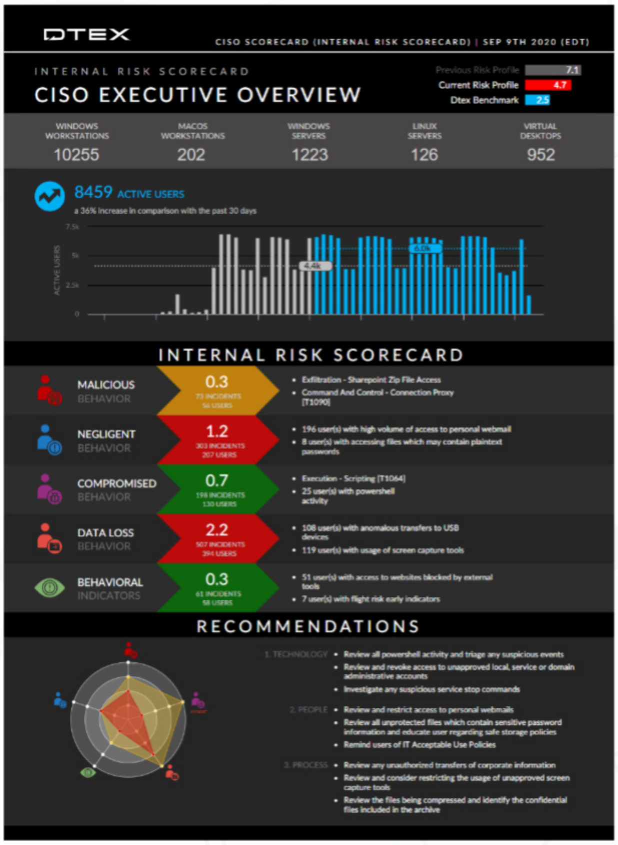
DTEX INSIDER RISK ASSESSMENT



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

DTEX has helped hundreds of enterprise organizations kick-start their Insider Risk Management program. Before making a considerable investment in the People, Processes and Technologies (PPTs) that underpin the program, it's best to first understand the actual Insider Risk Profile of the organization, from which an Auditing and Enforcement Program can be proposed and implemented to mitigate enterprise risk.

WHY PERFORM A 30-DAY RISK ASSESSMENT?

UNDERSTAND YOUR ORGANIZATION

The DTEX platform's visibility and analytics allow you to understand where your data is living, how your users interact with it, and where and how it's leaving the organization. You'll also be able to get an understanding of how users behave both on and off the corporate network. This knowledge is invaluable when it comes to understanding your organization's internal risk profile and prioritizing the PPTs to mitigate the actual risks.

AUDIT EXISTING SECURITY

Whether you're just starting the journey or have an extensive security program that includes DLP, UBA and SIEM, you still have no way of knowing if these tools are failing. Worse, there is no way to identify what data is slipping through the cracks. An Insider Risk Assessment will show you where your security is lacking.

SUPPORT REGULATORY COMPLIANCE

An Insider Risk Assessment will show you how your organization is either meeting or falling short of regulatory compliance. Enterprises in healthcare, financial services and other regulated industries across the globe use DTEX to ensure that they remain compliant.

WHAT WILL I RECEIVE?

At the end of your Insider Risk Assessment, DTEX will present a findings report, including:

- A benchmark comparing your Insider Risk Profile against other peer organizations
- A summary of each key finding by risky activity and threat severity level
- Details about the number of users engaging in each risky activity
- Details about the user population included in the assessment

WHAT DATA IS CAPTURED?

The DTEX platform comes pre-installed with hundreds of patterns of known-risky behavior. It also baselines normal user behavior so, over time, it begins to automatically identify sudden, high-risk behavior changes. This combination of visibility and analytics allows DTEX to identify all types of Insider Threats: malicious users trying to steal data, credential thieves and negligent insiders who may inadvertently put your security at risk.

PRIVACY BY DESIGN

DTEX's visibility doesn't come at the expense of privacy. There are no screenshots, no videos and no keylogging – no invasive information that could breach employee privacy regulations. What's more, DTEX collects its information in the form of metadata. This metadata goes through an optional anonymization process to strip out all identifying user information. As a result, DTEX is privacy compliant even under some of the strictest privacy laws in the world, including GDPR.

HERE'S HOW IT WORKS

FIRST HOUR
DTEX is installed in the cloud.

FIRST DAY
The platform starts detecting high-risk user activity.

TWO-WEEK COLLECTION PERIOD
The platform gets better at identifying anomalies as it learns your user baselines.

INSIDER RISK ASSESSMENT REPORT
Expert DTEX analysts analyze your data as it is collected. At the end of the assessment, they will generate a report to summarize and prioritize the DTEX Platform's findings in your organization.