Introduction

Introduction

In late 2014, a steel mill in Germany suffered massive damage as the result of a cyber attack that required advanced hacking skills, applied industrial control knowledge and endurance. No one has claimed responsibility for the attack and the lack of attribution and clear objective emphasize that not only are the threats very real, but anyone can become a target without apparent reason. This incident is only one of many examples of successful cyber attacks of industrial automation and control systems, and together with Stuxnet manifests the reality of cyber threats.

Unless you have experienced a serious security incident first hand, it is easy to believe such attacks only happens to someone else, but not having experienced such an incident however, does not mean you haven't been compromised. In fact, according to a report from KPMG from 2014, it is more likely than not that information is being exfiltrated by malware without your knowledge from your office networks. 14 companies were studied, and data was actively stolen from 10 of them without their knowledge.

The report is yet another strong indication traditional, best-practice defense like anti-virus, perimeter firewalls and network intrusion detection systems based on signatures are easily avoided. It also indicates insufficient organizational readiness as no action was taken even when malicious code was detected.

Westermo present a series of five basic applications assets owners can apply in their own networks to improve the security posture in a sustainable way.

Intrusion Detection

Intrusion detection is really exactly what it says, about detecting intrusion, which is not a single technology or solution but a range of different techniques and approaches. The abbreviation IDS, or intrusion detection system, is often used somewhat ambiguously to describe the need of intrusion detection mechanisms that integrate in an overall intrusion detection architecture rather than a separate system that only monitors a limited set of indicators, such as a NIDS or network intrusion detection system.

A critical component in any detection architecture is centralized monitoring, in this case a security event monitoring system (SEM or SIEM), which collects and analyzes as much information as possible that may indicate intrusion. Everything else is basically only different event sources that forward events to the SEM.

WeOS devices contribute to the intrusion detection architecture by forwarding events that may indicate intrusion to a SEM, for example;

- Dropped unknown or blacklisted packets
- Failed login attempts

Typical Application

Single system scenarios typically have a single SEM onsite with the system. The WeOS devices are configured following the Network Segregation, Perimeter Protection and Spoofing Protection application concepts and all unknown or known bad traffic is logged and reported to the SEM.

