Identifying Insider Threats Through Machine Learning and Behavioral Analysis

NETWORKS®

Table of Contents

Foreword

When we speak of insider threats various connotations come to mind. Perhaps you think of whistleblowers trying to damage an organization by leaking proprietary information or maybe employees seeking to profit through persistent industrial espionage. While these examples certainly represent a credible danger, there's a category of risk that includes a much more significant threat — malicious outsiders who penetrate systems by stealing legitimate credentials and thus appear as insiders.

Existing perimeter security mechanisms are proving to be ineffective against the insider threat. Hackers have also evolved their abilities to the point that the security perimeter has become extremely porous. Traditional perimeter security relies on white lists / black lists and signature files that are continuously updated to address the latest threats. Such tools aren't geared towards detecting and preventing potentially harmful activities performed by (allegedly) trusted corporate entity acting for within the boundaries of the organization. Traditional perimeter security tools are positioned in the wrong location on network to monitor for insider threats. Further, the organizations core assumption is that authorized corporate users should be trusted. In today's reality – such assumptions and security approaches are obviously falling behind the new breed of threats.

Given that the most important information resides in databases, organizations are increasingly turning their focus toward databases security technologies. To defend databases from attackers using stolen credentials, the industry is beginning to adopt a new security paradigm based on machine learning and behavior analysis.

How Credentials Are Stolen

Recently cyber attackers broke into the databases of a very large U.S. financial institution. The attackers stole detailed account information of 76 million households and 7 million businesses. This information, combined with data stolen from several other financial institutions, was then put to nefarious uses ranging from stock manipulation to Internet gambling crimes.

Fortunately the group was not particularly talented at covering their tracks—three out of the four hackers were arrested and charged with cyber crimes. Investigations revealed the criminals had actually used tried and true attack methods. One hacker stole the credentials to online brokerage accounts through a simple phishing attack while other sites fell to brute force attacks. It appears the cyber defenses of these financial institutions fell as a result of fairly pedestrian forms of credential theft.

In some cases credentials can be trivially easy to steal. One of the most basic forms of credential theft involves a phishing email that invites the user to log into their account. The attack instead directs the victim to a fake login page that harvests their username and password. A more sophisticated form of this approach, known as a "man in the middle" attack, will immediately transmit the captured information to the actual login page, and seamlessly log the real user in—rendering the user entirely unaware that an attack has taken place. This attack works equally well for external websites as well as internal applications and servers.

Detecting Stolen Database Credentials

Most organizations lack the necessary security tools to identify when compromised credentials have been used to access the organization's databases. An attacker who has obtained legitimate credentials essentially appears as a legitimate insider. As far as SIEM tools or firewalls are concerned, they're a ghost. If database monitoring were operational it may detect the unusual activity. However database monitoring is often configured for compliance rather than security. Also agent-based database monitoring tends to be complex, rules base, expensive software that is difficult to configure properly. It also must be implemented individually on every database in the enterprise requiring monitoring and this is rarely done. Does the organization even know how many databases they possess? Sadly for the majority of organizations, research indicates the answer is "no."

Human intervention—assigning a pair of human eyes to watch for signs of compromise—may seem to be a reasonable solution. However, security teams

tend to be chronically under-staffed as it is. A 2016 Osterman Research report found that 47 percent of companies don't have an individual or team specifically assigned to database security. In an enterprise with thousands of users and hundreds of databases, it seems highly unlikely that any amount of human resources could detect a malicious insider.

DB Networks "Dataflow Model"

DB Networks introduces a new approach, combining internal network monitoring, deep analysis of every database conversation (dataflows) on the network, and an adaptive model to create and maintain a corporate policy of what's considered safe vs. unauthorized or risky. Oftentimes, in the absence of explicit detailed corporate policy for what every user and role can do, the best way to determine the policy is to observe live traffic on the internal network to determine a 'controlled normal operation mode', which is precisely what DB Networks solution does. Once sufficiently established, the monitoring system (DBN-6300) assesses the risk of every deviation from the norm to decide whether to trigger a security related action, require the attention of a user, or render the deviation safe and integrate it into the already established baseline. Reaching a proper determination of the risk may appear simple but in reality it requires advanced technologies. This involves a combination of unique methods to extract data from every dataflow as well as structural and semantical algorithms to analyze the observed traffic. The system continually refines and adapts an efficient behavioral model to compare new behaviors to the learned model. In addition, the system allows security staff to layer internal facing policy controls on top of the behavioral model to leverage their knowledge of the network.

