

Rapid OT Visibility and Continuous Monitoring for Critical Infrastructure Supporting Department of War

Industrial Defender OT Asset Management, Change Management, Vulnerability Management, and MOSAICS/NERC-CIP Compliance Reporting

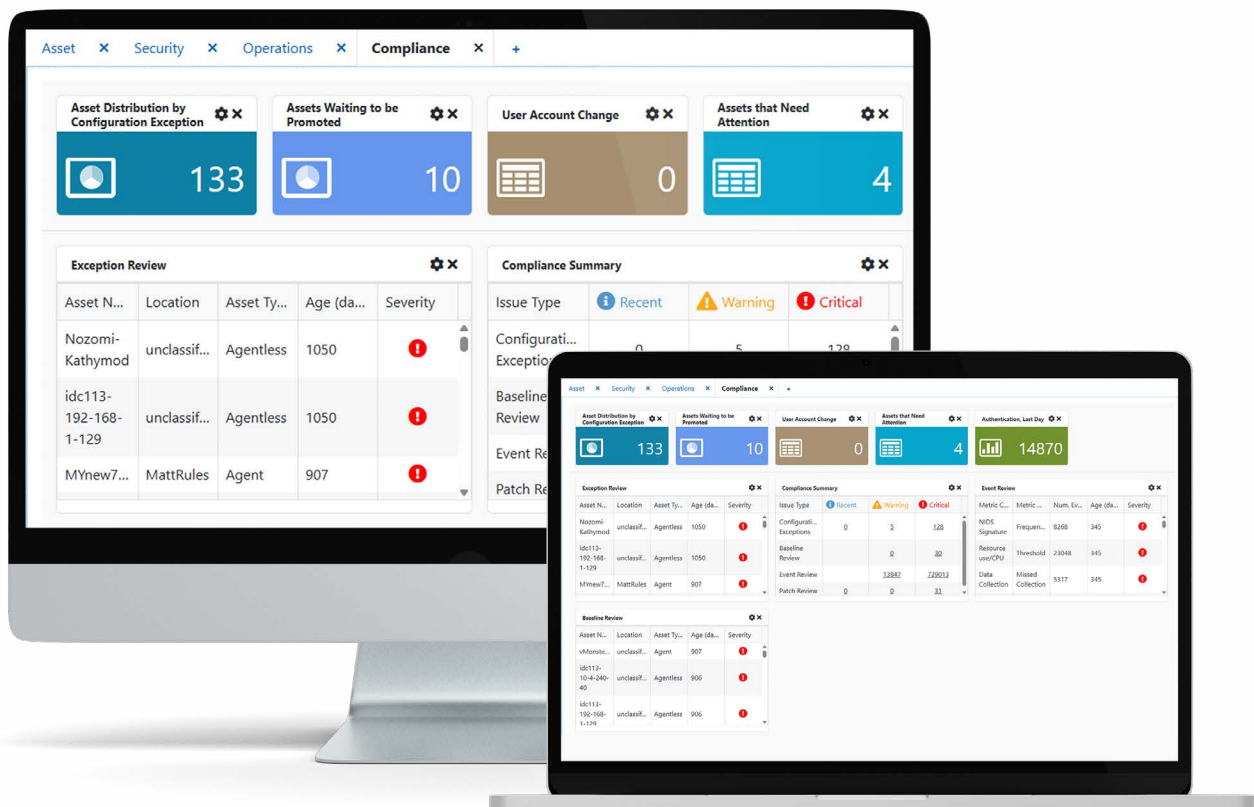
MISSION

A public-sector agency contracted with Industrial Defender to secure and sustain the highest levels of uptime for critical infrastructure supporting both public and private-sector operations across a strategic territory.

The engagement spanned power generation and distribution, water and wastewater treatment, and port operations, delivered through inter-agency collaboration for the affected entities.

CHALLENGE AND RESULTS:

14 working days to full sensor deployment	1,300+ OT/IT assets identified (from a baseline of zero)	1,500+ vulnerabilities identified across IT and OT	15 critical sites monitored across 4 facility types
---	--	--	---



“This engagement proved what Industrial Defender can deliver at scale: real-time OT visibility across a fragmented, high-risk critical infrastructure environment.”

