LIGHTCYBER

Protecting SCADA and Industrial Control System Networks

LightCyber Magna safeguards critical infrastructure from cybercriminals, malicious insiders and state-sponsored attackers without affecting performance and uptime

Challenge

Defend sensitive industrial control systems from internal and external threats without impacting performance or reliability

Solution

LightCyber Magna delivers an intelligent and non-intrusive solution that detects advanced attacks and insider threats

Detect

movement and command and control in SCADA networks

Gain visibility

into network activity in highly-sensitive environments

Secure

both Operation Technology (OT) and Information Technology (IT) assets

Produce

security assurance reports for compliance

LightCyber Magna Behavioral Attack Detection secures industrial control system (ICS) networks by monitoring network traffic, users, and devices and building a baseline of expected behavior. Using machine learning, Magna can detect anomalous behavior indicative of attack. Because Magna focuses on post-intrusion activity such as reconnaissance and lateral movement, it is ideally suited to detect threats targeting or originating from SCADA systems.

Critical Infrastructure Under Siege

National security and prosperity depend on critical infrastructure and, often, critical infrastructure depends on ICS networks. From energy to transportation and agriculture to national defense, many commercial and government organizations rely on specialized industrial equipment. Attacks on these organizations' ICS networks could result in economic disruption or even loss of life. It's not surprising, then, that the World Economic Forum listed "Cyberattacks" and "Failure of Critical Infrastructure" as two significant global risks that nations face in 2017.

"Energetic Bear" APT managed to infect:

2,800	101	6
Systems	Organizations	Sectors

From the Stuxnet malware to an assault on Ukraine's power grid that cut power to 230,000 people for six hours, attacks on industrial controls are all too real. No country and no sector is immune to the threat. As a case in point, a single threat targeting industrial equipment, the "Energetic Bear" APT, managed to infect over 2,800 systems in 101 organizations across six sectors. Even non-targeted industrial equipment could become collateral damage in a widespread attack.

Protecting SCADA and Industrial Control System Networks

CASE STUDY:
A US electric delivery company secures its transmission equipment with LightCyber

A leading electric transmission and delivery company needed to secure its SCADA systems from threats and address process gaps.

The company's SCADA network was physically separated from other networks. As a result, security solutions that relied on cloud-based threat analysis or daily signature updates were not suitable for them and their focus was on internal device and user behavior. In addition, the OT team was reticent to deploy agents on their SCADA systems.

After comparing LightCyber Magna and another behavioral analytics solution, the company decided to implement Magna in their SCADA Network.

The OT team stated that Magna was easy to deploy; one Magna Detector appliance and several probes have been installed to monitor all traffic in their OT network.

The SOC team regularly reviews the Magna dashboard for signs of unusual activity. They also plan to generate LightCyber Magna Security Assurance Reports for their executive management.

Overall, LightCyber Magna helps the electric company protect its transmissions controllers and meet compliance without impacting SCADA network uptime or performance.

The Importance of Being Up

Critical infrastructure is, by definition, critical. Industrial controls that manage power transmission lines or water management systems must be available around the clock.

To ensure continuous operations, security teams might be reticent to install traditional anti-virus software on sensitive equipment, or SCADA equipment may be several years old and not support current anti-virus agents. Security teams may also wish to avoid deploying inline security products that could potentially block legitimate traffic.

Because many ICS networks are isolated through an air gap to other networks, an effective security solution should be focused on behavioral analysis, such as abnormal behavior and not on malware-based command and control activity or signatures to detect external attacks. In many cases, cloud-based threat intelligence is not even possible to deploy in these environments.

LightCyber Magna for SCADA and ICS Networks

Organizations can protect their SCADA networks and address compliance with LightCyber Magna Behavioral Attack Detection. LightCyber Magna accurately and efficiently detects advanced attacks, insider threats, and malware that have bypassed traditional security controls. LightCyber Magna employs on-premises supervised and unsupervised machine learning techniques to learn the expected behavior of users and devices. Then Magna detects the behavioral anomalies indicative of attack.