Most Typical Insider Threat Scenarios

In most cases an insider threat will rely on some form of compromised or abused credentials to gain database access. There are several methods in which credentials may be abused, each one posing a different risk level. We'll next examine some of the most interesting scenarios.

1) Rogue Agent Infiltration

A primary concern in corporate IT security is that of an agent penetrating the internal network. This agent could be a piece of malware that a corporate user unintentionally brought in or an attacker that managed to find their way into the network. Should this occur many bad things are possible, chief among these involve gaining access to high value information assets. Such an infiltration most commonly targets a vulnerable system and makes use of its credentials (user or machine credentials) to access resources within the corporate environment. In

recent years, such rogue agents have developed significantly and are now able to penetrate and execute their attacks — overcoming traditional defense layers. They operate in a stealthy fashion and for an extended period of time, thereby causing much wider damage.

2) Corporate User Misconduct or Going Rogue

In every organization, privileged users are authorized to perform highly sensitive activities in the general course of their job requirements. There's an inherent difficulty in making certain that privileged users are in fact performing in accordance with corporate policies and expectations. Typically these privileged users access and maintain high-value corporate information assets. Obviously each of these privileged users should be considered a risk factor for data loss, not just because of a breach of their credentials, but also because these privileged users may be driven to act against corporate interests and abuse their credentials for a personal gain. Traditional perimeter security tools would be completely blind to such a risk.

3) Shared Privileged Accounts

This scenario, while being an unfortunate common practice in the corporate environment, poses a significant risk to the whole organization. In this case a single privileged administrator account is shared among multiple users. It is done for convenience and ease of operations. While typically the existence of these accounts is not a result of a malicious intent, shared privileged accounts pose a risk of uncontrolled access to data, as well as a higher potential of credentials reaching the wrong hands. At the same time, they provide a larger space for malicious users to hide, confounding monitoring and investigation of malicious activity. Security aware corporations today are looking for way to eliminate this phenomenon using every possible mean, in many cases not with a great success.

The above scenarios may appear in different flavors and specifics however they all do have a key common theme, which is the access and exploitation of legitimate corporate credentials. The result is that new security mechanisms can no longer rely on the assumption that privileged user accounts or computers on the network should be trusted. Alternatively, new approaches to manage the risk begin with a risk assessment, most typically by analyzing a large set of data to create a risk score that is then used to establish a policy.

The Insider Threat Framework

To address the problem of abused credentials alongside other types of insider threats, DB Networks developed an insider threat mitigation framework to assess, monitor and analyze potential insider risks. Making use of specialized

algorithms to analyze data flows on the network, DB Networks designed a way to prepare for, detect and analyze actual insider threats that appear on the network. The use of the framework is done in three phases –

- **Baselining the Database Infrastructure**: During this phase, a model of normal behavior is created. The portion of the network and database activity that does not converge into a normal model is identified.
- **Stability Analysis**: Over time a relatively stable picture of database interactions should emerge. Consistent variability and unstable behaviors tends to indicate the existence of a threat. As an example, the reconnaissance phase of and Advanced Persistent Threat would be revealed in activity that would vary greatly, perhaps even chaotically from the norm.
- **On-going Monitoring**: IT environments can change quite significantly over a relatively short period of time. With an initial baseline assessment and active threat detection in place, on-going monitoring identifies behavioral changes that represent threats to the database environment.

