



IMTS THREATDETECT™

Advanced Detection. Actionable Insights. Mission Readiness.

"it stands out for its ability to streamline employee monitoring while promoting ... security, and compliance within the workplace."

Verified User in Computer Software Industry



Overview

IMTS ThreatDetect™ (ITD) is a scalable User Activity Monitoring (**UAM**), enhanced with User Entity Behavior Analytics (**UEBA**) into a power platform providing unparalleled visibility into user activity to detect, investigate, and even mitigate some insider threats through Data Loss Prevention (**DLP**) capabilities. Purpose-built for modern insider threat challenges, ITD is grounded in decades of proven expertise.



ITD combines its UAM/UEBA/DLP technology—continually improved since its creation two decades ago—with the advanced training and mission rehearsal capabilities of the Mission Readiness Range (MRR), Powered by Capture the Packet™ (established in 2008). This powerful synergy ensures that ITD not only detects and mitigates risks but also equips teams with operational expertise for real-world challenges.

Fully compliant with **CNSSD 504**, ITD meets the stringent requirements for monitoring cleared personnel in government environments while delivering enhanced security across networks. To further bolster readiness, ITD provides access to MRR's scenario-driven exercises and mission rehearsal tools, ensuring that teams are prepared to tackle the

"It solves challenges in monitoring employee activities, ensuring compliance... and protecting data security, particularly beneficial in managing remote work environments, ultimately streamlining operations and reducing risks for businesses."

Jessica W., IT Specialist in Construction Industry

evolving threat landscape with confidence.

Proven Experience and Trusted Customer Satisfaction

IMTS ThreatDetect™ (ITD) stands on a foundation of trusted, award-winning platforms—Controlio and the Mission Readiness Range (MRR)—delivering unparalleled insider threat detection and operational readiness capabilities.

ThreatDetect UAM-UEBA-DLP Engine: A Legacy of Excellence

Over Two Decades of Reliability: Built on a platform established in 2005, our solution has been a cornerstone in insider threat detection for enterprises and government agencies.

Mission Readiness Range: Hands-On Excellence

Global Reach: Deployed across all branches of the U.S. military, MRR's core engineer is trusted for mission-critical training at top-secret levels. The Mission Readiness Range (MRR) stands alone as the **only training range** offering both **prebuilt and fully customizable scenarios and challenges** explicitly tailored for the **Insider Threat Mission**. Designed to address mission-critical insider threat risks, MRR also bridges seamlessly into broader cybersecurity roles, ensuring comprehensive readiness across both defensive and offensive operational needs.



"This [platform] provides exactly the training form factor that Cyber Protection Teams need—hands-on, real-time traffic capture and analysis."

U.S. Navy

"The hands-on experience was exceptional and beats the hell out of PowerPoints and online quizzes. I learned more today than in one year of online training."

U.S. Air Force

"It simulates real environments perfectly. The hands-on training is second to none in the realm of packet analysis."


U.S. Marine Corps

Built to Perform, Trusted to Deliver


ITD combines these proven platforms to deliver a complete solution for insider threat detection and mission readiness. Fully compliant with CNSSD 504, ITD ensures your organization meets the highest standards for monitoring and preparedness.

Key Features - 504-Compliant Technical Capabilities


Keystrokes, application usage, and file movements

	Tracks keystrokes, application usage, and file movements in full compliance with CNSSD 504 standards. Through APIs, provides seamless integration with government-mandated security protocols to ensure audit readiness.
---	--


Customizable Rules, Alerts and Reports

	Ability to create custom rules and policies to detect behavior indicative of a threat. Generates real-time alerts for anomalous activity and provides actionable insights via dashboards. Users can configure and schedule tailored reports to align with agency-specific risk criteria.
---	--


Data Loss Prevention (DLP)

	Tracks and blocks unauthorized data transfers via email, cloud, or external storage devices to thwart Unauthorized Disclosures . Provides fine-grained policy controls to prevent data exfiltration before it occurs.
---	--

Advanced Behavioral Analytics (UEBA)


Detects anomalies through trend analysis and integration with collected user activity. Utilizes advanced behavioral analysis techniques to enhance detection accuracy and minimize false positives.	
---	---

Comprehensive Screen Recording

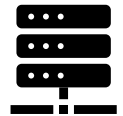
Captures video playback of user sessions as well as live sessions for auditing and forensic investigations. Ensures an immutable record for forensic analysis, helping build a complete incident timeline and confirm attribution.	
--	---

