TECH BRIEF

CMMC For Insider Risk Programs

How an Integrated Insider Risk Program Helps Defense Contractors, Meet CMMC Requirements and Protect What Matters Most.

A technical paper for CISOs, ISSMs, Insider Threat Program leads, and Contracts officers preparing for CMMC assessments.

EVERFOX

Know what authorized users are doing. Get deep technical visibility that delivers behavior-based risk modeling, proactive misuse detection, and response that drives continuous organizational improvements.

Know what authorized users are doing. Get deep technical visibility that delivers behavior-based risk modeling, proactive misuse detection, and response that drives continuous organizational improvements.

Executive Summary

The Cybersecurity Maturity Model Certification (CMMC) Program, codified at 32 CFR Part 170, asks every organization in the Defense Industrial Base to do something harder than pass an audit: demonstrate - with evidence - that the people, systems, and processes handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) are working together to protect it.

Insider risk is where that demand concentrates. Many CMMC security requirements at Levels 2 and 3 are, at their core, about **knowing what authorized users are doing, separating intent from accident, and rapidly responding to incidents with audit artifacts continuously captured, retained, and ready for rapid response.**

This paper maps the capabilities of a modern insider risk stack - User Activity Monitoring (UAM), User and Entity Behavior Analytics (UEBA), and investigative Case Management - to specific CMMC requirement families, and describes the outcomes a defense contractor can expect from operating them as a unified program.

The goal isn't to pass an assessment. The goal is **Speed to Clarity** - moving from an alert to an answer fast enough to protect the mission, the workforce, and the contract.

A mature Insider Risk Management (IRM) solution is your foundation toward sustainable, scalable, and effective insider risk mitigation.

While a lot of cybersecurity focuses on firewalls and external bad actors, CMMC recognizes that a significant threat to CUI is the people using the network and the sensitive data it contains.

EverShield is a national-security-grade insider risk management platform trusted by 100+ government entities and Fortune 500 companies around the world. Built by analysts for analysts, EverShield combines deep user activity monitoring, data-source agnostic behavioral analytics, advanced linguistic analysis, and case management to facilitate productivity and performance to address real world risk scenarios.

- Improve insider threat prevention
- Reduce insider incidents with early detection
- Reduce alert triage and investigation time

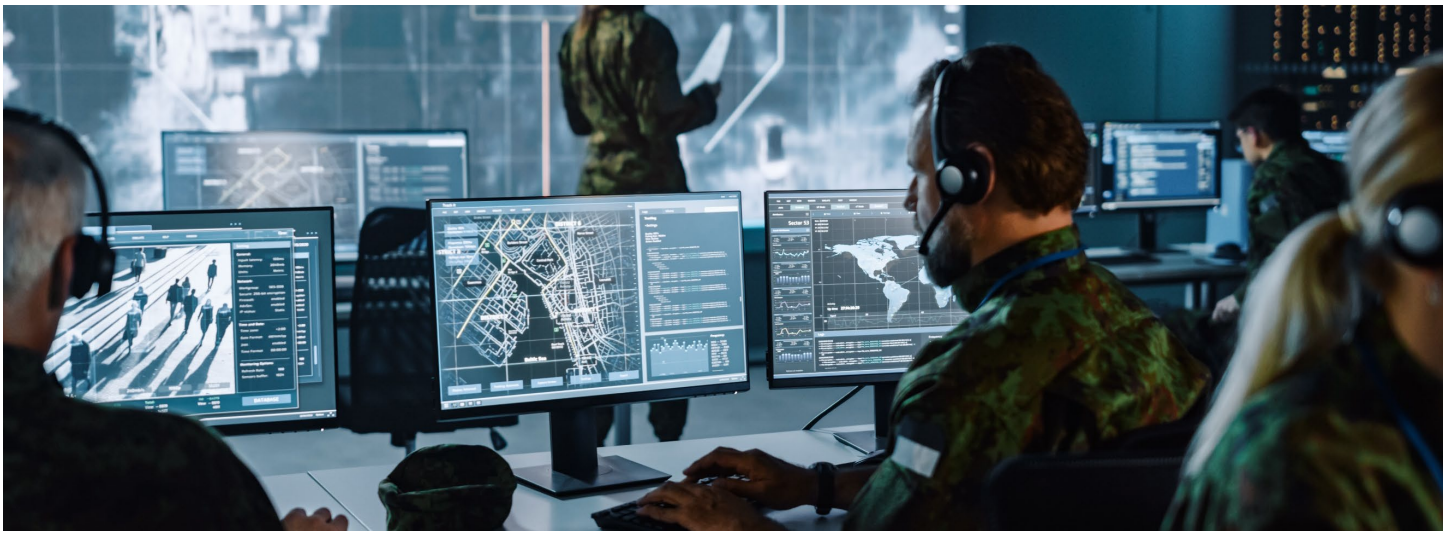
The CMMC Landscape Overview

CMMC organizes cybersecurity expectations into three levels, each with a distinct scope, assessor, and rulebook:

Level	Protects	Requirements	Assessment
Level 1	Federal Contract Information (FCI)	15 basic safeguarding requirements from FAR 52.204-21	Annual self-assessment
Level 2	Controlled Unclassified Information (CUI)	110 requirements from NIST SP 800-171	Self-assessment or C3PAO certification
Level 3	CUI under advanced persistent threat (APT) conditions	24 additional enhanced requirements from NIST SP 800-172, on top of Level 2	DCMA DIBCAC certification only

Each requirement is verified through **assessment objectives** - determination statements in NIST SP 800-171A and 800-172A that must *all* be MET. Assessors rely on three methods - **examine, interview, and test** - applied to four kinds of objects: specifications, mechanisms, activities, and individuals.

What this means in practice: compliance rests on producing defensible evidence that a control is implemented correctly, operating as intended, and producing the desired outcome. For the control families that govern user behavior, data movement, and incident response, that evidence almost always comes from the same places - an activity record, an analytic signal, a case file.



Why Insider Risk Sits at the Center of CMMC

A review of the Level 2 and Level 3 requirement catalogue makes the pattern clear. The control families most directly supported by an integrated insider risk program include:

- **Access Control (AC)** - authorized use, least privilege, session controls, remote access.
- **Audit and Accountability (AU)** - system auditing, event review, audit correlation, audit protection.
- **Awareness and Training (AT)** - insider threat awareness, role-based training.
- **Configuration Management (CM)** - baseline enforcement, least functionality, user-installed software.
- **Identification and Authentication (IA)** - identifier handling, authentication lifecycle.
- **Incident Response (IR)** - incident handling, reporting, and testing.
- **Personnel Security (PS)** - screening, personnel actions, and (at Level 3) adverse information.
- **Risk Assessment (RA)** - risk assessments, vulnerability identification, and (at Level 3) threat hunting and threat-informed risk assessment.
- **Security Assessment (CA)** - control monitoring, System Security Plan (SSP), operational plan of action.
- **System and Information Integrity (SI)** - monitoring for attacks, identifying unauthorized use.

An organization that can *see* what users do, *separate* unusual from unusual-and-concerning, and *resolve* the concerning ones with full audit fidelity is an organization that has already done most of the evidentiary work CMMC assessors look for.

The Three Capabilities, and What They Produce

1 - User Activity Monitoring

Objective Evidence on the Endpoint

A modern UAM platform - in this paper, represented by **Everfox EverShield UAM** - places a lightweight agent on Windows, Linux, and Mac endpoints and collects a detailed record of user activity: file operations, logons, web activity, keyboard and window focus, removable media use, and (when policy permits) video of the session.

Designed to enable:

- **AU.L2-3.3.1 System Auditing** and **AU.L2-3.3.2 User Accountability** - a continuous, attributable record of user actions that survives log tampering on the endpoint.
- **AC.L2-3.1.21 Portable Storage Use**, **AC.L2-3.1.20 External Connections [CUI Data]**, **SC.L2-3.13.1 Boundary Protection [CUI Data]** - observable evidence when CUI crosses a trust boundary via USB, cloud upload, or email attachment.
- **AT.L2-3.2.3 Insider Threat Awareness** - concrete training content drawn from real (de-identified) activity patterns, which makes awareness programs more credible to an assessor than slideware alone.
- **SI.L2-3.14.7 Identify Unauthorized Use** - a direct, assessable answer to the determination statement "unauthorized use of the system is identified."

The value isn't the volume of data; it's **the ability to answer the question "what actually happened on this workstation, at this time, with this file?"** without reconstructing it from logs that weren't designed to answer that question.

2- User and Entity Behavior Analytics

Context That Drives Action

A UAM platform shows what happened. A UEBA platform - represented here by **EverShield Behavioral Analytics** - tells you whether what happened is *unusual*, and whether it matters.

Behavioral analytics ingest activity events, email, chat, and file operations; apply an analytic chain of **lexicons → features → models → scenarios** (the Risk-Based Behavioral Analytics Model, RBAM); and publish an hourly risk score and level per monitored entity.