DB Networks Technology

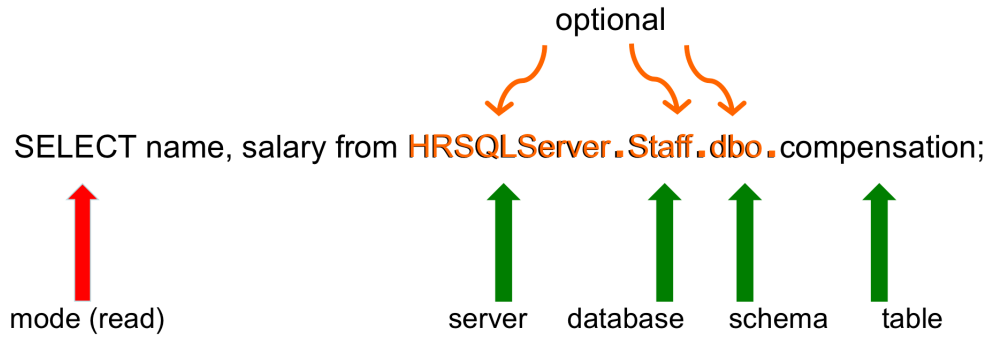
To achieve an effective insider threat framework, DB Networks has built new technology to generate a behavioral model of a large set of database activities observed on the network. This representation is intelligent and will detect a wide array of behavioral changes, whether they are major (such as a significant surge in new types of dataflows directed at a specific database table) or minute (such as an authorized user querying a table not accessed previously).

DB Networks uses continuous network monitoring and analysis technology to achieve these capabilities. It observes and analyzes every communication on the network. It then delves deep into the database interactions (dataflows) and extracts a wide array of attributes. As part of this process each extracted SQL statement is semantically analyzed. The system then automatically generates a behavioral model combining the contextual attributes of each dataflow with semantical artifacts that are extracted from each dataflow. Combining a large number of dataflows this model establishes a strong representation of normal business related SQL activities in the observed corporate environment. This model is then used to detect new behavioral patterns not previously seen. An implicit behavioral policy determines the risk level of each new behavior and whether or not it should be authorized or restricted. New dataflows that violate this policy may point to insider threats in the form of insider breach, an APT activity or other risk bearing policy breaches.

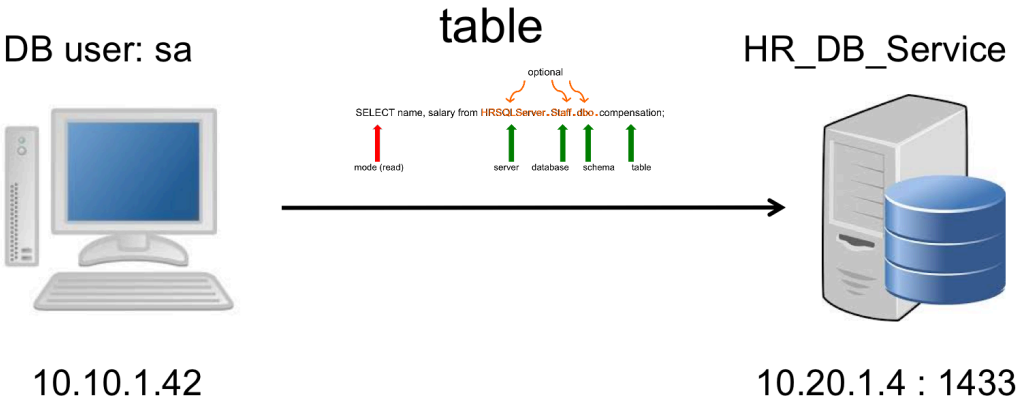
Diving deeper into the technology, DB Networks collects information about every

dataflow observed on the network. A dataflow is defined as the combination of a context and a database object, for example a table being accessed.

Table Example: The (fully qualified) table name, which is the actual asset that is being accessed.