— Industrial Defender

CHALLENGE

The partner entities had little to no visibility into their operational technology environments prior to engagement.

Asset inventories were not tallied while vulnerability posture was unknown, and there was no established baseline to detect malicious or unauthorized change in the OT environment.

Compounding the challenge, the region’s infrastructure had also sustained recent storm damage, limiting connectivity at some sites and constraining options for continuous, always-on monitoring.

APPROACH AND RESULTS

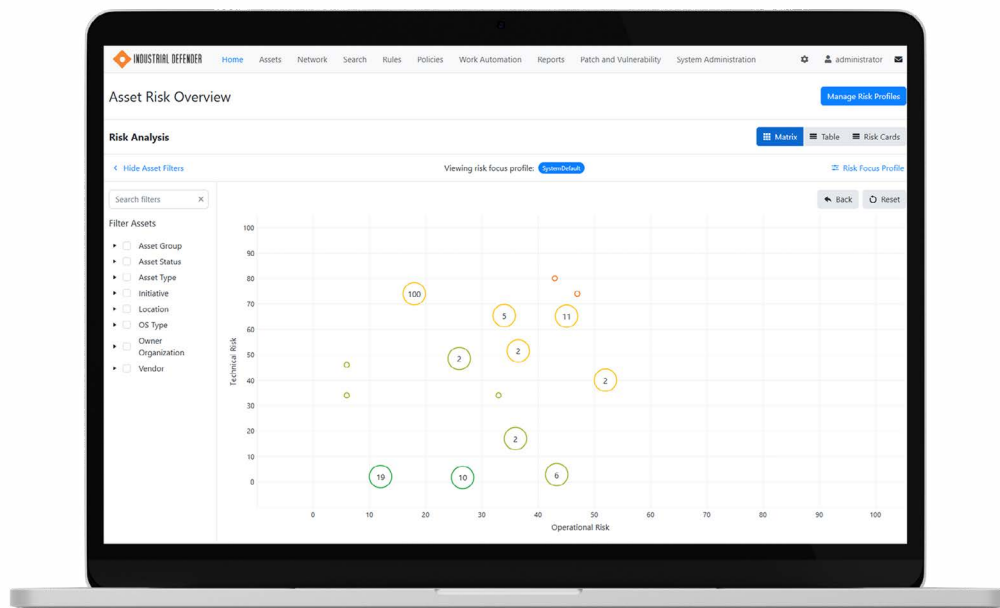
Working alongside the utility, water authority, and port operator, Industrial Defender deployed OT sensors and asset management capability across

- ▶ four wastewater treatment facilities
- ▶ two datacenters
- ▶ 30 substations
- ▶ and one port central yard

All accomplished in a mere 14 working days.