CMMC requirements this directly supports:

- **RA.L2-3.11.1 Risk Assessments** - risk scoring that updates as behavior changes, rather than point-in-time self-attestation.
- **RA.L3-3.11.1e Threat-Informed Risk Assessment** and **RA.L3-3.11.2e Threat Hunting** - analytic scenarios configured around current threat intelligence, with a search language (RQL) purpose-built for hypothesis-driven hunts.
- **SI.L2-3.14.3 Security Alerts and Advisories** and **SI.L3-3.14.6e Threat-Guided Intrusion Detection** - alerts tied to entity-level risk changes, not just signature matches.
- **AU.L2-3.3.5 Audit Correlation** - analytic correlation across email, chat, endpoint activity, and file events as a single entity timeline.
- **PS.L3-3.9.2e Adverse Information** - the analytic layer where a change in behavior can be surfaced alongside a personnel event, under proper access controls, to the authorized reviewers.

The important outcome is not "more alerts." It's **fewer, better alerts** - the move from **alert to answer** that a CMMC assessor and an analyst both care about.

3- Investigative Case Management

Defensible Resolution

Detection without disciplined resolution is an audit finding waiting to happen. **Everfox Case Management** provides a defense-grade, COTS investigative case management platform that turns a signal into case documentation designed to support courtroom admissibility.

CMMC requirements this directly supports:

- **IR.L2-3.6.1 Incident Handling**, **IR.L2-3.6.2 Incident Reporting**, **IR.L2-3.6.3 Incident Response Testing** - a single system of record for intake, triage, assignment, and closure, with enforceable deadlines and tested workflows.
- **CA.L2-3.12.2 Operational Plan of Action** - the operational plan of action called out in 32 CFR § 170.4 is itself a document to be managed, versioned, and attributed; Case Management is built for exactly that.
- **CA.L2-3.12.4 System Security Plan** - the SSP and its supporting artifacts benefit from the same version control, check-in/check-out, and hash-verified integrity that case files receive.
- **AU.L2-3.3.8 Audit Protection** and **AU.L2-3.3.9 Audit Management** - immutable audit history on every record, with need-to-know access controls at the record, file, and field level.
- **MP.L2-3.8.1 Media Protection** and **MP.L2-3.8.3 Media Disposal [CUI Data]** - evidence - including removable media imaged during an investigation - kept under chain of custody from acquisition to disposition.
- **PS.L2-3.9.1 Screen Individuals** and **PS.L2-3.9.2 Personnel Actions** - the administrative record that substantiates screening decisions and the actions that followed.

The outcome is the ability to move from **alert to answer to action** with a paper trail that holds up in an assessment, a contract dispute, or a courtroom.

Integration: Why the Three Are Stronger Together

Each capability is valuable on its own. Together they close a loop that is otherwise very hard to close inside a CMMC assessment:

1 

UAM produces the facts. An analyst working a scored entity can click through to the endpoint evidence record in the UAM Investigation Workbench on the Web (IWW) - the "View Source" integration introduced in UEBA 3.8 - and examine the underlying activity without losing context.

2 

UEBA provides the priority. Rather than reviewing every event, analysts work from a ranked list of entities of interest. The Analytic Dashboard shows the top 50 entities by risk; the behaviors page surfaces the model scores behind the rank

3 

Case Management resolves the concern. When a signal warrants investigation, the case record, attached evidence, chain of custody, and workflow artifacts live in a zero-trust, accredited, NIST 800-53r5-compliant system of record.

Three distinct outcomes emerge:

Speed to Certainty - analysts can move from an alert to an answer quickly, because the evidence, the context, and the case workflow are available in a coordinated sequence rather than in three disconnected tools.

Frictionless Security - a lightweight endpoint agent, role-based access controls, and pseudonymization options keep the program aligned with HR and Legal expectations about employee trust.

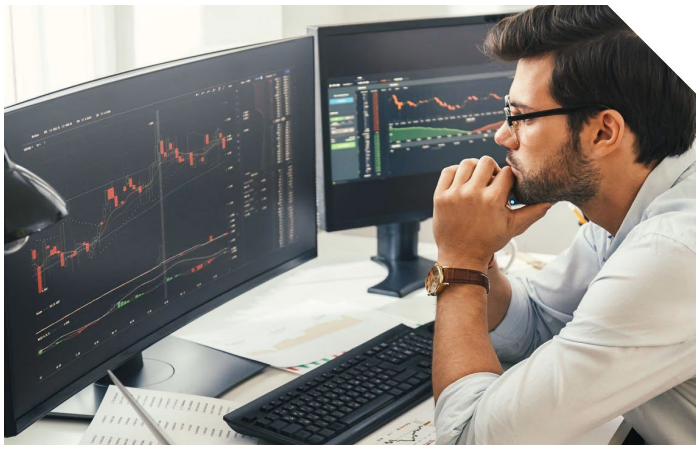
Full-Spectrum Context - a single story that spans the endpoint, the communication channels, the behavioral pattern, and the administrative record.

