DTEX FEDERAL

DTEX InTERCEPT

Next-Generation Insider Risk Management

Michael Crosland
Vice President – IC/DoD

CNSSD 504 REQUIREMENTS MAPPING – DTEX FEDERAL

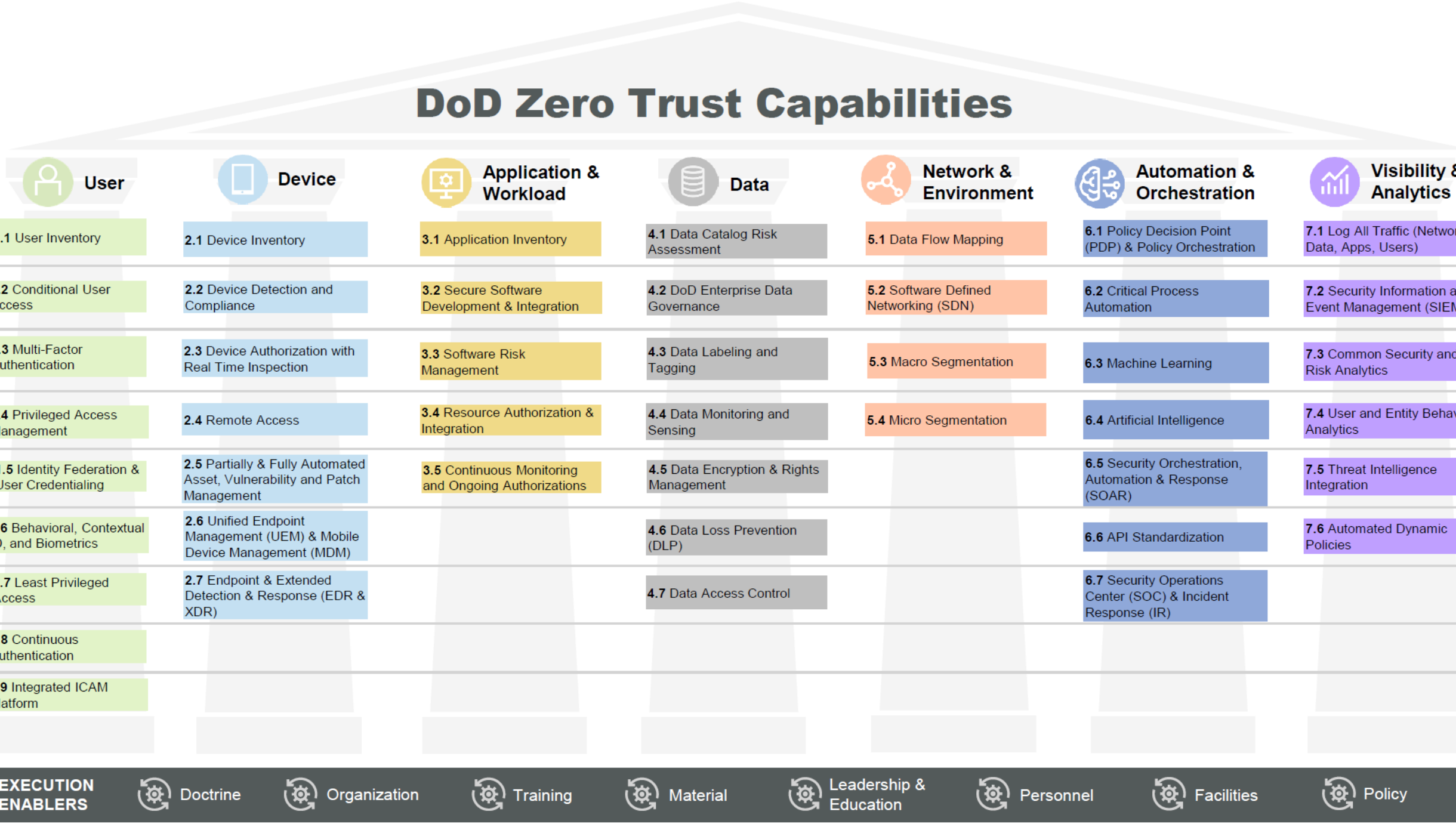
No.	Requirement (Must)	DTEX Capability	DTEX Overview	Reference
1	Must safeguard user activity data at rest, in transit, and during use	☑ Requirement Met	Data encrypted at rest, in transit, and during use. See attached encryption policy & SOC 2 Type II Audit report.	Document Link
2	User activity data must be protected from unauthorized access, modification, or destruction	☑ Requirement Met	All administrative access is fully monitored and protected from unauthorized access / modification / destruction. See security safeguards document.	Document Link
3	Must ensure the chain of custody of user activity data	☑ Requirement Met	DTEX ensures confidentiality and integrity through multiple means including PKI (CAC) enabled access control, restricted roles, and data encryption to protect chain-of-custody.	Document Link
4	Keystroke monitoring	☑ Requirement Met	Full continuous capture of keystrokes (Focused Observation module)	Demo Link
5	Full application content (e.g., email, chat, data import, data export	☑ Requirement Exceeded	Full application content monitored, including inspection of encrypted communication channels (http inspection filtering) and via SaaS API integrations.	Demo Link
6	Obtain Screen captures	☑ Requirement Met	Continuous or triggered screen captures with configurable resolution and bit rate (Focused Observation module)	Demo Link
7	Perform file shadowing	☑ Requirement Exceeded	Full file shadowing via lineage and digital fingerprinting.	Demo Link
8	UAM data must be attributable to a specific user	☑ Requirement Met	All data attributed to specific users.	Demo Link
9	Data generated by triggers must be provided to the insider threat program for storage, analysis, and possible investigative action	☑ Requirement Met	All data layers, including alerts and triggers is exportable to third party systems for storage, analysis and investigation. DTEX also includes an in-built data lake capability.	Demo Link
10	Data must be retained for a minimum of 5 years to support detection of behavioral patterns and relationships with other insider threats	☑ Requirement Met	Storage is configurable to meet / exceed minimum storage requirements	Document Link
	Recommended (Should) - Demonstration not required			
11	Privacy Information: Potential to damage an individual's reputation	☑ Requirement Exceeded	Patented pseudonymization for tokenization of PII and removal of bias from Insider Threat Analysts - patent link	Demo Link
12	Should incorporate this data into an analysis system capable of identifying anomalous behavior that may provide indications of insider threat activity and support D/A investigative requests	☑ Requirement Exceeded	DTEX incorporates UAM data into a UEBA analysis system capable of aggregating cyber physical and psycho-social indicators of anomalous behavior to proactively support investigations. All risk models are fully customizable.	Document Link
13	The events or indicators in Table 1 (Categories of potential insider threat events or indicators on NSS) are recommended for consideration	☑ Requirement Met	NEXT PAGE	NEXT PAGE

