NERC CIP-015 SOLUTION BRIEF

INDUSTRIAL DEFENDER®

Turn internal network visibility into a defensible NERC CIP-015 workflow.

Understand what is normal. Prioritize what is not. Preserve the evidence behind every decision.

BUILT INTO IDCM

Industrial network monitoring can produce enormous volumes of traffic data and anomalies. The challenge is not simply collecting more data. It's establishing expected network behavior, identifying meaningful deviations, determining what those deviations mean, and maintaining evidence of how each one was handled.

Industrial Defender brings network activity together with the asset, configuration, vulnerability, and historical context already available in IDCM — into one unified workflow for monitoring internal communications, evaluating anomalies, documenting decisions, and preparing defensible CIP-015 evidence.

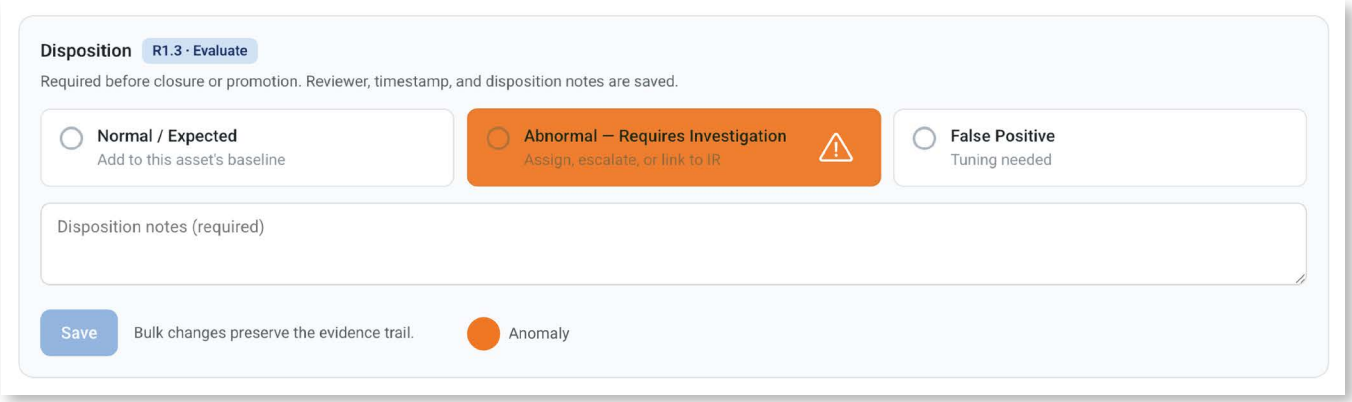
WHY IT'S DIFFERENT

1	2	3
Asset context prioritizes what matters	**Asset-centric, built into IDCM**	**The full CIP-015 workflow, end to end**
Network visibility becomes more actionable when deviations are tied to asset criticality, risk, impact, anomaly type, and unknown or unauthorized devices.	Network anomalies are reviewed alongside the asset information, risk, events, baselines, and reporting workflows customers already use.	Monitor network activity, detect deviations, evaluate what needs action, and retain/protect the evidence needed to support compliance — not just pieces of it.

ONE WORKFLOW, END TO END

01	02	03	04	05
Scope	**Baseline**	**Detect**	**Evaluate**	**Retain**
Define what must be monitored.	Establish expected network behavior.	Identify deviations from normal.	Turn anomalies into prioritized decisions.	Retain the complete record.

CIP-015 requires documented processes for risk-based network data feeds, anomaly detection, and anomaly evaluation — with anomalous network data retained until the associated action is complete, protected against unauthorized deletion or modification, and generally retained for three calendar years.



THE ANOMALY WORKSPACE

Network deviations are presented in one consolidated, prioritized queue — rather than forcing analysts to investigate isolated alerts across multiple tools or product areas.

Each deviation shows

- Assets and communication endpoints involved
- Source and destination IP addresses
- Port and protocol
- First and last observed time
- Frequency and traffic volume
- Deviation type
- Asset criticality and risk
- Related configuration changes, vulnerabilities, and security events
- Current review state, reviewer, and disposition

Suggested deviation categories

Connection deviations
New or changed source, destination, session, or communication path.

Port & protocol deviations
Unexpected ports, protocols, or communication methods.