Flexible Deployment Options

Private Cloud-Hosted Deployment and Hybrid Cloud

	<p>Fully managed in AWS GovCloud or Azure Government (Cloud) for secure, scalable operations or a hybrid environment, ready for final enhancements to meet NIST RMF requirements and achieve Authority to Operate (ATO). Offers the flexibility to scale resources dynamically based on mission needs.</p>
---	--

On-Premises Deployment

<p>Deployed on your infrastructure for maximum control and compliance. Provides full ownership and control of the infrastructure, ensuring alignment with operational and security priorities.</p>	
--	---

Mission Readiness Range: Your Platform for Operational Readiness

Each ITD deployment includes 3-month access to Essentials Tier licenses (SaaS Range component) for the MRR and 12-month access to courses, scaled according to analyst-to-endpoint ratios and deployment size. The Mission Readiness Range (MRR) is a world-class training and assessment suite designed to prepare individuals and teams for real-world cybersecurity challenges. Built on over 15 years of proven performance, the MRR delivers scenario-driven mission rehearsal, advanced training, and skill-building tailored to meet the needs of government and enterprise organizations.

Key Features

- **Scenario-Based Training:** Participants engage in realistic, progressively challenging exercises that develop both offensive and defensive skills in dynamic environments.
- **Team-Based Competitive Training:** Teams operate collaboratively in secure networks, analyzing vulnerabilities and defending against active threats, mirroring real-world cyber operations.
- **Challenge Diversity:** Includes simulations for insider threats, system forensics, malware analysis, and more—aligned with NICE and DCWF frameworks.
- **Flexible Deployment Options:** Offered as a scalable SaaS solution or upgrade to a portable appliance for classified spaces, including TS/SCI environments.

MRR Essentials Licenses

MRR SaaS Essentials Licenses are assigned based on the following Analyst-to-Endpoint Ratios:

Endpoint Range	Analyst-to-Endpoint Ratio	MRR Essentials Licenses
250–999	1 per 3,000	1
1,000–1,999	1 per 3,000	1
2,000–4,999	1 per 3,000	1–2
5,000–9,999	1 per 4,000	2–3
10,000–24,999	1 per 5,000	3–6
25,000–49,999	1 per 5,000	6–10
50,000–99,999	1 per 6,000	10–17
100,000–249,999	1 per 7,000	17–34
250,000–499,999	1 per 8,000	34–50
500,000–749,999	1 per 9,000	50–84
750,000–999,999	1 per 10,000	84–100
1,000,000+	1 per 10,000	100+

For more information on the Mission Readiness Range, see the [MRR Brochure](#).

MRR Tiers Overview

The MRR provides scalable training and readiness resources with the option to upgrade from the Essentials Tier to Advanced, Pro, or Elite Tiers:

- **Essentials Tier:** Includes **3 months of access to the Mission Readiness Range** and **12 months of access to over 100+ curated courses** from leading providers such as CompTIA, ISC2, and EC-Council.
- **Advanced Tier:** Includes Essentials features plus **100+ interactive labs**, offering hands-on experience with real-world scenarios.
- **Pro Tier:** Adds the Tech Pro Library, offering advanced resources for certification preparation and leadership-focused training.
- **Elite Tier:** Comprehensive access to the EC-Council On-Demand Catalog, including certification exams and mission-critical training resources.

Flexible Extensions: Range access can be extended in 3-month increments for ongoing team development and mission rehearsal.

Conclusion

IMTS ThreatDetect™ delivers a comprehensive solution for insider threat detection, investigation, and mitigation, built on decades of proven technology and operational expertise. With full compliance to CNSSD 504, ITD offers the confidence and reliability required to meet the most stringent government standards.

By integrating the Mission Readiness Range, ITD goes beyond detection—empowering organizations with advanced operational readiness through cutting-edge training, customizable scenarios, and mission rehearsal capabilities. Whether safeguarding critical data or preparing teams for real-world challenges, ITD ensures your organization is equipped to anticipate, prevent, and respond to evolving threats.

With scalable deployment options, tailored resources, and flexible extensions, IMTS ThreatDetect™ is more than a tool—it's a strategic partner in securing your mission. Join the leaders in insider threat management and operational readiness by choosing IMTS ThreatDetect™.

Take the Next Step Today. Visit us at **IMTS.US** or email ITD@IMTS.US to schedule a consultation and learn how we can enhance your organization's security and readiness.

Contact Us - Visit us on the web at IMTS.US or email us at ITD@IMTS.US for details.