CASE STUDY · MANUFACTURING · ORANGE COUNTY, CA

From OT Blind Spot to Secured Factory Floor

0	118	100%	2 hrs
CRITICAL VULNERABILITIES	DAYS TO CMMC READINESS	OT/IT SEGMENTATION	RESPONSE SLA

CLIENT SNAPSHOT

CLIENT	INDUSTRY	STAFF	LOCATION	TIMELINE
Ironclad Precision Manufacturing	**Defense Subcontractor · CNC Machining**	**145 Users · 2 Facilities**	**Anaheim / Garden Grove, CA**	**118 Days**

THE CHALLENGE

A DoD contract win that exposed a decade of deferred IT investment

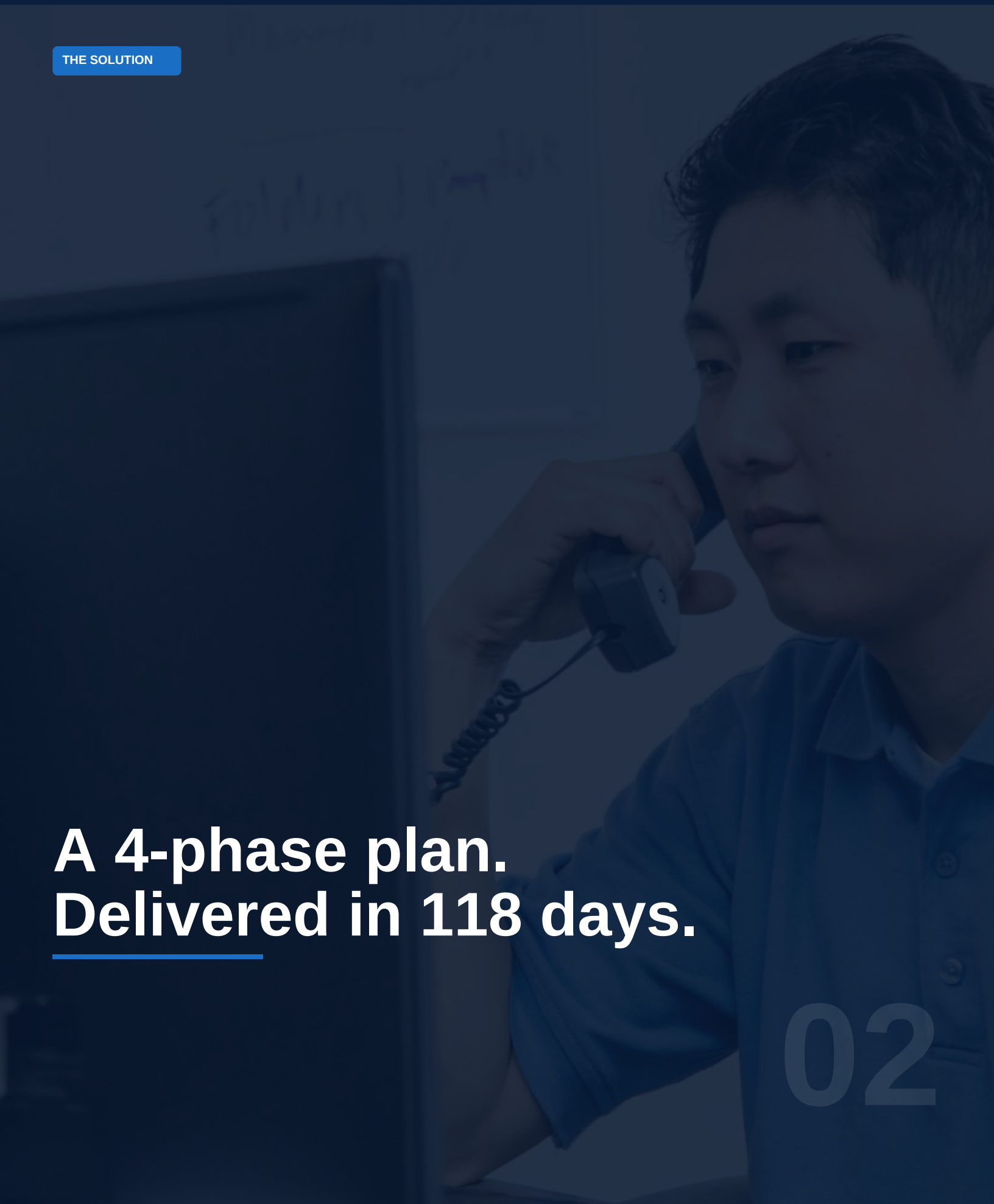
Ironclad Precision Manufacturing had built a strong reputation producing aerospace and defense components across two Orange County facilities. When the company was awarded a new DoD subcontract in mid-2024, the contract required CMMC Level 2 compliance — triggering the first formal cybersecurity assessment in the company's history. The results were alarming.

