PROACTIVE INSIDER RISK MANAGEMENT FOR THE PUBLIC SECTOR

How DTEX meets UAM Requirements of CNSSD 504

The National Insider Threat Task Force and Directive 504 from the Committee on National Security Systems (CNSSD 504) prescribes minimum measures for User Activity Monitoring (UAM) on all classified networks. All US Federal agencies and entities are required to implement these measures to "detect indicators of insider threat behavior" and to have the "technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information."

How DTEX InTERCEPT meets CNSSD 504 UAM Requirements

The DTEX Insider Risk Management InTERCEPT platform enables focused observation for the early detection, deterrence, and mitigation of insider threats. Using patented DMAP+ Technology, DTEX provides contextual intelligence across Data, Machines, Applications, and People to surface early warning indicators of intent, to identify when malicious actors are performing reconnaissance, circumvention, aggregation, and obfuscation—and stop them well before exfiltration occurs.

CAPTURE OF FULL APPLICATION CONTENT

DTEX provides a continuous audit trail of unique endpoint metadata to observe, record, and correlate the actions and activities of Data, Machines, Applications, and People in near-real-time, including the full capture of all Session, Process, File System, and Window activities, on and off the organizational network.

SCREEN CAPTURE AND KEYSTROKE MONITORING

When a user has been elevated for focused observation, DTEX provides application content monitoring (includes SSL inspection for web browser-based activities), video/screen capture and key stroke capture. Capture can be based on specific device, application, user rules, or for individuals flagged as "persons of interest." All captures can be exported for further analysis.

FILE SHADOWING

Malicious insiders will often attempt to disguise (obfuscate) their actions by changing file names or extensions. DTEX continuously tracks documents, even when names and locations have changed, using configurable hashing algorithms including MD5, SHA1 and SHA256. It can determine the "lineage" of a file to answer who, what, when, where, and why was a file was copied, modified, obfuscated or exfiltrated. DTEX also tracks file classification meta-data as well as the usage of the Alternate Data Stream (ADS) for advanced attempts to obfuscate data.

SET TRIGGERS/ALERTS BASED ON USER ACTIVITY

When a skilled insider wants to steal data, they often separate their activities into smaller steps over a period of time to avoid detection. Alerting on every activity (which could be benign) can result in alert fatigue. DTEX uplifts insider risk detection and mitigation:

- Alert stacking and machine learning capabilities combine behavioral rules and anomaly detection to reduce false positives and analyst overhead.
- Automated activity correlation allows multiple disparate events to be attributed to a defined sequence of events occurring within a given time window.
- This further improves true positive detection rates by elevating alert scores for events that occur sequentially across the full Insider Threat Kill Chain, over and above alerting rules triggered in isolation.

DTEX also provides the ability to automatically increase monitoring and alerting mechanisms for high-risk user populations (e.g., new joiners, leavers or "flight-risk" detected employees and individuals flagged as "persons of interest") and automatic correlation of these populations with insider threat related activities.

SUPPORTED PLATFORMS

UNIFIED TELEMETRY

USER ENDPOINT	SERVER ENDPOINT	VDI	CLOUD	SaaS / OTHER
Microsoft	Microsoft	CITRIX	aws	Active Directory
mac OS	Linux	vmware	Google Cloud	CROWDSTRIKE
				helpsystems
				snowflake
				Google Workspace
				Microsoft 365

ZERO-IMPACT → 5MB PER DAY (PER ENDPOINT)

DTEX

REQUEST A DEMO

Contact us today to schedule a demonstration at demo@dtexsystems.com

ABOUT DTEX SYSTEMS

DTEX Systems empowers organizations to prevent data loss and support a trusted workforce by proactively stopping insider risks from becoming insider threats. Its InTERCEPT™ platform consolidates the essential elements of Data Loss Prevention, User Activity Monitoring, and User Behavior Analytics in a single light-weight platform to detect and mitigate insider risks well before data loss occurs. Combining AI/ML with behavioral indicators, DTEX enables proactive insider risk management at scale without sacrificing employee privacy or network performance.

To learn more about DTEX Systems, visit www.dtexsystems.com.