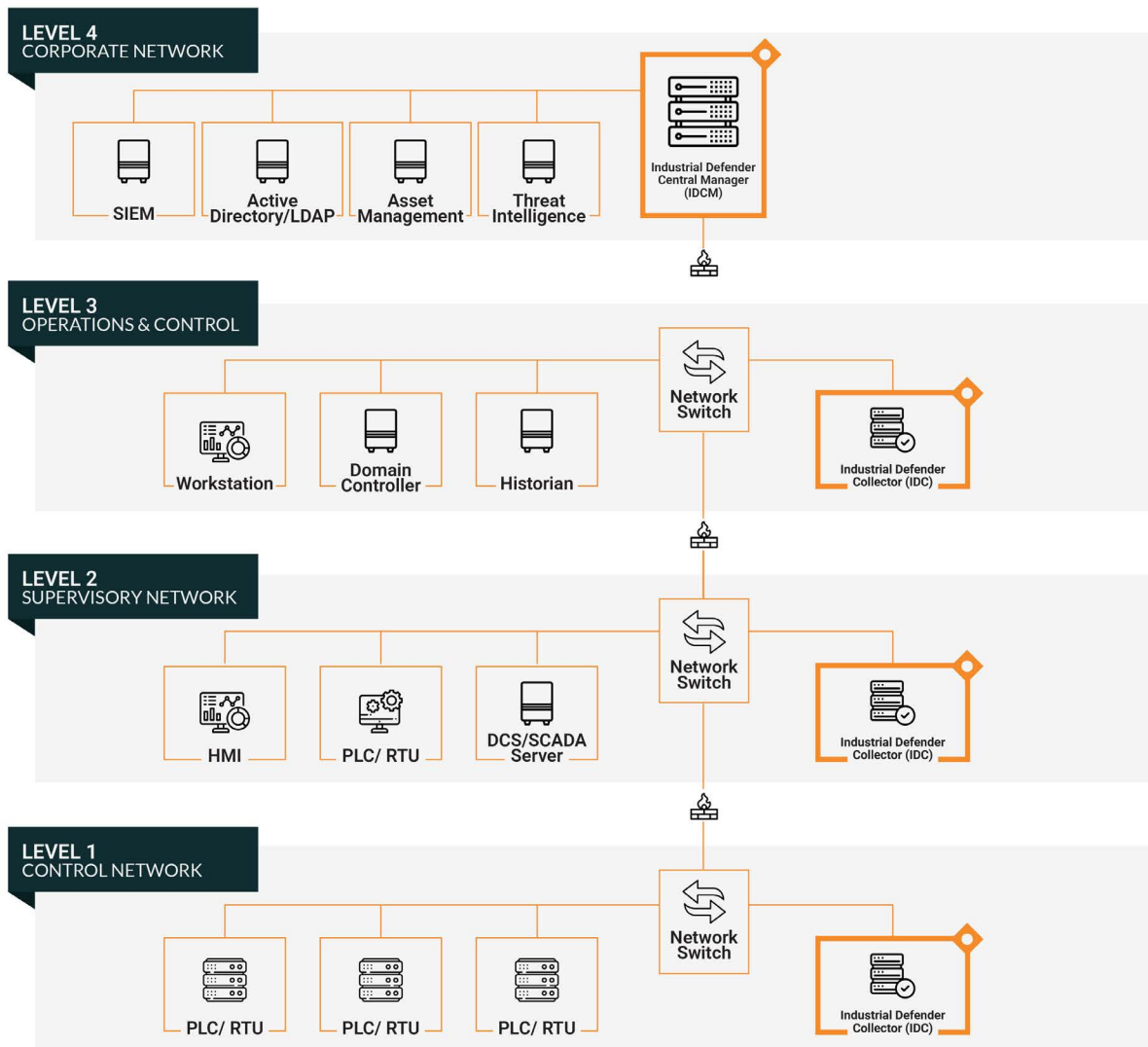
This rapid deployment took OT asset visibility from zero to more than 1,300 assets, enabling vulnerability reporting and change baselining across the environment for the first time.