CNSSD 504 REQUIREMENTS MAPPING – DTEX FEDERAL (CONT.)

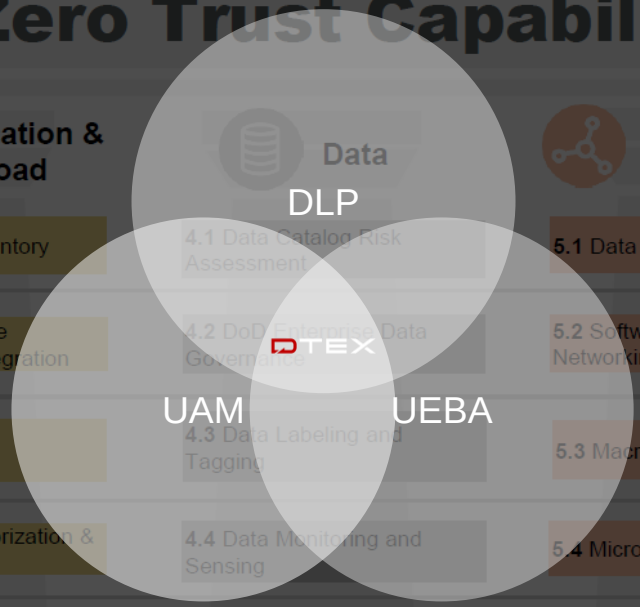
No.		DTEX Capability	DTEX Overview	Reference
13	The events or indicators in Table 1 (Categories of potential insider threat events or indicators on NSS) are recommended for consideration	☑ Requirement Met	**DTEX InTERCEPT Federal provides 'Out-of-the-box' capability for CNSSD 504 Table 1**	SEE BELOW

Account Change	☑ Requirement Met	All unauthorized or anomalous account changes tracked (includes Event Log Collection)	Demo Link
Authentication Failure / Anomaly	☑ Requirement Met	All failed authentication attempts tracked, and anomalies alerted upon (includes (Event Log Collection)	Demo Link
Baseline Anomaly	☑ Requirement Exceeded	All behavioral indicators and system configurations are automatically baselined and anomalies/outliers alerted	Demo Link
Excessive Activity	☑ Requirement Met	Configurable thresholds allow for 'excessive' activity to be defined across numerous activity types.	Demo Link
Evidence Tampering	☑ Requirement Met	Any attempt to tamper with security controls, audit data and other record keeping mechanisms is tracked and alerted upon.	Demo Link
Exfiltration	☑ Requirement Met	Comprehensive coverage of all data egress and exfiltration vectors.	Demo Link
Malware	☑ Requirement Met	Mapping to MITRE ATT&CK as well as 3rd Party EPP/EDR Integrations	Demo Link
Network Traffic Anomaly	☑ Requirement Met	Full network anomaly detection (includes HTTP Inspection / Geo-Location / DNS / NetFlow).	Demo Link
Privilege Violation	☑ Requirement Exceeded	Comprehensive detection of credential misuse ('credential misuse detection' was the focus of the 2017 DTEX DISA RIF)	Demo Link
System Configuration Change	☑ Requirement Met	Unauthorized or anomalous changes to system configuration settings detected (includes Event Log Collection / Tagging Rules)	Demo Link
User Behavior Anomaly	☑ Requirement Exceeded	DTEX Meta Data Collection / DMAP+ / Tagging Rules	Document Link

