CyberX at a Glance

- Founded in 2013 by military cyber experts with nation-state expertise defending critical infrastructure
- 4 Offices around the world
- Industrial cybersecurity platform build from the ground-up for OT
- Most widely-deployed solution
  - 500+ deployments world-wide
  - Oil & gas, manufacturing, energy, pharmaceuticals, chemicals, nuclear, water…
- – Northwest Venture Partners (NVP) backed
- Selected by best-of-breed cybersecurity partners

paloalto NETWORKS® IBM Security CYBERARK® OPTIV SECURITY Deutsche Telekom

CyberX Global ICS & IIoT Risk Report

A data-driven analysis of vulnerabilities in our critical industrial infrastructure (October 2017), based on analyzing 375 production ICS networks via proprietary Network Traffic Analysis (NTA) algorithms

The air-gap myth:

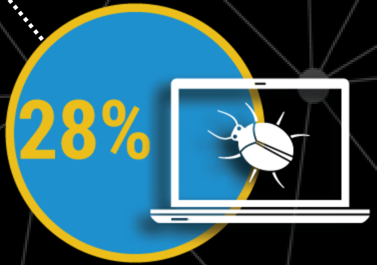
1 out of 3 industrial sites are connected to the public Internet

Weak authentication: 60% have passwords traversing the network in plain-text

These passwords can easily be sniffed by attackers performing cyber reconnaissance, who can later use the passwords to manipulate critical control systems

Un-patchable Windows everywhere: 3 out of 4 sites have Windows systems that are no longer provided with security patches from Microsoft

These systems can easily be compromised by modern ransomware, password-stealers, and back-doors (especially if they're Internet-facing!)



On average, 28% of all devices in each site are vulnerable (critical CVEs, open ports, etc.)

Critical CVEs represent serious vulnerabilities such as buffer overflows that provide the attacker with complete control of the device

https://cyberx-labs.com/en/iiot-ics-scada-security-knowledge-base/

50%

No AV protection: 50% of industrial sites aren’t running any antivirus

Lack of AV protection increases the risk of having known malware on these systems — such as Conficker, WannaCry, and NotPetya — without even knowing about it

61%

Median Security score across all sites: 61%

Significantly below the recommended minimum score of 80%. All industries are within +/- 5% of the overall median score

Manufacturing	Oil & Gas	Energy & Utilities	Pharmaceuticals /Chemicals
66%	63%	62%	56%

82%

82% are running remote access management protocols (RDP, SSH, etc.)

Once an attacker has compromised the OT network, it’s significantly easier for them to remotely access & control other devices

Distribution of industrial protocols

Industrial networks have a complex mix of specialized protocols, both open and proprietary, that are not visible to corporate IT monitoring tools

Modbus TCP	Ethernet/IP	Siemens S7/S7+	OPC	OSIsoft PI	MMS	Other (17)*
58%	28%	18%	16%	14%	12%	60%

* “Other” encompasses 17 industrial protocols that appeared in less than 10% of the sites: including: DNP3, GE SRTP, GE Turbine, Wonderware Suitelink, GE EGD, GE Bently Nevada, Schneider Electric Telvent, ABB HCS, DeltaV, Honeywell, Yokogawa Centum, Beckhoff, Mitsubishi MELSEC, ICCP, IEC 104, ISO, and GOOSE.