SCADAfence

Ensuring Operational Continuity

SCADAfence offers cutting edge cybersecurity solutions designed to ensure the operational continuity of industrial networks in manufacturing industries and critical infrastructure, such as pharmaceuticals, chemicals, food & beverage and energy.
The company's products are developed by OT cybersecurity professionals together with world-renowned experts in control systems and cybersecurity, such as Joel Langill, a.k.a. SCADAhacker. The company is financially backed by JVP, a global leader in cybersecurity investments.

The Challenge – Avoiding Unnecessary Downtime

In recent years, adoption of connectivity and IT technologies in operational networks has provided many benefits, such as easier maintenance and centralized management. While these technologies increase productivity and reduce production costs, they expose mission critical systems to new risks that can cause operational downtime.
Most of today's downtime is caused by non-malicious operations such as human error and misconfiguration. With that being said, now more than ever, cyber-attacks pose a risk to system uptime and availability.
Pinpointing the root causes of downtime and other errors is often difficult, making it hard to differentiate operational and security-related incidents and making repeat incidents inevitable. Traditional IT and security technologies were designed for IT networks, not high-availability systems and may pose a risk to industrial environments. Most existing solutions available today are unfit for use in high-availability networks and by OT personnel, and such networks are often left unprotected.

"Majority of [ICS Security] incidents have an "unknown" access vector due to the lack of monitoring and detection capabilities", ICS-CERT, February 2015

Our Solution – Passive Network Monitoring

Our solution is a passive, risk-free network monitoring system, built to address the needs of both OT and IT security personnel and allow them to gain control of their networks. The solution offers full visibility of day-to-day operations and real-time detection of cyber-attacks – from previously-known malware and disclosed vulnerabilities, to sophisticated attack vectors. In addition, predictive alerts on incidents that may cause downtime allow preventive measures to be taken. In case of downtime, forensic analysis enables root cause identification and reduction of response time.
The cost of downtime in operational environments is significant and has a direct impact on the company's revenue stream. By passively monitoring the industrial network, you can increase the productivity and availability of your systems, while giving you peace of mind, knowing that our solution does not pose any threat to your environment.

Solution Benefits – Ensure Operational Continuity

Passive & Seamless Deployment

Passive integration, requiring no changes to existing network equipment

Auto Configuration & Baseline Generation

No configuration needed – automatically map your network's activity

Real-Time Network Visibility

Fully understand your network using real-time visualization tools

Monitoring Network Changes

Monitor new devices, sessions and industrial operations in the network

Detection of Operational Threats

Detect errors and misconfigurations before they threaten operations

Detection of Attack Vectors

Detect industrial attacks and use advanced forensics tools to analyze incidents

Mail: info@scadafence.com **Web:** www.scadafence.com **LinkedIn:** company/SCADAfence **Twitter:** @SCADAfence