DoD Zero Trust Capabilities



DoD Zero Trust Capabilities



User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
1.1 User Inventory	**2.1** Device Inventory	**3.1** Application Inventory	**4.1** Data Catalog Risk Assessment	**5.1** Data Flow Mapping	**6.1** Policy Decision Point (PDP) & Policy Orchestration	**7.1** Log All Traffic (Network, Data, Apps, Users)
1.2 Conditional User Access	**2.2** Device Detection and Compliance	**3.2** Secure Software Development & Integration	**4.2** DoD Enterprise Data Governance	**5.2** Software Defined Networking (SDN)	**6.2** Critical Process Automation	**7.2** Security Information and Event Management (SIEM)
1.3 Multi-Factor Authentication	**2.3** Device Authorization with Real Time Inspection	**3.3** Software Risk Management	**4.3** Data Labeling and Tagging	**5.3** Macro Segmentation	**6.3** Machine Learning	**7.3** Common Security and Risk Analytics
1.4 Privileged Access Management	**2.4** Remote Access	**3.4** Resource Authorization & Integration	**4.4** Data Monitoring and Sensing	**5.4** Micro Segmentation	**6.4** Artificial Intelligence	**7.4** User and Entity Behavior Analytics
1.5 Identity Federation & User Credentialing	**2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management	**3.5** Continuous Monitoring and Ongoing Authorizations	**4.5** Data Encryption & Rights Management		**6.5** Security Orchestration, Automation & Response (SOAR)	**7.5** Threat Intelligence Integration
1.6 Behavioral, Contextual ID, and Biometrics	**2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)		**4.6** Data Loss Prevention (DLP)		**6.6** API Standardization	**7.6** Automated Dynamic Policies
1.7 Least Privileged Access	**2.7** Endpoint & Extended Detection & Response (EDR & XDR)		**4.7** Data Access Control		**6.7** Security Operations Center (SOC) & Incident Response (IR)	
1.8 Continuous Authentication						
1.9 Integrated ICAM Platform						

EXECUTION ENABLERS Doctrine | Organization | Training | Material | Leadership & Education | Personnel | Facilities | Policy

WHAT'S MISSING?

NEXT-GEN AV

MALWARE FOCUS

1. EPP (AV)
2. EDR
3. IOC's
4. MITRE ATT&CK

CROWDSTRIKE Microsoft

?

NEXT-GEN SIEM

DATA FOCUS

1. SIEM
2. SOAR
3. CASE MGMT
4. APP ECOSYSTEM

splunk> exabeam

NEXT-GEN FIREWALL

NETWORK FOCUS

1. IDS / IPS
2. NDR
3. WAF
4. FIREWALL

paloalto NETWORKS zscaler

**logos shown are key DTEX integration partners*

WHAT IS NEEDED?

HUMAN FOCUS

WHAT WENT WRONG?

HUMAN FOCUS

DLP

- Heavy on the endpoint
- Primarily detects negligent behavior, not malicious data loss
- Doesn't scale

UAM

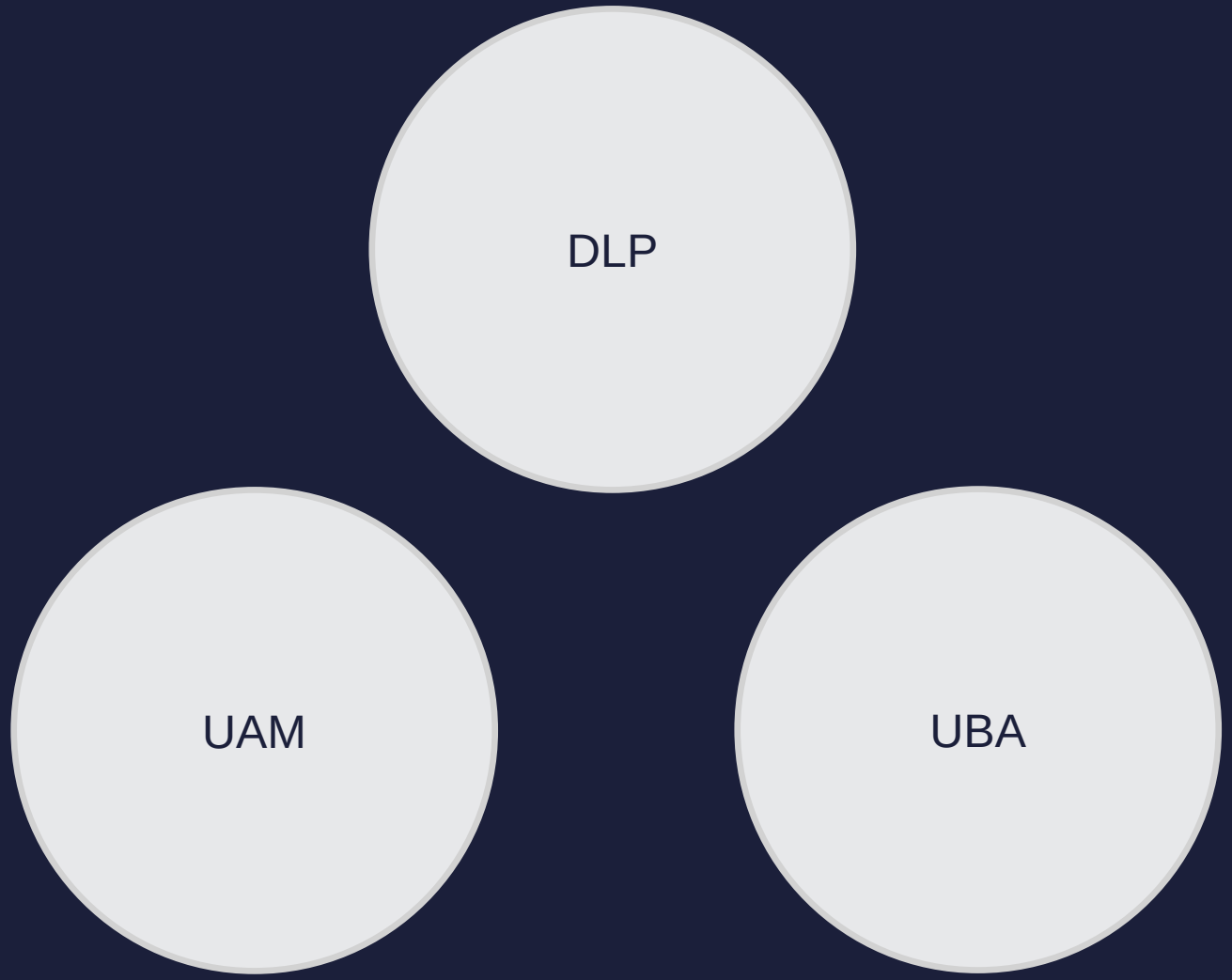
- Surveillance based → too intrusive
- Point and shoot → used reactively
- Often not GDPR and CCPA compliant

