THE DTEX INSIDER THREAT RISK MODEL

Insider threats can come from just about any angle, so that means you don’t just need visibility, you also need to know where to look. While the Dtex micro-agent provides the visibility, the Dtex Insider Threat Risk Model lets you know where you should be looking first.

Context is Key
The reason why lots of DLP and SIEM solutions don’t work is because they don’t take history, trends, and context into account. The result is a lot of false positives, wasted time, and ineffective monitoring. Dtex tracks each of your employees’ normal behavior and crafts finely-tuned alerts based on suspicious activity changes. By putting each user’s behavior in context, we create intelligent insider threat detection that picks up on only the activity that really matters.

How does it work?

1. Profile Known Risks: Sometimes the threat is known. Over the past 15 years, Dtex has continued to evolve and refine its library of known high risk activities. Every endpoint event is parsed through the Dtex library to highlight known high-risk behaviors.

2. Baseline Normal Behavior: Sometimes the threat is new. When trying to identify new or unknown threats, Dtex first focuses on what is normal. A baseline of normal activity is created for each user, device and application. Baselining metrics can include:
   - **Endpoint utilization metrics** – cluster analysis of software applications used, working hours, websites visited and task switching behavior
   - **File access metrics** – what files are regularly accessed, from where and in what quantities
   - **Account access metrics** – what login accounts are regularly accessed (users often have access to multiple accounts)

Total User Visibility

**Intelligent Endpoint Monitoring** – Dtex combines an incredibly lightweight micro-agent on each endpoint with a powerful server-based analysis engine to deliver security, visibility, and cost saving solutions.

**Advanced User Behavioral Analytics** – Dtex automatically builds a user-level profile of activity based on Dtex data not found in any log files, and automatically identifies sudden changes in behavior that indicate high-risk activity.

**Leading Insider Threat Detection** – Despite massive spending on security tools, the threat from insiders is greater than ever. No combination of existing security tools comes close to the simple, scalable visibility from Dtex.

Anonymous for privacy compliance
The Dtex patent pending approach to anonymization ensures that international privacy laws are adhered to and employee privacy is respected.

Metadata collected by the micro-agent is stripped of personal identifiable information without affecting the underlying risk model. This empowers the Security Team to rapidly investigate alerts while ensuring Legal and HR oversight when an alert turns into an Insider Threat event.

© Dtex Systems Group of Companies 2015
To determine whether activities are abnormal, we compare a user’s recent events against themselves (i.e. their own historical baseline), against their peer group (i.e. the baseline of users in similar departments or roles) and against the entire organization.

3. Understand the Context: The reason WHY is often overlooked. However it is often the most important factor in any Insider Threat investigation and usually cannot be answered without the experience of a seasoned security analyst with extensive domain knowledge.

Dtex has simplified this by incorporating contextual information of the events leading up to, and following, an Insider Threat event. An analyst can then use these contextual cues to easily investigate, acknowledge or ignore alerts generated by the system.

4. Evaluate the Risk: A risk is not always a risk. Some security risks (e.g. malware) are black and white; however when dealing with people risk (like an Insider Threat), black and white is rarely the case. Dtex understands this and incorporates the company IT Acceptable Use Policy within the Risk Model so that acceptable behaviors can be ignored and policy breaches highlighted.

The severity associated with known risky behavior, abnormal behavior and the context behind each event is aggregated into a single Insider Threat score which is used to prioritize alerts.

About Dtex

Dtex Systems brings visibility, transparency, and security to leading global organizations.

Now headquartered in Silicon Valley, Dtex was launched in Australia in 2000. Dtex has evolved into the lightest, most scalable endpoint solution in the world. Specifically designed for scalability and near-zero performance impact, Dtex is configurable for both local and multinational organizations. This mature, hardened technology enables Dtex to deliver the visibility, transparency and security needed by global businesses to prevent internal threats without compromising user privacy.

In addition to the core technical expertise, our international team has a deep knowledge of the legal, regulatory and business requirements for protective monitoring. While often supported by its service partners, Dtex retains full responsibility for project management to ensure the highest possible standard of service delivery for every customer.