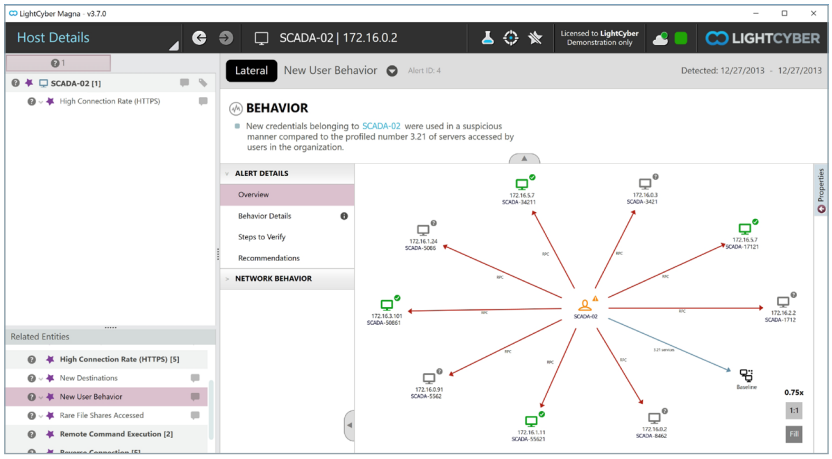


Figure 1: LightCyber Magna detects post intrusion activity such as lateral movement in SCADA networks.

Protecting SCADA and Industrial Control System Networks

LightCyber Magna profiles over 1,000 dimensions of user and device behavior to detect attacks. Its on-premises machine learning is impervious to signature evasion, SSL encryption, and zero day attacks because Magna is not looking for individual attack signatures.

In SCADA environments, once an attacker has infiltrated one system, the attacker may try to gain control of more systems. In the case of the Stuxnet attack, the Stuxnet worm leveraged several zero-day vulnerabilities to spread from one system to many more. The original system that propagated the worm would have exhibited anomalous network behavior—the type of behavior that LightCyber Magna is designed to detect.

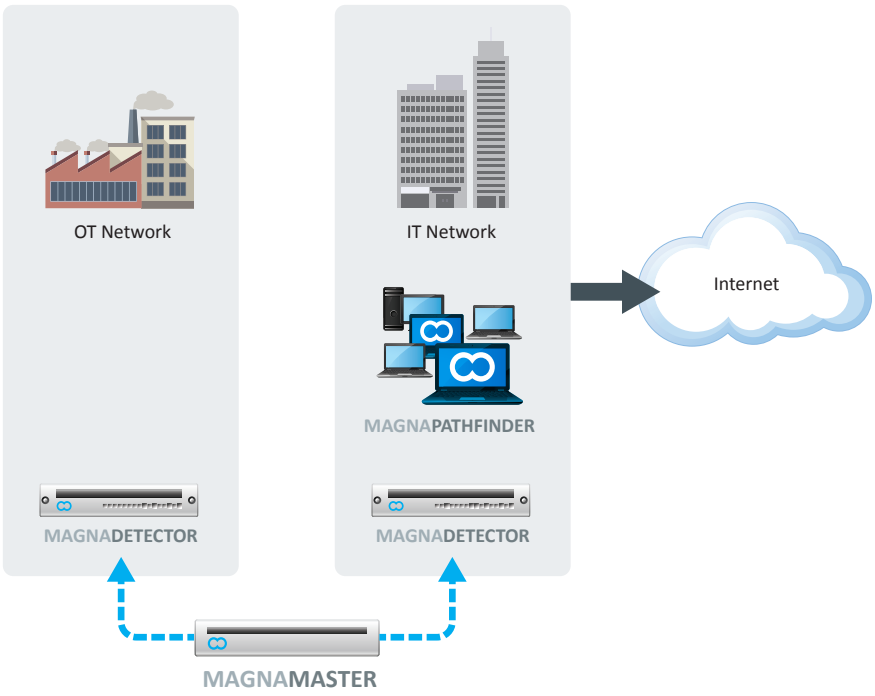


Figure 2: LightCyber Magna can monitor and secure OT and IT networks simultaneously. The Magna Master can centrally manage Magna Detectors deployed in OT and IT networks or each deployment can be managed separately.