UBA

- Log data lacks context
- Too much time spent on data engineering – NOT data science
- Too many false positive

THE CONVERGENCE

HUMAN FOCUS

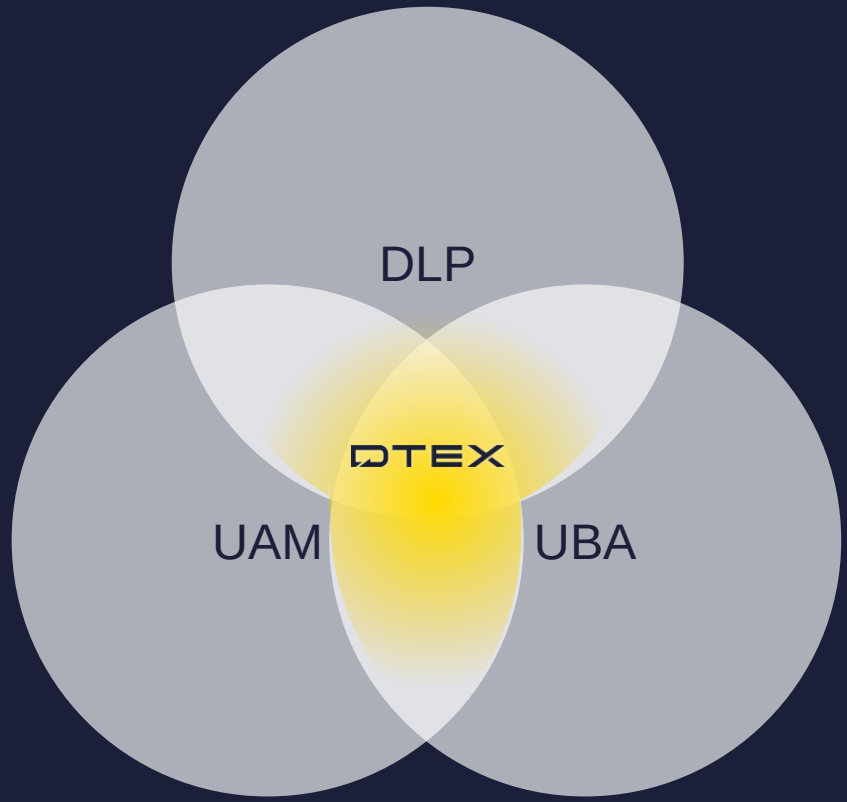


THE CONVERGENCE

HUMAN FOCUS

Gartner®

“By 2027, 70% of CISOs in larger enterprises will adopt a consolidated approach to address both insider risk and data exfiltration use cases.”



NEXT-GEN INSIDER

HUMAN FOCUS

1. UAM
2. DLP
3. UBA
4. FORENSICS

DTEX

COMPLETING THE PICTURE

NEXT-GEN AV

MALWARE FOCUS

1. EPP (AV)
2. EDR
3. IOC's
4. MITRE ATT&CK

CROWDSTRIKE Microsoft

NEXT-GEN INSIDER

HUMAN FOCUS

1. UAM
2. DLP
3. UBA
4. FORENSICS

DTEX

NEXT-GEN SIEM

DATA FOCUS

1. SIEM
2. SOAR
3. CASE MGMT
4. APP ECOSYSTEM

splunk> exabeam

NEXT-GEN FIREWALL

NETWORK FOCUS

1. IDS / IPS
2. NDR
3. WAF
4. FIREWALL

paloalto NETWORKS zscaler

**logos shown are key DTEX integration partners*

DTEX InTERCEPT PLATFORM

DTEX
ZERO-IMPACT FORWARDER
→ 5MB PER DAY/ ENDPOINT

USER ENDPOINT
Microsoft · mac OS

SERVER ENDPOINT
Microsoft · Linux

VDI
CITRIX · vmware

CLOUD
aws · Azure · Google Cloud

SaaS / OTHER
Active Directory · CROWDSTRIKE · helpsystems · snowflake · Google Workspace · Microsoft 365

Threat Intel
DTEX Insider Threat Advisories

Malicious Users

Non-Malicious Users
Negligent · Mistaken · Compromised

Insider Risk (UAM+UEBA)

Behavioral Data Loss Prevention

Account Compromise

Digital Forensics

Fraud, Risk & Compliance

ENCRYPTION LAYER: Employee Privacy & GDPR Compliance

DMAP+ TECHNOLOGY

A real-time correlation of DMAP telemetry introspection and predictive modeling that leads to accurate detection of insider threats at scale

