

Delivering Trusted Insider Intelligence and Investigations Support

SOLUTION BRIEF



DTEX Insider Intelligence and Investigations (DTEX i³) is an investigations and research division focused on delivering counter-insider threat research, intelligence packages, Threat Advisories, forensic investigations, and insider risk management support.

As workforce behavior deviates from the norm, DTEX i³ works side by side with customers to respond to DTEX InTERCEPT's automated reports and findings, identify internal risks, evaluate their severity, and proactively protect against malicious, negligent, and compromised users while preventing data loss.

DTEX i³ Services

DTEX i³ Services are designed to augment insider threat, data loss prevention and risk teams with the skills and experience of the DTEX Insider Investigation and Intelligence (i³) team.

DTEX i³ brings together experienced behavioral researchers, consultants, and an elite team of insider threat investigators to create an intelligence-driven, investigation-ready capability. The founding members of DTEX i³ bring a combined 100+ years of experience in advanced insider threat and data loss research, analysis, and hunting from notable companies, including Deloitte, Raytheon, Sophos, Symantec, FireEye and more.

i ³ SERVICES OVERVIEW	i ³ BASIC	i ³ ENHANCED	i ³ PREMIUM
Investigation Support	2 investigations per year	6 investigations per year	12 investigations per year
Intelligence Requests and Risk Model Adjustment	Semi-annual review and implementation	Semi-annual review and implementation + 6 on-demand requests per year	Monthly review and implementation + 12 on-demand requests per year
Alert Prioritization and Review ¹		Weekly review and presentation	Daily review and presentation
Emerging Risk Insights			Monthly review and presentation

¹DTEX Alert Prioritization and Review is not regarded as a replacement for your first response and incident management processes. Alerts prioritized are expected to be reviewed by the customer to provide contextualized domain knowledge


i³ Service Deliverables

<p>Investigation Support</p>	<p>In the case of an identified insider event, the i³ team performs evidentiary-quality forensic investigations. This offers full details of insider activity and intent to determine severity and provides customers with the cyber evidence required to escalate internally, notify law enforcement, and inform user education programs. Includes preparation and presentation of an investigation report.</p>
<p>Intelligence Requests and Risk Model Adjustment</p>	<p>Customize the DTEX InTERCEPT Risk Model through Use Case Prioritization, Risk Model Adjustment and Rule Development. Includes requesting new content specific to the environment through on-demand requests and scheduled reviews of the efficacy of these custom changes.</p>
<p>Alert Prioritization and Review</p>	<p>The i³ team reviews and suggests alerts for further response and presents findings in frequency defined by the service plan. Includes identification of potential risks and false positives. Alert review will focus on highest risk scores identified by the InTERCEPT platform. Regular review and suggestions made by the i³ team help to improve the outputs of the automated InTERCEPT reports and collaboratively reduce the DTEX Organizational Risk Profile.</p>
<p>Emerging Risk Insights</p>	<p>The i³ team leverages a range of proprietary DTEX techniques and tools to identify new risks or business insights that have not otherwise been surfaced by typical outputs. Emerging Risk Insights focuses on behavioral profiles which evolve over time or those that may be specific from organization to organization. Any urgent risks identified are flagged during the next alert review, and other interesting statistics or patterns are presented in the frequency of the selected service plan.</p>

“To fully understand any insider incident, visibility into the nuance and sequence of human behavior is pivotal. DTEX i³ brings unparalleled experience investigating the human behaviors and early warning indicators that are always the root cause of an insider incident.”

Rajan Koo,
DTEX Systems CTO





Roles and Responsibilities

Tools, Technology, and Implementation	Investigation Support	Intelligence Requests and Risk Model Adjustment	Alert Prioritization and Review ¹	Emerging Risk Insights	First Response, Domain Knowledge and Escalation ¹
	DTEX i3 BASIC			CUSTOMER	
	DTEX i3 ENHANCED				CUSTOMER
	DTEX i3 PREMIUM				CUSTOMER

¹DTEX Alert Prioritization and Review is not regarded as a replacement for your first response and incident management processes. Alerts prioritized are expected to be reviewed by the customer to provide contextualized domain knowledge.

About DTEX InTERCEPT

DTEX InTERCEPT is a purpose-built insider risk management platform that operates at the intersection of data loss prevention, user activity monitoring and user behavior analytics. InTERCEPT surfaces early warning indicators to detect, deter, and disrupt insider risks well before data loss occurs – quickly, easily and at scale.

			
<p>Prevent data loss with behavioral intent intelligence.</p>	<p>Detect insider threats with dynamic risk scoring.</p>	<p>Fast-track investigations with real-time forensics.</p>	<p>Maintain privacy and compliance with human telemetry.</p>



ABOUT DTEX SYSTEMS

As the trusted leader of insider risk management, DTEX transforms enterprise security by displacing reactive tools with a proactive solution that stops insider risks from becoming data breaches. DTEX InTERCEPT™ consolidates Data Loss Prevention, User Activity Monitoring, and User Behavior Analytics in one lightweight platform to enable organizations to achieve a trusted and protected workforce. Backed by behavioral science, powered by AI, and used by governments and organizations around the world, DTEX is the trusted authority for protecting data and people at scale with privacy by design.

To learn more about DTEX Systems, please visit dtxsystems.com.