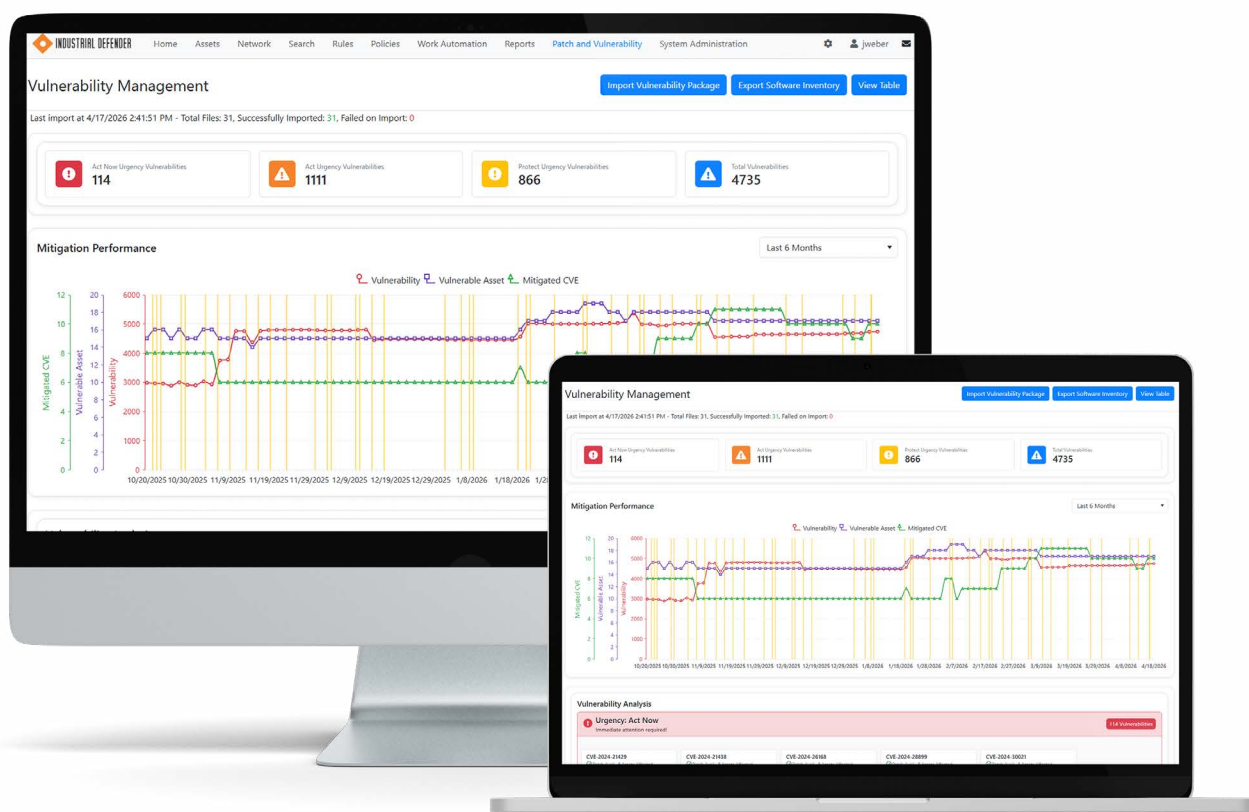
- ▶ **Vulnerability discovery:** More than 1,500 vulnerabilities were identified across IT and OT devices, with the highest operational impacted assets remediated in the first week and remediation continuing in the weeks following deployment.
- ▶ **Framework alignment:** Fully deployed, the platform positions the partner to achieve 21 of 23 (91%) **MOSAICS** Operational Requirements, 71 of 98 (72%) Functional Requirements, and 255 of 332 (77%) Technical Requirements — 347 of 453 total requirements (76.6%) — alongside alignment with **NERC-CIP**, the utility industry’s gold-standard compliance framework.



IMMEDIATE RESULTS:

- ▶ **Stale credentials:** Updated Passwords after accounts were found enabled with passwords unchanged for more than a year
- ▶ **Anomalous authentication:** Repeated failed logins from an unrecognized, unusually long username, and repeated “Guest” login attempts against another asset, were identified and blocked or disabled
- ▶ **Outdated OT/IT firmware:** Legacy field-device firmware and network OS versions at or approaching end-of-support were flagged as high-severity OT vulnerabilities and queued for patching and upgrade.
- ▶ **Unmanaged removable media:** Notable USB device activity was observed with no clear governing policy — reviewed by affected entities
- ▶ **Suspicious protocol behavior:** Passive monitoring of control-system protocol traffic surfaced two distinct high-frequency anomalous alarm patterns at a substation; each tied to a single asset communicating with multiple downstream devices
- ▶ **Unexplained configuration changes:** Continuous audit-policy changes on a single asset raised concern over unauthorized access; credentials were modified
- ▶ **Spoofed addressing:** One asset was found assigned to a public DNS provider’s IP address — a possible indicator of DNS poisoning — and was blocked at the firewall





Based in Massachusetts and protecting critical infrastructure since 2006, Industrial Defender serves many of the nation's largest power utilities as well as diverse global organizations with complex, demanding OT environments. Organizations turn to Industrial Defender to streamline compliance work related to NERC CIP, and NIS2 as well as comply with best practices associated with IEC 62443.

SCHEDULE A DEMO

CONTACT

1 (877) 943-3363 • (617) 675-4206
 info@industrialdefender.com
 225 Foxborough Blvd, Foxborough, MA 02035
[industrialdefender.com](https://www.industrialdefender.com)

© 2026 Industrial Defender, LLC. All Rights Reserved.