A Practical Mapping

The table below summarizes the most direct mappings discussed in this paper. It is intended as a starting point for an SSP section, not a substitute for the official CMMC Assessment Guides and their assessment objectives.

CMMC Requirement	Level	UAM	UEBA	Case Management
AC.L2-3.1.20 External Connections [CUI Data]	2	✓	✓	
AC.L2-3.1.21 Portable Storage Use	2	✓		✓
AT.L2-3.2.3 Insider Threat Awareness	2	✓	✓	✓
AU.L2-3.3.1 System Auditing	2	✓		✓
AU.L2-3.3.2 User Accountability	2	✓	✓	✓
AU.L2-3.3.5 Audit Correlation	2	✓	✓	
AU.L2-3.3.8 Audit Protection	2			✓
AU.L2-3.3.9 Audit Management	2			✓
CA.L2-3.12.2 Operational Plan of Action	2			✓
CA.L2-3.12.3 Security Control Monitoring	2	✓	✓	✓
CA.L2-3.12.4 System Security Plan	2			✓
IR.L2-3.6.1 Incident Handling	2	✓	✓	✓
IR.L2-3.6.2 Incident Reporting	2			✓
IR.L2-3.6.3 Incident Response Testing	2			✓
MP.L2-3.8.3 Media Disposal [CUI Data]	2			✓
PS.L2-3.9.1 / 3.9.2 Personnel Security	2		✓	✓
RA.L2-3.11.1 Risk Assessments	2		✓	✓
SI.L2-3.14.3 Security Alerts & Advisories	2	✓	✓	✓
SI.L2-3.14.6 Monitor Communications for Attacks	2	✓	✓	
SI.L2-3.14.7 Identify Unauthorized Use	2	✓	✓	✓
RA.L3-3.11.1e Threat-Informed Risk Assessment	3	✓	✓	✓
RA.L3-3.11.2e Threat Hunting	3	✓	✓	
PS.L3-3.9.2e Adverse Information	3		✓	✓
SI.L3-3.14.6e Threat-Guided Intrusion Detection	3	✓	✓	

A check mark indicates a capability that directly supports the assessment objectives of the requirement. In every case, final MET/NOT MET determinations depend on the specific assessment objectives in NIST SP 800-171A or 800-172A as adopted by CMMC, and on how the capability is implemented and documented in the organization's SSP.



Notes for the Reader

Outcomes vary. CMMC compliance is a property of an organization, not of a product. Performance, coverage, and assessment outcomes depend on deployment scope, configuration, SSP quality, and the training of the people operating the program. An insider risk program is a supporting mechanism for the requirements above - not a substitute for the policies, procedures, and specifications that CMMC also expects.

Scope matters. Level 2 and Level 3 requirements apply to the assets that process, store, or transmit CUI, as defined in the CMMC Scoping Guide. The controls above apply where the insider risk program is in scope; out-of-scope assets remain out of scope.

People first. The most mature insider risk programs are the ones that treat the hard-working majority as the population being protected, not the population being watched. Role-based access controls, analyst audit trails, pseudonymization where appropriate, and a case management system that enforces need-to-know are what let a program operate with the trust of employees, HR, and Legal - and with the confidence of an assessor.

Next Steps

For organizations preparing for Level 2 certification or already planning toward Level 3, a practical sequence is:

1. **Scope the assets** that process, store, or transmit CUI.
2. **Map existing tools** against the control families above - organizations commonly find gaps in audit correlation, entity-level risk scoring, and defensible case management.
3. **Document the program in the SSP** - include the operational plan of action, the assessment methodology, and the evidence location for each in-scope requirement.
4. **Pilot the insider risk workflow end-to-end** - from a real (but low-sensitivity) activity event through analytic triage into a case, with the artifacts each step produces.
5. **Run the assessment against the objectives**, not against the headline requirement - MET/NOT MET is determined objective by objective.

The organizations that treat CMMC as a forcing function to build a real insider risk program, rather than a checklist to defend against, tend to find the same thing: the work needed to protect CUI and the work needed to demonstrate it to a DoD assessor are the same work.

That's the value of **Speed to Clarity** - not that it makes the assessment easier, but that it makes the mission more defensible on every day that isn't an assessment day.

About Everfox

Everfox delivers trusted connectivity to protect the world's most critical environments and safeguard the sensitive data powering decision advantage. Built for mission-critical operations, Everfox protects what matters most by securing how data moves, how users access it, and how threats are neutralized across every domain.

Mission speed and secure collaboration are enabled across networks, domains, and allies, while the data powering AI and advanced analytics remains trusted and protected.

Everfox doesn't just defend systems —Everfox delivers decision dominance.

Learn More

www.everfox.com