A vulnerability scan identified 14 critical vulnerabilities, including several on Windows 7 CNC machine controllers that had never been patched or isolated from the corporate network. Controlled Unclassified Information related to defense drawings and specifications was stored on an unencrypted file server with no access logging. The company's operational technology network — encompassing CNC machines, PLCs, and quality systems — was fully flat with the corporate IT network, creating catastrophic lateral movement risk. With a CMMC assessment window of 120 days, the company engaged Advanced Networks to lead the remediation.

RISK PROFILE AT INTAKE

CRITICAL	14 unpatched critical vulnerabilities including on CNC machine controllers
CRITICAL	OT and IT networks fully flat — no segmentation between factory and corporate
HIGH	CUI stored on unencrypted file server with no access logging or controls
HIGH	No MFA on any employee, engineering, or administrative account
MEDIUM	Legacy Windows 7 CNC controller endpoints with no available patch path
LOW	No documented incident response plan or employee cybersecurity training

THE SOLUTION



A 4-phase plan. Delivered in 118 days.

02

THE SOLUTION

A 4-phase CMMC Level 2 remediation plan built around NIST SP 800-171

Advanced Networks structured a 118-day engagement mapped to CMMC Level 2's 110 NIST SP 800-171 practices — prioritizing OT/IT segmentation and CUI protection to eliminate the most critical exposure before the assessment window opened.

PHASE 01

Assessment & CMMC Gap Analysis

Days 1–16

Conducted a full CMMC Level 2 gap assessment mapped to all 110 NIST SP 800-171 controls, inventoried every IT and OT asset across both facilities, and produced a prioritized System Security Plan with a Plan of Action and Milestones ready for C3PAO review.

✓ Full IT and OT asset inventory across 2 facilities
✓ CMMC Level 2 gap analysis mapped to all 110 controls
✓ System Security Plan (SSP) draft
✓ Plan of Action and Milestones (POA&M;) for C3PAO submission

PHASE 02

OT/IT Segmentation & Critical Patching

Days 17–52

Designed and implemented full OT/IT network segmentation using industrial-grade next-generation firewalls, creating isolated zones for CNC machines, PLCs, quality systems, and corporate IT. Patched all reachable critical vulnerabilities and implemented compensating controls for legacy Windows 7 CNC endpoints.

✓ OT/IT segmentation: dedicated firewall and VLAN architecture
✓ Isolated zones for CNC, PLC, quality, and corporate networks
✓ All 14 critical vulnerabilities patched or compensating controls applied
✓ Legacy CNC endpoints isolated with application whitelisting

PHASE 03

CUI Protection, MFA & Endpoint Security

Days 53–88

Migrated CUI from the unencrypted file server to a CMMC-compliant SharePoint environment with sensitivity labels, access logging, and DLP policies. Enforced MFA across all 145 accounts and deployed enterprise EDR across all corporate endpoints. Implemented encrypted backup with air-gap replication for CUI data.

✓ CUI migrated to CMMC-compliant environment with DLP
✓ MFA enforced across all 145 accounts
✓ EDR deployed across all corporate and engineering endpoints
✓ Encrypted backup with air-gap replication for CUI

