User Behavior Intelligence for Defense:
The Key to Insider Threat Protection

Insider threats are a growing concern for defense organizations around the world, especially in the wake of high-profile insider breaches like the infamous data theft by Edward Snowden. A number of governments are going so far as to act on the insider threat vector through policy or regulation. For example, here in the United States, some organizations must comply with Executive Order 13587, which requires the development of an executive program for the deterrence, detection, and mitigation of insider threats. However, effectively fighting insider threats is complex and difficult. Dtex's User Behavior Intelligence gives defense organizations the cornerstone tool they need in order to detect and stop this growing problem.

The Dtex User Behavior Intelligence Platform

The Dtex platform combines lightweight user visibility, analytics that detect both "known-bad" behavior patterns and suspicious anomalies, and actionable alerts to provide powerful intelligence.

USER VISIBILITY

Our lightweight collector captures a complete audit trail in real-time. It is scalable, privacy-conscious, and gives you online and offline visibility.

USER BEHAVIOR INTELLIGENCE

Advanced intelligence pinpoints suspicious user behavior. Dtex detects both "known-bad" behavior patterns and baselines normal behavior to detect anomalies.

ACTIONABLE ALERTS

Dtex produces alerts based on an entity's risk score. This 'alert stacking' means that analysts only receive an alert when the user's total risk score reaches a pre-defined threshold, reducing noise and false positives.

Dtex Use Cases in Defense

For projects across a number of different defense organizations, Dtex has proved particularly useful directed towards the following specific use cases:

- Detection of unusual lateral movement within the network by authorized users
- Detection of unusual or malicious use by users who have legitimate credentials (employees or contractors)
- Detection of users executing multiple simultaneous logins
- Detection of unusual file access or file downloads
- Detection of data exfiltration (both from negligent and malicious users)
- Detection of user behavior in offline or off network modes (travel, mission, others)

Monitor Privileged Users

Dtex allows defense organizations to monitor privileged users without limiting their productivity.

Privileged and administrative users are often the most difficult to catch, as they cannot be restricted by lock-and-block policies. In fact, Edward Snowden was an IT admin with elevated access, which no doubt contributed to his success.

Dtex, however, is able to catch privileged malicious actors because it relies on visibility and analytics at the user-level, not broad rules or blocking. Unlike log-based monitoring tools, Dtex collects data straight from the endpoint – so it captures the data you need in order to catch advanced data theft, including every application used, every window open, all file and folder activity, all web activity, and more.

Dtex then establishes a baseline of normal behavior for every user. There's no need to develop special rules, which means that privileged users are covered the same as every other employee. When a privileged user behaves suspiciously, Dtex will alert immediately.

Achieve Security Off the Network

Dtex provides endpoint-based visibility that doesn't go dark when the user leaves the network.

With the rise of remote work and portable technology, defense organizations can no longer rely on perimeter security to protect extremely sensitive data. Dtex provides user behavior visibility directly from the endpoint itself. Dtex gives defense organizations visibility into devices even when they're off network (like at home or a coffee shop).

Stop Phishing and Infiltration

Dtex monitors and baselines behavior patterns that immediately alert on signs of external infiltration.

Dtex's ability to detect and alert on suspicious anomalous behavior also allows it to detect when a user's account has been compromised by an outside attacker. When a user exhibits wildly unusual behavior, combined with red flags like privilege escalation or lateral movement, Dtex alerts on compromised credentials for immediate remediation.

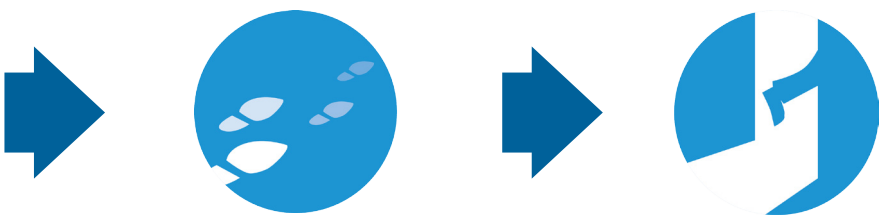
Detect Insider Threats at Every Stage

Dtex's visibility and analytics allow you to map insider incidents to each stage of the kill chain, allowing analysts to quickly evaluate, mitigate, and investigate threats.

RECONNAISSANCE
The user does research in preparation to steal data.

CIRCUMVENTION
The user circumvents security to exfiltrate data.

AGGREGATION
The user collects the data that they intend to steal.



OBFUSCATION
The user covers their tracks.

EXFILTRATION
The data leaves the organization.

Get a User Threat Assessment

to see firsthand how Dtex works in your defense organization.

E-mail: info@dtexsystems.com
Phone: +1 (408) 418 - 3786