Securing Critical Infrastructure and the Industrial Internet of Things

The growing threat of cyberattacks to industrial targets is a major global concern and customers are demanding effective cybersecurity to assist and protect assets and people.

Critical Infrastructure Landscape

- 70% of critical infrastructure organizations suffered breaches in the last year¹
- 76% increase in Worldwide SCADA attacks from 2013 to 2014²
- Standards and regulations are now government mandated (i.e. NERC CIP)³

Real-World Breach

- Worm enters nuclear program’s system via USB stick
- Worm exploits multiple zero-day vulnerabilities of Windows Distributed Control Systems (DCS)
- Worm hides from automated detection systems
- Once vendor-specific DCS is found the worm morphs and begins attack
- Worm targets system’s logic controllers and spies on operations
- Worm gains control of centrifuges and provides false feedback to mask corruption in progress
- Worm destroys systems and damages machinery, causing over 6 countries to be affected

Security by Design

Protect industrial control systems, smart grids, sensors, monitors, robotic systems, communication, and network systems.

Learn more mcafee.com/embedded

Protect your system and data from exploits

Detect exploits of your systems and data

Correct damage to systems and lost or stolen data


Intel and the Intel and McAfee logos are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others.
Copyright © 2016 Intel Corporation. 62303info_embedded-critical-infrastructure_0316_kgs