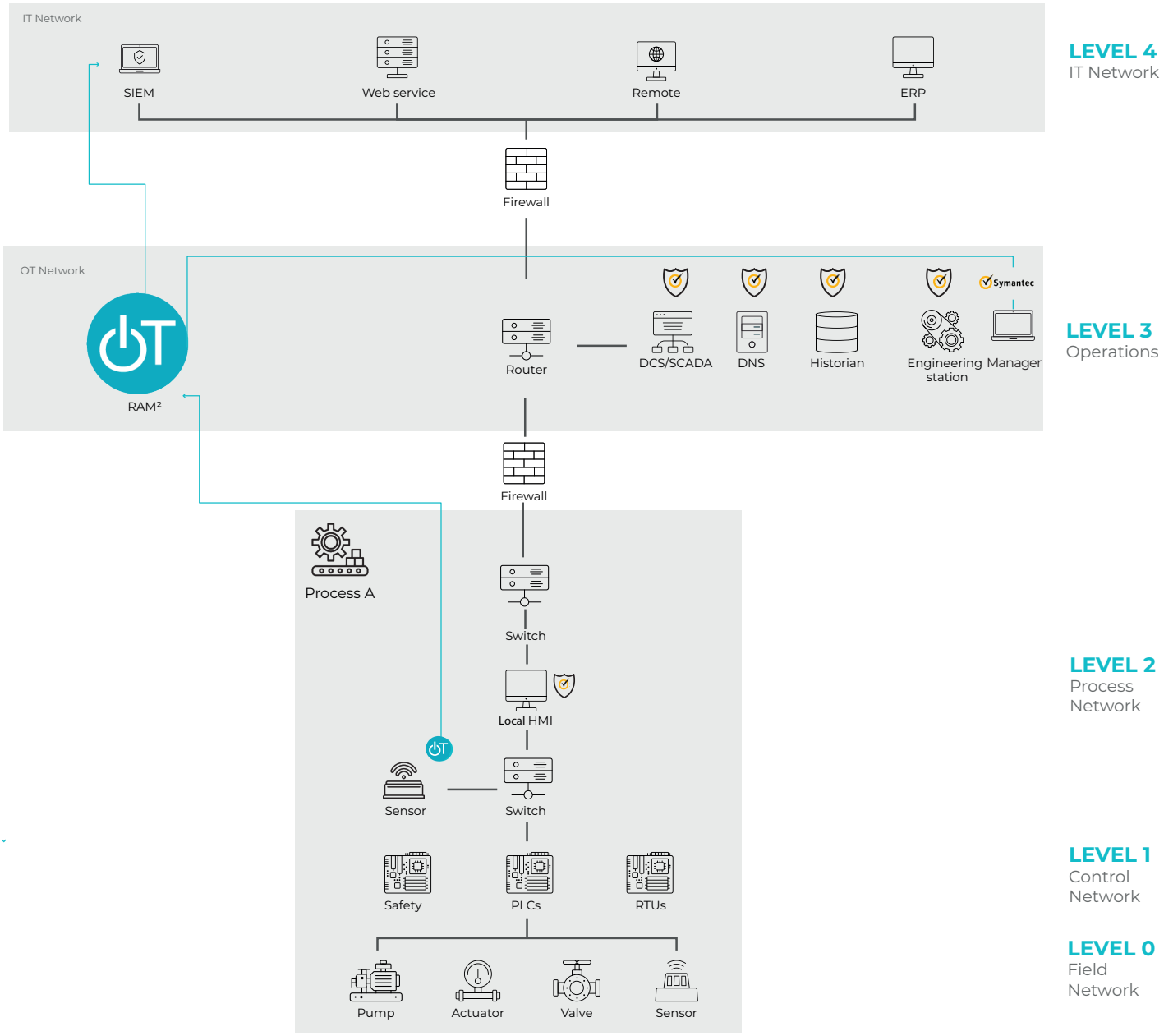
RAM² monitors events that are generated by CSP for industrial malware detection and analyzes them within the operational context. Malicious attacks that affect multiple assets within an operational unit increases the security risks. Detecting an infection within multiple operational units indicate that an uncontained attack is spreading in the network and requires immediate mitigation.

OTORIO's RAM² Solution

OTORIO's Risk Assessment, Monitoring & Management platform (RAM²) is a Next Generation Orchestration, Automation and Response (SOAR) and SIEM platform. RAM² was designed to provide cybersecurity and digital risk management capabilities in converged IT/OT/IoT environments comprising hundreds of multi-protocol devices

Integration Benefits

- Reduces risks and supports the operation personnel to make the best use of their resources with CSP's intrusion prevention
- Provides mitigation playbooks that are suitable for the unique needs of the operational network
- Delivers advanced risk assessment based on correlations between CSP alerts and data and events from multiple security and industrial systems



About OTORIO

OTORIO combines the professional experience of top nation-state cyber-security experts with cutting edge digital risk management technologies to provide the highest level of protection for the manufacturing industry. OTORIO's automated Digital Risk Based Maintenance solution aggregates threat data analysis to provide deep insights into industrial control systems, identifying risks and mitigating them before they can cause damage. OTORIO empowers industrial companies to implement, automate, and operate secure production, making way for a safer, more reliable, and productive industry.

Learn more at www.otorio.com