Because most SCADA systems behave consistently, any deviations in behavior are easy to identify. Control nodes often communicate in standardized patterns using designated protocols. In many SCADA networks, nodes would only communicate with a small number of systems, such as control servers or management stations. Unusual behavior, such as a worm connecting to a vulnerable TCP port on many systems at once, or even human-operated lateral movement that affects only a handful of devices would stand out clearly in a SCADA network.

LightCyber Magna is well suited to detect reconnaissance and lateral movement in SCADA environments. In networks that are connected to the Internet, additional attack behaviors that Magna detect are relevant, such as command and control, data exfiltration and malware behavior.

Address Regulatory and Executive-Level Reporting Requirements

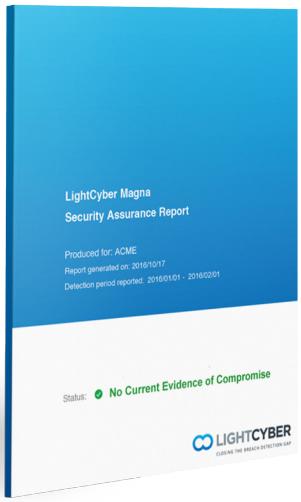
Because national security depends on the uptime and integrity of ICS networks, these networks are highly regulated. LightCyber Magna helps utilities address compliance requirements such as NERC CIPv5 by detecting internal threats in OT and in IT networks. LightCyber Magna satisfies the following requirements in CIP-005-5 table R1 by:

- Detecting known or suspected malicious communications for inbound and outbound communications (Part 1.5)
- Detecting malicious code (Part 3.1)
- Detecting successful and failed login attempts and failed access (Part 4.1)
- Generating alerts for security events such as detected malicious code (Part 4.2)
- Retaining event logs for at least 90 consecutive calendar days (Part 4.3)

Protecting SCADA and Industrial Control System Networks

- Identifying individuals who have authorized access to shared accounts (Part 5.3)
- Generating alerts after a threshold of unsuccessful authentication attempts (Part 5.7)

LightCyber Magna also allows organizations to demonstrate to regulators and auditors that there is no sign of an active attacker in a SCADA environment. The LightCyber Magna Security Assurance Report documents whether Magna security alerts have been reviewed and resolved, showing auditors as well as board members that suspicious activity has been investigated and that there is no evidence of compromise in the network.



Thwart Insider Attacks

Organizations that manage SCADA environments must also consider internal threats from malicious insider. With the access and the credentials they have, or can easily obtain, they can cause massive damage. And since they understand the environment, they should know what systems to target, how to access them, and even what security controls they will need to evade.

However, insiders cannot conceal their network behavior from Magna. If a malicious insider uses the network to manage or exploit SCADA systems or to expand their control to other systems, Magna can detect these actions and alert on any behavioral changes over time or any peer-based anomalies.

Conclusion

Critical infrastructure has never been under greater threat than today. As nation states look to undermine their adversaries without firing a shot, they have turned to stealthy cyber-attacks, and many of these attacks target critical infrastructure.

LightCyber Magna can uncover advanced attacks in SCADA networks before the damage is done, without requiring the installation of intrusive endpoint software or degrading network performance. LightCyber Magna detects dangerous threats, such as advanced attacks, insider threats and malware, by spotting behavioral anomalies and provides automated investigative data, enabling swift triage and resolution.

Learn how you can protect your ICS network with LightCyber Magna. Contact LightCyber today to learn how to receive a LightCyber Magna Security Assurance Report for your organization.

Find out more:

Visit our website (lightcyber.com) or call us at 1 650-388-9240 to start a PoV and assure your board of directors and executive that your network is safe and free from attackers.

LIGHTCYBER

5050 El Camino, Suite 226
Los Altos, CA 94022
Ph: (844) 560-7976
www.lightcyber.com