Device deviations
New, unknown, unauthorized, or provisional devices participating in communication.

Volume & timing deviations
Unexpected traffic increases or decreases, unusual cadence, or repeated beaconing behavior.

DEPLOYMENT

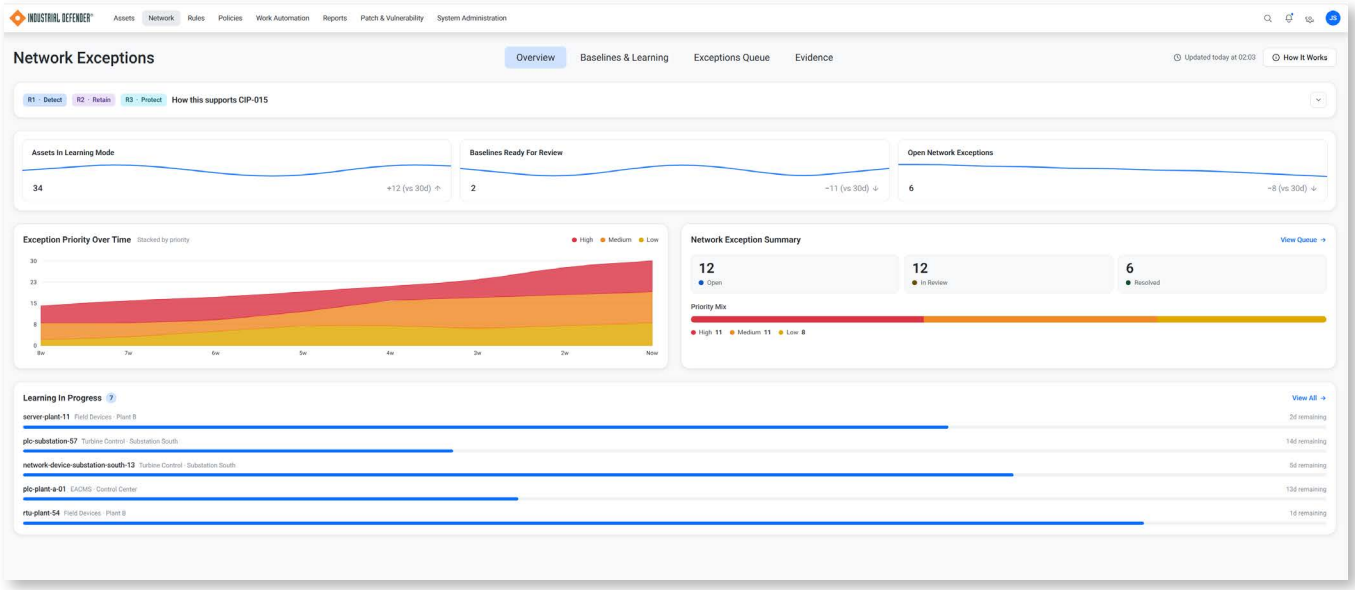
Network baselines are only as strong as the collection underneath them. Industrial Defender reaches Purdue Level 1 through Passive Monitoring, agentless active collection (IDC), and a persistent Agent — see the Deployment page for a full breakdown of all three methods.

FROM VISIBILITY TO PRIORITIZATION

Inputs
Network baseline · NetFlow/ IPFIX · asset identity & criticality · configuration history · vulnerabilities · known relationships · threat & event context · collection coverage

Prioritize
Highest operational consequence · critical assets · unknown/unauthorized devices · significant behavioral deviation · suspicious patterns · correlated changes · CIP-008 escalation

Output
An explainable, auditable decision: what was detected, why it was prioritized, which assets were affected, who reviewed it, when, and what action followed.



A DYNAMIC NETWORK BASELINE

The network baseline is not a static whitelist. It supports an ongoing lifecycle. Users can evolve normal behavior without losing the history of what changed, who approved it, or why.

01	02	03	04	05
Learn	**Review**	**Promote**	**Monitor**	**Update**
Observe communication patterns during a controlled learning period.	Validate learned connections, protocols, ports, devices, and traffic characteristics.	Approve expected behavior into the authoritative baseline	Continuously compare current communications against the approved baseline.	Add legitimate new behavior with reviewer attribution and justification.