HUMAN · ORGANIZATIONAL · **Unified Telemetry** · CYBER · PHYSICAL

THIRD-PARTY INTEGRATIONS
SIEM
SOAR
ITSM

DTEX

CISO SCORECARD (INTERNAL RISK SCORECARD) | SEP 9TH 2020 (EDT)

INTERNAL RISK SCORECARD

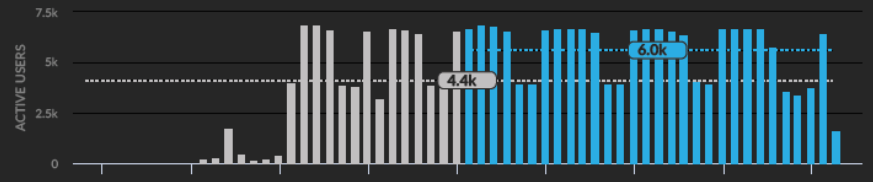
CISO EXECUTIVE OVERVIEW

Previous Risk Profile	7.1
Current Risk Profile	4.7
Dtex Benchmark	2.5

WINDOWS WORKSTATIONS	MACOS WORKSTATIONS	WINDOWS SERVERS	LINUX SERVERS	VIRTUAL DESKTOPS
10255	202	1223	126	952

8459 ACTIVE USERS

a 36% increase in comparison with the past 30 days



INTERNAL RISK SCORECARD

MALICIOUS BEHAVIOR	0.3	73 INCIDENTS 56 USERS	• Exfiltration - Sharepoint Zip File Access • Command And Control - Connection Proxy [T1090]
NEGLIGENT BEHAVIOR	1.2	303 INCIDENTS 207 USERS	• 196 user(s) with high volume of access to personal webmail • 8 user(s) with accessing files which may contain plaintext passwords
COMPROMISED BEHAVIOR	0.7	198 INCIDENTS 130 USERS	• Execution - Scripting [T1064] • 25 user(s) with powershell activity
DATA LOSS BEHAVIOR	2.2	507 INCIDENTS 394 USERS	• 108 user(s) with anomalous transfers to USB devices • 119 user(s) with usage of screen capture tools
BEHAVIORAL INDICATORS	0.3	61 INCIDENTS 58 USERS	• 51 user(s) with access to websites blocked by external tools • 7 user(s) with flight risk early indicators

RECOMMENDATIONS

1. TECHNOLOGY
   - Review all powershell activity and triage any suspicious events
   - Review and revoke access to unapproved local, service or domain administrative accounts
   - Investigate any suspicious service stop commands
2. PEOPLE
   - Review and restrict access to personal webmails
   - Review all unprotected files which contain sensitive password information and educate user regarding safe storage policies
   - Remind users of IT Acceptable Use Policies
3. PROCESS
   - Review any unauthorized transfers of corporate information
   - Review and consider restricting the usage of unapproved screen capture tools
   - Review the files being compressed and identify the confidential files included in the archive

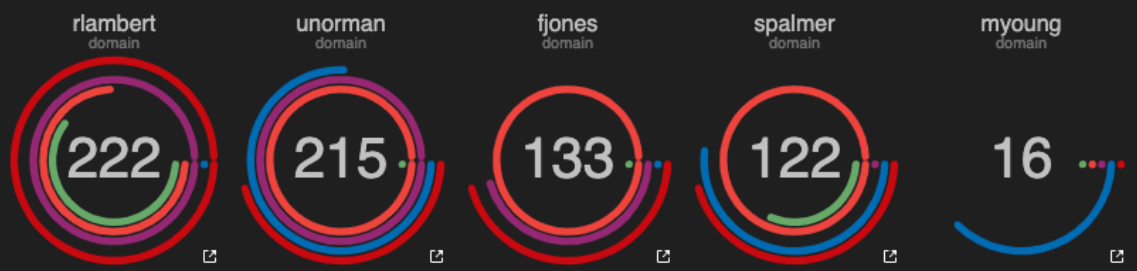
InTERCEPT CONTROL CENTER

Previous Risk Profile	4.2
Current Risk Profile	3.2
DTEX Benchmark	2.5

Windows Workstations	macOS Workstations	Windows Servers	Linux Servers	VDI Endpoints
10,752	1,112	252	789	690

MALICIOUS BEHAVIORS	NON-MALICIOUS BEHAVIORS	COMPROMISED BEHAVIORS	DATA LOSS BEHAVIORS	POTENTIAL RISK INDICATORS
Intentional Acts of Concern	Negligent, Mistaken or Outsmarted	MITRE ATT&CK Techniques	Possible Exfiltration Methods	PRI / Risk Multipliers
13	7	11	32	5

