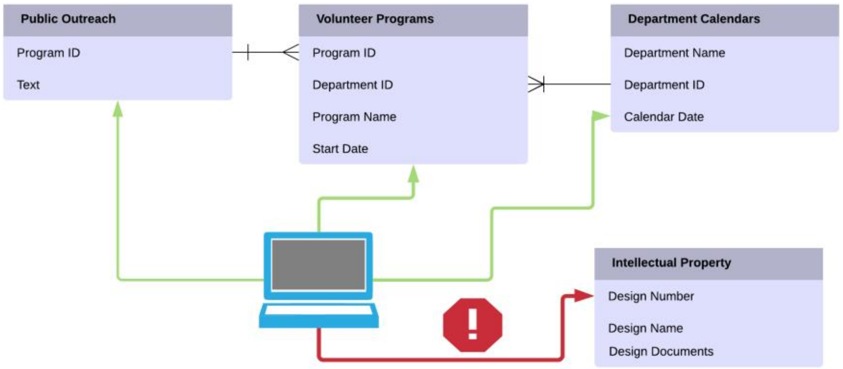
DB CyberTech Security Solutions:
Insider Threat

Predictive Data Loss Prevention
for Structured Data

Autonomous Threat Detection | Continuous Monitoring | Behavioral Analysis



Access behavior anomalies detected and alerted in real-time

Insider threats against high value structured data present a unique combination of challenges for security professionals:

- The tell tale signs of attack may be removed from the original point of compromise
- The technology involved often spans separate domains of expertise – networking and databases
- The source, by definition, is a trusted member within the environment

Insider threats pose a *substantial* business risk for loss of high value data. Nowhere else is sensitive data so concentrated as in structured data stores. This is because it's typically utilized across the organization and is a valuable information asset.

DBC Insider Threat uses predictive analytics to reduce your business risk of loss of high-value and sensitive data.

Major breaches that result in data loss are invariably preceded by days, and often weeks, of reconnaissance and other nefarious behavior. Rather than focusing on a narrow time window when the data was exfiltrated from the organization, DBC Insider Threat predictively identifies the behavior indicative of malicious intent. By proactively alerting you to such threats, DBC Insider Threat enables you to properly address data loss threat *before* it happens.

By spanning both the network and database domains, DBC Insider Threat shows threats in context.

KEY BENEFITS

DBC Insider Threat enables security professionals to:

- Stop the loss of high-value structured data *before* it happens
- Predictively identify behavior indicative of malicious intent
- Focus resources on threat analysis, not activity audit logs
- Continuously and non-intrusively monitor all structured data behavior

PREDICTIVE MACHINE LEARNING

DBC Insider Threat uses machine learning to:

- Automatically analyze the intent of each database query
- Pinpoint deviations from normal behavior that indicate compromised credentials and suspicious activity
- Provide the earliest possible warning – ahead of data loss
- Minimize security analyst work with intelligent anomaly clustering

CONTINUOUS MONITORING

As opposed to scanning and agent based technologies, DBC Insider Threat solution operates in real-time. Modeling and alerting are adaptive to change and always up to date with your structured data environment.

DB CyberTech
15015 Avenue of Science :: Suite 150 :: San Diego, CA 92128
www.dbcybertech.com

INTELLIGENT BEHAVIORAL ANALYSIS

DBC Insider Threat uses deep SQL protocol decoding and semantic analysis to understand the structured data conversation in context:

- Which database was accessed?
- Which table was accessed?
- What kind of access was it (read, write, grant, etc.)
- Which client was used?
- When did it happened?
- What queries were used?

NON-INTRUSIVE OPERATION

DBC Insider Threat operates processes a copy of network traffic. The solution is not inline, so there are no performance impacts on your structured data environment. In addition, it's discovery capabilities require no scanning or configuration setup to locate and monitor structured data assets.

FLEXIBLE EXTENSIBLE POLICY

DBC Insider Threat includes an optional policy layer. This layer enables security professionals to build up a *behaviorally-driven* set of policies for alerting, or encode existing network and database policies for continuous monitoring.

Scanning based approaches are inherently out of date, limited to a subset of your environment, and have no visibility to data in motion. In contrast, DBC Insider Threat uses patented layer 7 extraction and deep SQL protocol decoding to identify, parse, and understand each database conversation in full detail. This occurs in real time ensuring DBC Insider Threat events are timely, high quality, and detailed for adjudication. You will see which client maliciously accessed which tables on a database, and exactly how they did it.

Underpinning DBC Insider Threat's approach are a collection of predictive machine learning technologies. Since insider threats cannot be identified based on their identity alone, DBC Insider Threat uses machine learning driven behavioral modeling to recognize anomalous *behavior* involving structured data. Related anomalies are grouped together using intelligent clustering to form easily adjudicated incidents. Incidents group behaviors such as abuse of credentials or distributed attacks on specific high-value assets.

DBC Insider Threat operates off of a network SPAN or TAP. Therefore, it's not inline and operates completely non-intrusively. Agent based solutions can fail, destabilizing your critical infrastructure, while also limiting the scope of what they monitor. In contrast, DBC Insider Threat imposes no load on a database infrastructure. Moreover, DBC Insider Threat is agnostic to the location of structured data assets in the environment, automatically monitoring and modeling the behavior around each and *every* one.

For additional information or to arrange for an online demonstration contact us at info@dbcybertech.com.

Requirements and Specifications

Supported Database Management Systems

Oracle server release 8i (8.1.7) or later
Microsoft SQL Server version 7 or later
SAP Sybase ASE version 12.5 or later
IBM Db2 Mainframe (DSN)
IBM Db2 LUW (SQL)

DB CyberTech