EVALUATION & CHAIN OF CUSTODY

Every anomaly preserves both the technical evidence and the decision history — extending familiar IDCM review mechanics rather than introducing a separate compliance process.

Review lifecycle

- New ▸ Under review
- Approved and added to baseline
- Suppressed or false positive
- Investigating
- Escalated or exported to incident response
- Closed

Evidence captured at every transition

- Reviewer, timestamp, comment/rationale
- Previous and new status
- Related asset and communication details
- Supporting reports or files
- Linked incident or ticket
- Relevant retained network data

NETWORK ACTIVITY IN FULL ASSET CONTEXT

Many network monitoring tools can identify that a communication changed. Industrial Defender helps explain what that change means to the operating environment — by correlating network deviations with the asset information IDCM already maintains, so analysts can answer:

Is asset risk score high?	**Has its configuration recently changed?**	**Linked to known vulnerabilities?**

This network-to-endpoint correlation is the central differentiator: connect what happened on the network with what changed on the asset.

CAPABILITIES & BENEFITS

001	**Risk-based monitoring scope** Document which network segments and data feeds are monitored and why.	**002**	**Network communication baselines** Define expected paths, ports, protocols, traffic levels, and timing.
003	**Consolidated anomaly queue** Bring network and asset-related anomalies into one review workflow.	**004**	**Asset-aware prioritization** Use criticality, risk, and vulnerabilities to identify what matters first.
005	**Network-to-endpoint correlation** Connect unusual communications with configuration and asset history.	**006**	**Explainable deviation review** Document whether activity is expected, abnormal, or false positive
007	**Auditable reviewer workflow** Capture who reviewed each anomaly, when, and why.	**008**	**Protected evidence retention** Retain and protect records with access control and audit history.
009	**CIP-015 reporting** Generate baseline, anomaly, coverage, and evidence reports.	**010**	**Embedded in IDCM** No new license, tool, or login — built into the platform you use today.

BEFORE

Fragmented network alerts and manual evidence collection, disconnected from asset context.

AFTER

One prioritized workflow with full asset context and an auditable decision record.

REQUIREMENT MAPPING AT A GLANCE

The approved CIP-015-1 standard is organized around three operational requirements: monitor, detect, and evaluate; retain relevant anomalous data; and protect collected and retained data from unauthorized deletion or modification.

Req.	Customer objective	Industrial Defender solution support	Primary evidence
R1.1	Define a defensible monitoring scope and risk-based network data feeds.	Configure monitored networks and collection points; ingest NetFlow/IPFIX and asset discovery data; map coverage to assets, segments, collectors, and topology.	Scope and rationale report; asset inventory; coverage and topology evidence.
R1.2	Detect anomalous network activity using those feeds.	Use a dynamic communication baseline plus detectors for new paths, ports, protocols, devices, external ingress, timing, volume, direction, drift, and suspicious patterns.	Baseline report; policy settings; anomaly records; baseline tuning.
R1.3	Evaluate anomalies and determine further action.	Review a prioritized queue with asset context; classify activity as expected, abnormal, or false positive; update the baseline; assign, investigate, escalate, export, or close.	Reviewer, timestamp, rationale, status history, disposition, linked ticket or incident.
R2	Retain data associated with anomalous activity at least until the related action is complete.	Apply configurable retention by queue state and disposition; retain linked evidence while it is still required; support longer evidence retention and per-item overrides.	Retention policy report; effective settings; data availability; exception and override history.
R3	Mitigate unauthorized deletion or modification of collected and retained INSM data.	Use RBAC, audit logs, restricted database access, controlled file permissions, encryption, hash-based integrity detection, and configurable storage destinations.	Protection status report; permissions and encryption status; audit logs.

FREQUENTLY ASKED QUESTIONS

How does this fit with our existing network monitoring? Does active collection require agents? What counts as a deviation? Find answers to these questions and more on our CIP-015 FAQ page.

Do more than collect network data. Build a defensible monitoring program.

See what changed. Understand what it means. Show how it was handled.

1 (877) 943-3363 • (617) 675-4206 | info@industrialdefender.com | 225 Foxborough Blvd, Foxborough, MA 02035
industrialdefender.com

SCHEDULE A DEMO