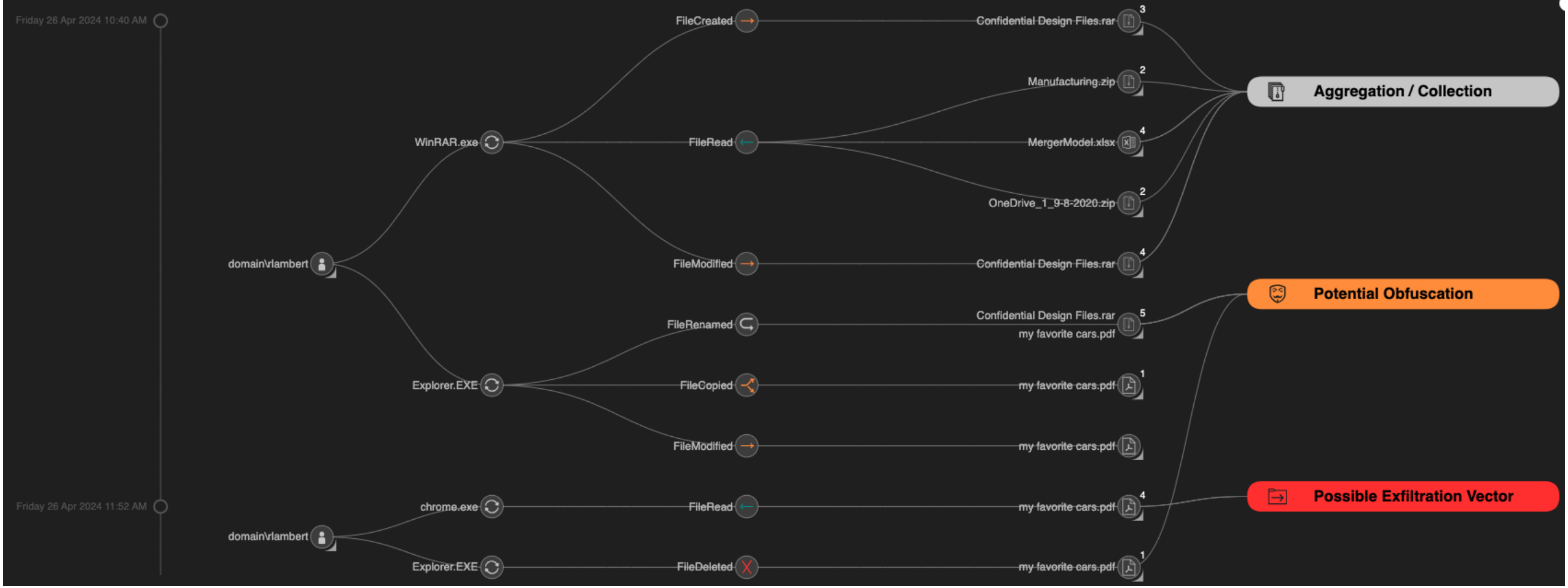
RISKY USERS



InTERCEPT DATA LINEAGE

DATA LINEAGE MAP

Historical file system activities linked via source file name(s), destination file name(s), file hashes and other correlated behaviors.



InTERCEPT USER TIMELINE

DOMAIN \ RLAMBERT

Malicious	65
Non-Malicious	0
Compromised	93
Data Loss	45
Behavior	19

Name: rlambert
First Seen: 2022-07-05
Last Seen: 2024-04-26
Active Days: 14

All data on this visualisation (including Active Days) is based on a fixed timeframe of the Last 30 Days only.

Malicious	This user shows escalated behaviors in multiple Malicious categories including "Obfuscation - Data Archive Creation and Deletion I4012".
Compromised	Additionally potentially compromised activity related to "Discovery" was elevated that could increase the possibility of a compromised account.
Data Loss	This user also shows escalated behaviors in multiple Data Loss categories including "Personal Webmail" activities.
Behavior	Unusual Behavioral activity related to "Flight Risk" was also elevated for review.