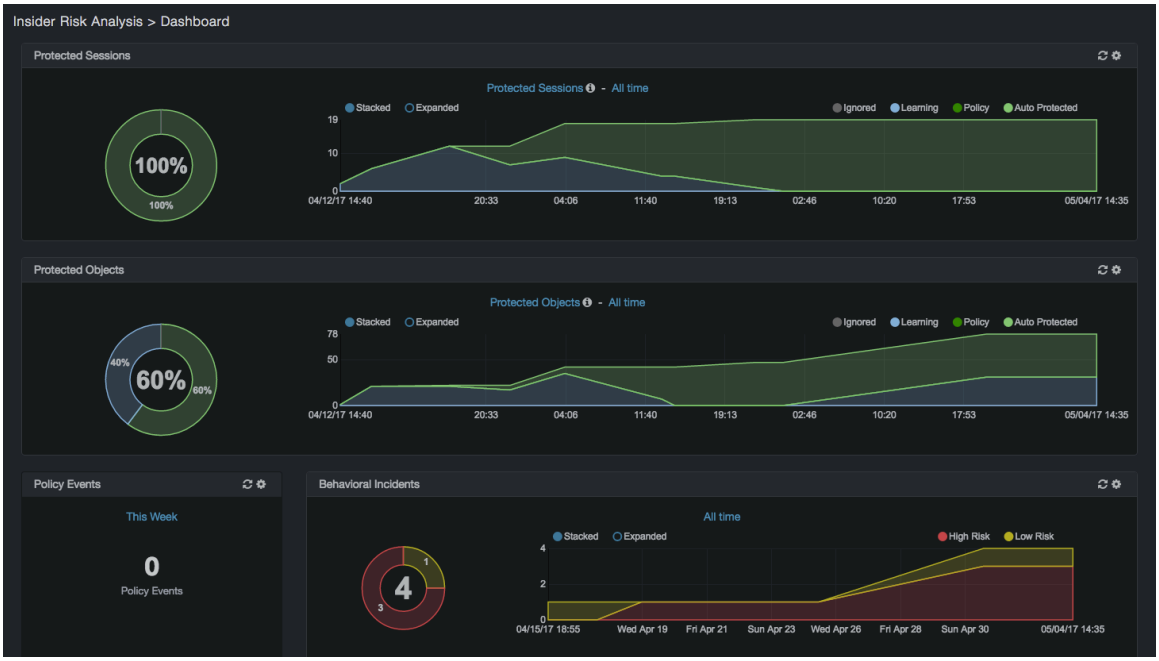
The dataflow context is defined based on the network connection characteristics - the client IP address, the server IP address and port, the database user account and the database service name that is being accessed.



DB Networks then builds a map of all the dataflows observed on the network. It automatically creates a behavioral model based on those database objects and contexts that demonstrate stability. Stability is reached when activity around a context or table is consistent over time. What's more, the model suggests that stable elements are strongly correlated with business value. That is – typically, a high-value table is accessed by a small and stable set of (privileged) contexts, and on the other hand – a single stable context – will access a small set of

stable high-value tables.

Once this model matures, DB Networks monitors deviations from the norm, or a change in the context of a stable element (e.g. the client IP used to access a table has changed or a new table name is observed from a previously stable context). Such a change may be associated with a new risk that needs to be managed; DB Networks offers a risk factor to focus the attention on the most significant anomalies.



Lastly, DB Networks offers an analysis and visualization layer that helps the user to quickly vet and focus his attention on high value assets and disregard parts of the environment that bear low or no risk. This visualization layer offers a multidimensional drilldown process of all the data flows in the system and focus the user's attention to critical areas, quickly and efficiently.

At each level of the drilldown process, any of the unspecified set of 20+ simple and aggregate dataflow features can be isolated, and then selected by distinct value (or set) to narrow down the scope and quickly zoom in on interesting behaviors.

It also enables to user to generate manual monitoring rules related to high-value assets that augment the machine-based models where appropriate.

Benefits of Continuous Monitoring

Using intelligent continuous monitoring of database traffic to identify insider risk and detect potential threats, DB Networks offers several benefits in the area of insider risk allowing the organization to maintain a reasonable risk level around their high value data assets.