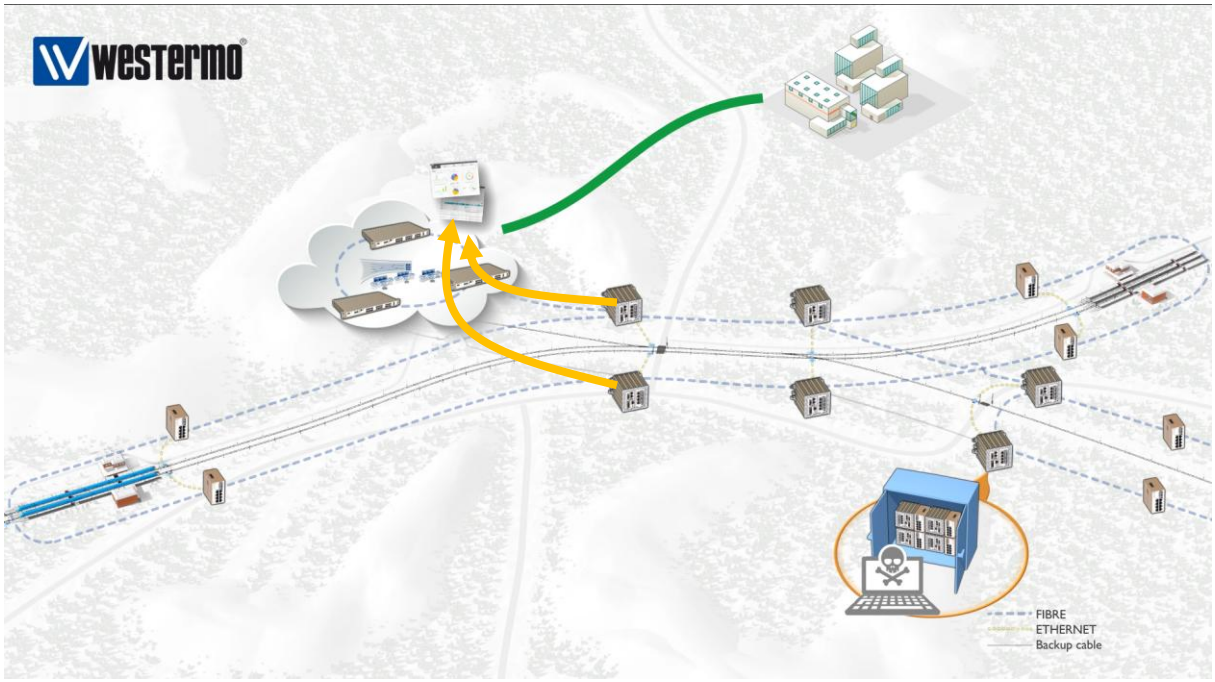

Figure 1 - Packets dropped in the filter are reported to the SEM

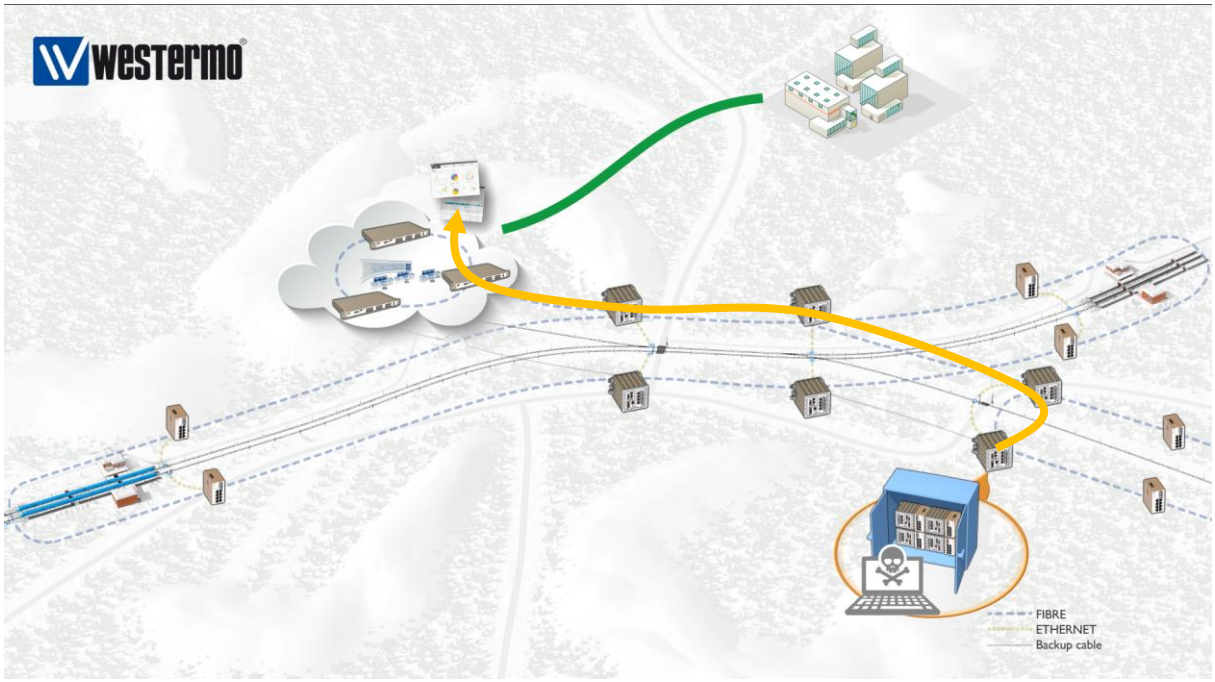

Figure 2 - Failed 802.1x authentication is reported to SEM

In more complex scenarios, there could be multiple sites with separate control systems that aren't connected to each other, but rather to a common regional control system. Manned stations would probably want to be able to see the security events from the local control system or systems, while the personnel at the regional control system would want to see security events from all stations.

The local SEM should therefore be able to forward all security events to a central SEM over protected channel, such as provided by the Network to Network application concept.

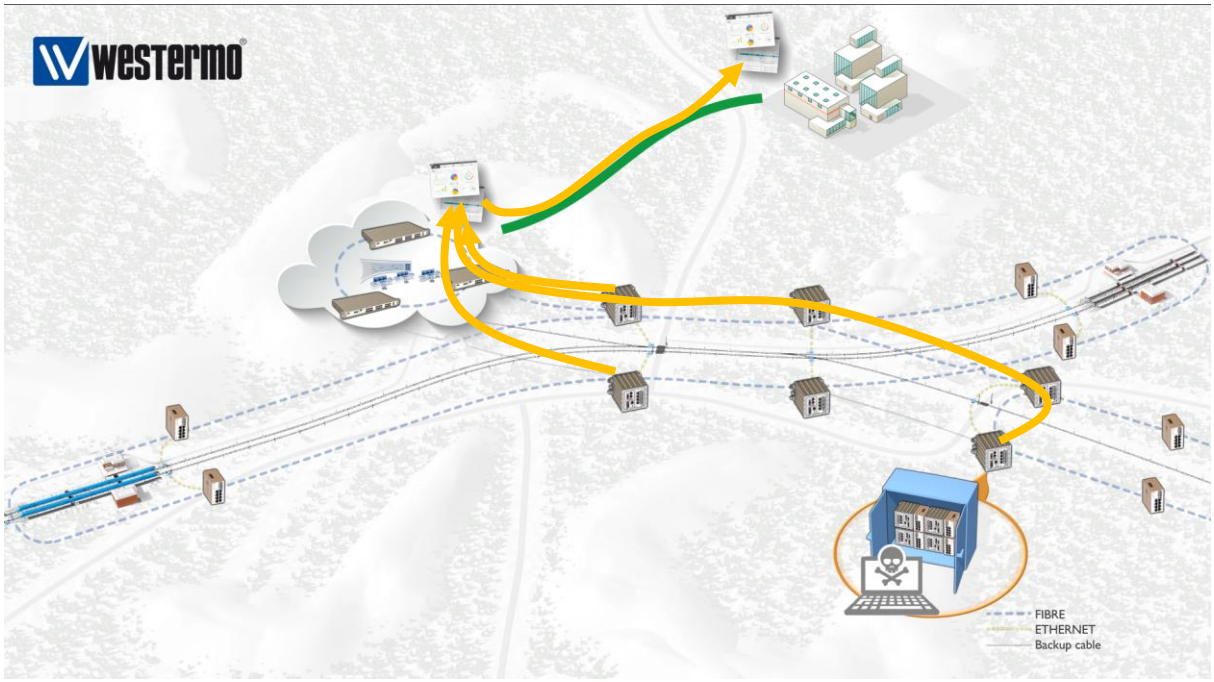

Figure 3 - Centralized SEM monitoring multiple sites

Westermo Teleindustri AB
SE-640 40 Stora Sundby, Sweden
Tel. +46 (0)16 42 80 00 I Fax. +46 (0)16 42 80 01
info@westermo.com I www.westermo.com

Corp ID No: 556361-2604
VAT: SE556361260401