

# 5 CYBERSECURITY TACTICS DEFENSE CONTRACTORS USE TO STAY CMMC COMPLIANT AND SECURE INTELLECTUAL PROPERTY

## Why It Matters



The aerospace and defense supply chain is under constant attack.

Nation-state groups target CAD files, communications, subcontractor networks, and test systems.

## Checklist

- Falcon EDR deployed across dev, test, and engineering environments
- Falcon Identity and Falcon Discover active for access and asset visibility
- Vulnerability remediation mapped via Falcon Exposure
- CMMC logging streamlined via Cribl Stream
- Lateral movement detection active with Corelight and Zeek
- AWS GovCloud and FedRAMP ready



### Step 1

#### CEO

Protect intellectual property and preserve government contracts

#### CISO/CTO/CIO

Use Falcon EDR to detect and contain threats in workstations, lab systems, and testbed infrastructure

#### Security Ops

Reduce alert fatigue by correlating endpoint telemetry with behavioral insights and threat intelligence



### Step 2

#### CEO

Avoid contract loss by passing CMMC reviews with clear access control evidence

#### CISO/CTO/CIO

Monitor and enforce user behavior policies with Falcon Identity and enforce least privilege across R&D zones

#### Security Ops

Detect anomalies in access patterns across secure email, design repositories, and subcontractor portals

ThreatDefend, powered by Vijilan, enables CMMC-aligned defense with:

**CrowdStrike Falcon** for EDR, Identity, cloud workload protection, and CMMC-aligned vulnerability management

**Cribl Stream** to route, retain, and redact logs from sensitive systems for DFARS and CMMC Level 2 audits

**Corelight** with Zeek to inspect internal traffic between engineering, testing, and external collaboration environments

**AWS GovCloud** infrastructure for FedRAMP and ITAR-aligned operations



### Step 3

#### CEO

Preserve vendor confidence and program integrity with full visibility and incident traceability

#### CISO/CTO/CIO

Prioritize vulnerabilities mapped to CMMC and DFARS controls using Falcon Exposure

#### Security Ops

Track which CVEs expose CUI and quickly generate remediation plans tied to audit logs



**Your contract. Your designs. Your reputation.**

**Get a Free Cyber Readiness Assessment for Defense Contractors and Supply Chain Partners**