PHASE 04

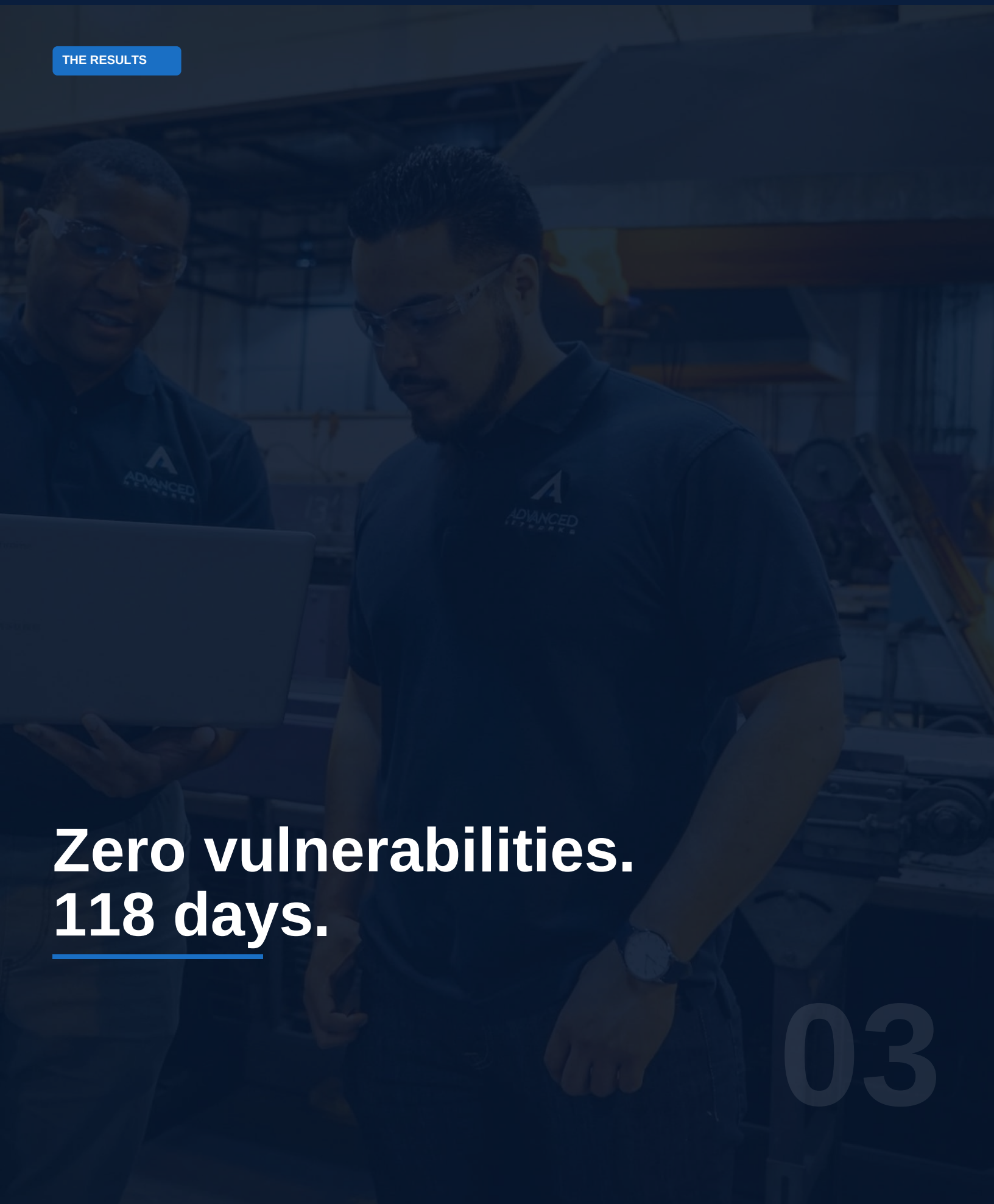
Training, Documentation & CMMC Readiness

Days 89–118

All 145 employees completed CMMC-aligned cybersecurity awareness training. The company's System Security Plan and POA&M; were finalized and reviewed for C3PAO submission. Enrolled in 24/7 SOC monitoring with OT-aware threat detection.

✓ 145-user CMMC security awareness training (100% completion)
✓ Final SSP and POA&M; documentation for C3PAO assessment
✓ 24/7 SOC monitoring with OT-aware threat detection
✓ Quarterly CMMC compliance review schedule established

THE RESULTS



Zero vulnerabilities. 118 days.

THE RESULTS

CMMC Level 2 ready. OT fully segmented. Zero critical vulnerabilities. 118 days.

0 Critical vulnerabilities remaining (down from 14)	**118** Days to CMMC Level 2 assessment readiness	**100%** OT/IT segmentation across both facilities
2 hrs Maximum incident response SLA	**$0** Contract penalties or compliance findings since remediation	**24/7** SOC monitoring with OT-aware detection

> *"We had 120 days to pass a CMMC assessment or risk losing a contract that represented a third of our revenue. Advanced Networks hit every deadline, navigated the complexity of our factory floor network with real expertise, and got us to the finish line with three days to spare. I wouldn't trust anyone else with our OT environment."*
>
> **— VP of Operations, Ironclad Precision Manufacturing**
> **Defense Subcontractor · Anaheim, Orange County**