Exfiltration File Read Via Browser I5012

Behavior - Flight Risk I 24

Potential Exfiltration - Personal Webmail I5004 I 30

Discovery - Permission Groups Discovery [T1069] I 50

Reconnaissance - Security Bypass Research I1001 I 25

Discovery - Network Service Scanning [T1046] I 25

Exfiltration - Archive Collected Data [T1560] I 20

Aggregation - Compressed Data I3006 I 20

Obfuscation - Data Archive Creation and Deletion I4012 I 75

Aggregation - Data Compressed - Movement of Archive Files I3009 I 15

Obfuscation - Suspicious Archive Renaming I4000 I 40

Potential Exfiltration - Obfuscated Internet File Upload I 75

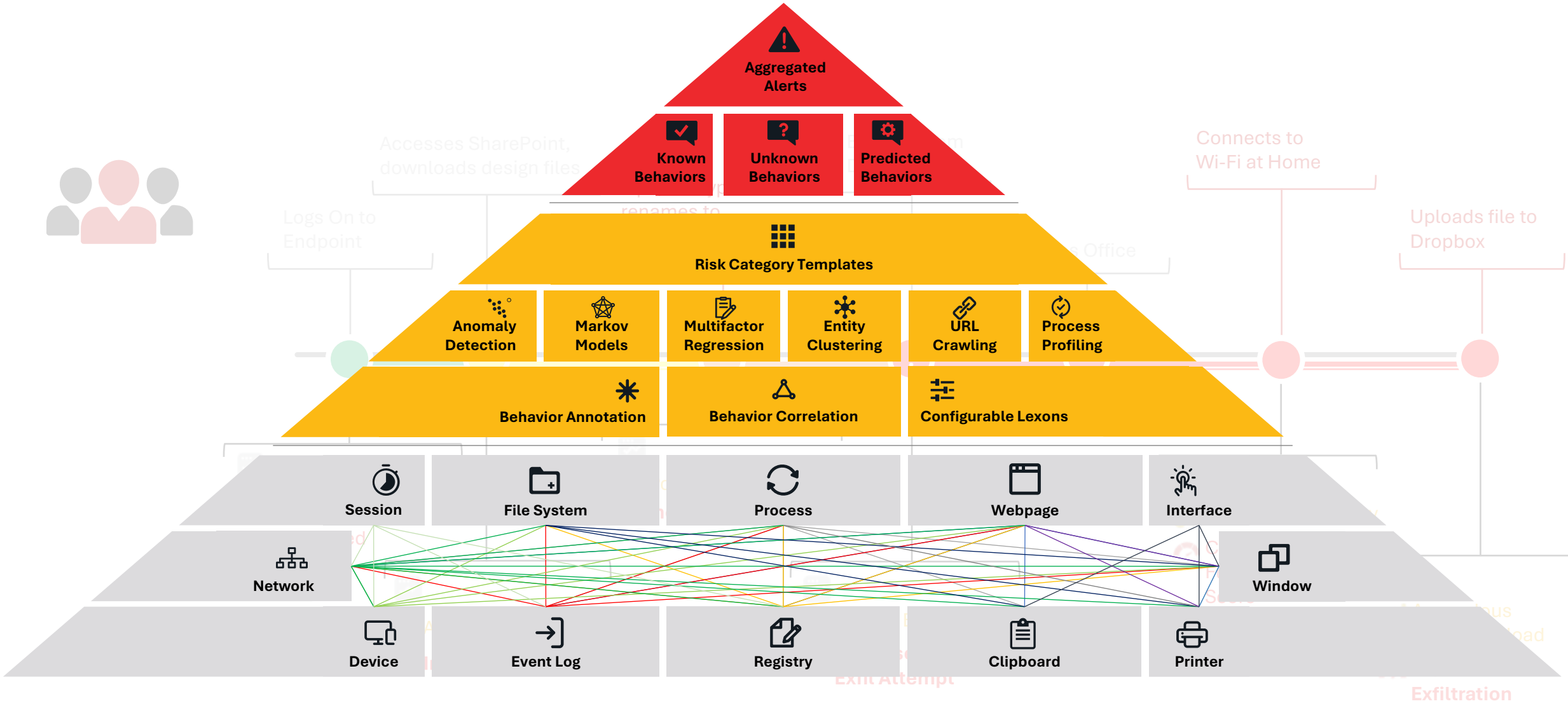
Obfuscation - Data Encrypted I4007 I 67

Exfiltration - Posting Data To Website I5013 I 20

17 additional behaviors not shown on timeline - zoom in for deta

AM 17 Apr · AM 19 Apr · AM 21 Apr · AM 23 Apr · AM 25 Apr · AM 27 Apr · AM 29 Apr

DMAP+ TECHNOLOGY



InTERCEPT DLP SUMMARY - OBFUSCATED INTERNET FILE UPLOAD

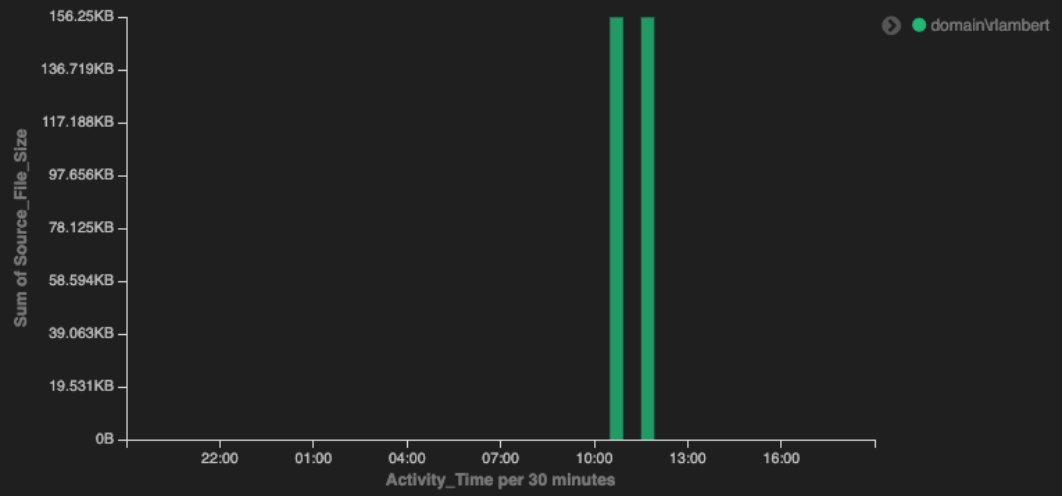
1 | 0.3 MB | 2 | 1

DTEX i3 AUTOMATED SUMMARY

User "domain\rlambert" was identified transferring files via multiple potential method.

- This occurred on endpoint, "domain\evo-d03197", utilizing multiple applications.
- There was a total of 2 unique files with a total file size of 319.7 KB.
- The user was identified performing all activities during normal business hours.
- Top file extensions involved were: "pdf", "rar".
- All of the files that were transferred stemmed from known location(s): "Desktop".
- Access to sensitive file(s) detected: "Confidential Design".