Continuous risk assessment: To stay ahead of the surfacing threats, every organization needs to keep track of key risk factors related to their high value data assets. DB Networks offers a unique and powerful way to continuously measure this risk. This is accomplished through sematic analysis of SQL activity constructed from a behavioral model of SQL activity. Advanced tools focus security personnel attention on risk bearing critical assets and how they are being used.

Detect credential abuse: Also importantly DB Networks offers a unique view of insider threats in action. Using its advanced algorithms, it detects anomalous activities indicating credential abuse. A risk score per anomaly and contextual explanations of the risk is provided to assist with remediation.

Advanced forensic analysis: Finally, DB Networks delivers investigation tools for incident response. DB Networks offers a multi-dimensional view to thoroughly review aspects of potential threats. It enables a user to easily correlate any suspicious activity associated with high-value assets and assess the potential impact.

Best Practices for Credential Management

The following are additional recommended best practices for enterprises that wish to reinforce the security of their network as part of a defense-in-depth strategy.

Audit the Entire Database Infrastructure

Assessments conducted by DB Networks suggest many enterprises possess far more active databases than they know about. It is vital, for purposes of both security and compliance to comprehend the entire database infrastructure. Often unknown databases are discovered they have default credentials enabled.

Implement Privileged Session Management

A privileged session manager acts as a credential proxy to connect users to target systems. It can then monitor and record the session without actually exposing privileged credentials to individual users or their endpoints

Enforce Least Privileges

As personnel move through positions within an organization, they will often accumulate numerous privileges, many of which are no longer required. Further, some users are given privileges that are larger than they need to ensure they can complete a task without any further change in permission. If these users are in IT, and if they have access to privileged accounts that they never relinquish, then these high-privilege individuals will become a single point of failure. Losing just one set of credentials could potentially expose numerous sensitive systems. Enterprises must be vigilant in tracking which users and applications have access to what databases.

Avoid Shared Credentials

Share credentials expose systems to multiple threat vectors and make detecting the source of credential loss harder to determine. It flies in the face of least privilege and should be avoided at all cost.

Improve Password Policies

Lacking policies to the contrary, employees will routinely choose simple-to-

remember and extremely weak passwords. For example, weak passwords have few characters with no numbers or any special characters. Such passwords are highly vulnerable to brute-force credential theft. Anyone with even a rudimentary knowledge of hacking tools can break a weak password in short order. It's not enough to simply enforce strong passwords. Enterprises should make credential management easy for employees. A Single Sign-On (SSO) solution with Multi-Factor Authentication is certainly a step in the right direction.

Conclusion

Insider threat is a widely observed risk in the IT industry today. It is considered one of the top concerns in IT security due to its devastating impact on business, reputation, and loss of intellectual property. In most cases an insider threat will rely on some flavor of compromised or abused credentials. Security technologies that are most widely used today fall short in attempting to mitigate this class of risks. Not only are corporations challenged with addressing the insider threat, they struggle with even defining and scoping the risk - given the visibility gap into the most sensitive assets in their environment. DB Networks technology targets this exact problem, focusing primarily on the most valuable data assets stored in the corporate databases. Through non-intrusive network monitoring, DB Networks collects information about every data flow observed on the network, analyzing and learning to create a behavioral model. Each new data flow is evaluated against this behavioral model to identify deviations, derive the risk levels, and determine the meaning of the observed gap. It then reports these deviations and attaches a risk score to each of them enabling security personnel to immediately focus on the most important events. Powerful tools are available to investigate the scope, the risk, and the business context of every deviation observed.

Through this approach DB Networks enables its customers to continuously assess the risk of the entire environment and of specific entities in it. While monitoring the network it surfaces suspicious activities that demonstrate risky anomalous aspects to allow the user to quickly focus on what might become the next insider breach. In today's hostile cyber environment, DB Networks offers what has become an essential line of defense against destructive cyber attacks.

Learn more

To find out more about how to gain deep visibility into your database networks and improve your database security, contact DB Networks at +1-800-598-0450 or email info@dbnetworks.com.

DB Networks®
15015 Avenue of Science
Suite 150
San Diego, CA 92128
Tel: +1-800-598-0450
www.dbnetworks.com