TIMELINE



FILE LOCATIONS

1 - 1 of 1

Source File Directory	Sum of File Sizes	Unique File Extensions	Unique Files
\Users\Demo_User_AL\Desktop\	0.3 MB	2	2

FILE TYPES

Archive

Confidential Design Files.rar
(0.2 MB)

PDF

my favorite cars.pdf
(0.2 MB)

Solution Demonstration

Single Customer Journey

- Phase 1 - Deployed
- Phase 2 - Deployed
- Phase 3 - Deployed

Insider Threat Detection (UAM + UEBA)			Risk, Audit and Compliance	Data Loss Prevention	Server Security	Forensic Investigations
MALICIOUS BEHAVIOR	COMPROMISED BEHAVIOR MITRE ATT&CK™	NEGLIGENT BEHAVIOR	Automated Risk Reporting (Benchmark & Baseline)	Wireless Transfers (i.e., Airdrop / Bluetooth)	Privileged Account Misuse	Audit trail of all activities
Bypass of Security Controls	Unusual Privilege Escalation	Teachable Moment Reporting	Inappropriate internet usage	USB device usage	File Integrity Monitoring (FIM) Contextualization	Leavers Forensic Audit (365)
Unusual Privilege Escalation	JSP Backdoor Detection	Accidental Data Loss	Use of personal webmail	Instant Messaging Applications	SWIFT Server Monitoring	Joiners Forensic Audit (Probation Period)
Obfuscation & Covering Tracks	Domain Fronting	Use of Non-sanctioned software	System configuration changes	Upload to Cloud Storage (Online File Sharing)	Unusual application behavior	File lineage
Unauthorized Use of Administrative / Cyber / Hacking Tools	Lateral Movement	Online File Sharing Misuse	Unauthorized use of decommissioned accounts and/or assets	Personal vs Corporate Webmail (i.e., G-suite)	Unusual Database behavior	Rogue applications
Flight Risk + Data Loss	ToR & Proxy Bypass	Shadow IT	Business continuity reporting	Printing	Unusual Privilege Escalation	Abnormal internet activity
On / Off Network Monitoring	Malicious or Unusual Application Behavior	Bulk Transfer Utilities	Use of Non-sanctioned software	FTP / sFTP / SCP	Bastion / Jump Server Monitoring	DMAP Contextual Audits (Data Machine Application People)
Portable Application Use	Unusual Data Aggregation	Instant Messaging Usage	Unauthorized use of communication software	Confidential / Sensitive File Transfers	Unusual Service Account Behavior	User to Admin Account Correlation

Single Customer Journey

- Phase 1 - Deployed
- Phase 2 - Deployed
- Phase 3 - Deployed

Insider Threat Detection (UAM + UEBA)			Risk, Audit and Compliance	Data Loss Prevention	Server Security	Forensic Investigations
MALICIOUS BEHAVIOR	COMPROMISED BEHAVIOR MITRE ATT&CK™	NEGLIGENT BEHAVIOR	Automated Risk Reporting (Benchmark & Baseline)	Wireless Transfers (i.e., Airdrop / Bluetooth)	Privileged Account Misuse	Audit trail of all activities
Bypass of Security Controls	Unusual Privilege Escalation	Teachable Moment Reporting	Inappropriate internet usage	USB device usage	File Integrity Monitoring (FIM) Contextualization	Leavers Forensic Audit (365)
Unusual Privilege Escalation	JSP Backdoor Detection	Accidental Data Loss	Use of personal webmail	Instant Messaging Applications	SWIFT Server Monitoring	Joiners Forensic Audit (Probation Period)
Obfuscation & Covering Tracks	Domain Fronting	Use of Non-sanctioned software	System configuration changes	Upload to Cloud Storage (Online File Sharing)	Unusual application behavior	File lineage
Unauthorized Use of Administrative / Cyber / Hacking Tools	Lateral Movement	Online File Sharing Misuse	Unauthorized use of decommissioned accounts and/or assets	Personal vs Corporate Webmail (i.e., G-suite)	Unusual Database behavior	Rogue applications
Flight Risk + Data Loss	ToR & Proxy Bypass	Shadow IT	Business continuity reporting	Printing	Unusual Privilege Escalation	Abnormal internet activity
On / Off Network Monitoring	Malicious or Unusual Application Behavior	Bulk Transfer Utilities	Use of Non-sanctioned software	FTP / sFTP / SCP	Bastion / Jump Server Monitoring	DMAP Contextual Audits (Data Machine Application People)
Portable Application Use	Unusual Data Aggregation	Instant Messaging Usage	Unauthorized use of communication software	Confidential / Sensitive File Transfers	Unusual Service Account Behavior	User to Admin Account Correlation

Immediate Time to Value & Protection

Real-Time Behavioral Telemetry	Sensitive Data Profiling	Risk Adaptive Data Protection	Cloud Architecture
Deploys in Minutes	**360° Enterprise Visibility in 24 Hours**	**Contextual Workforce & Data Forensics in Days**	**On-Demand Assessment & Reporting in 1st Week**
Lightweight forwarders collect 3-5MB of data per user per day, create no network impact, and do not harm employee productivity or endpoint performance, using < 0.5% CPU.	DTEX InTERCEPT delivers enterprise-wide visibility, investigative audit, and protection capabilities within the first 24 hours.	DTEX InTERCEPT begins identifying outlier behaviors that may be malicious, negligent, or compromised within 10 days of deployment.	DTEX InTERCEPT calculates an Internal Risk Benchmark and produces an executive overview of organizational risk and actionable recommendations.

Immediate ROI | Eliminate False Positives | Simplified Management

DMAP+ TECHNOLOGY