Gaining Visibility into Enterprise IT Security

BY YOSEF BECK AND JEFF B.

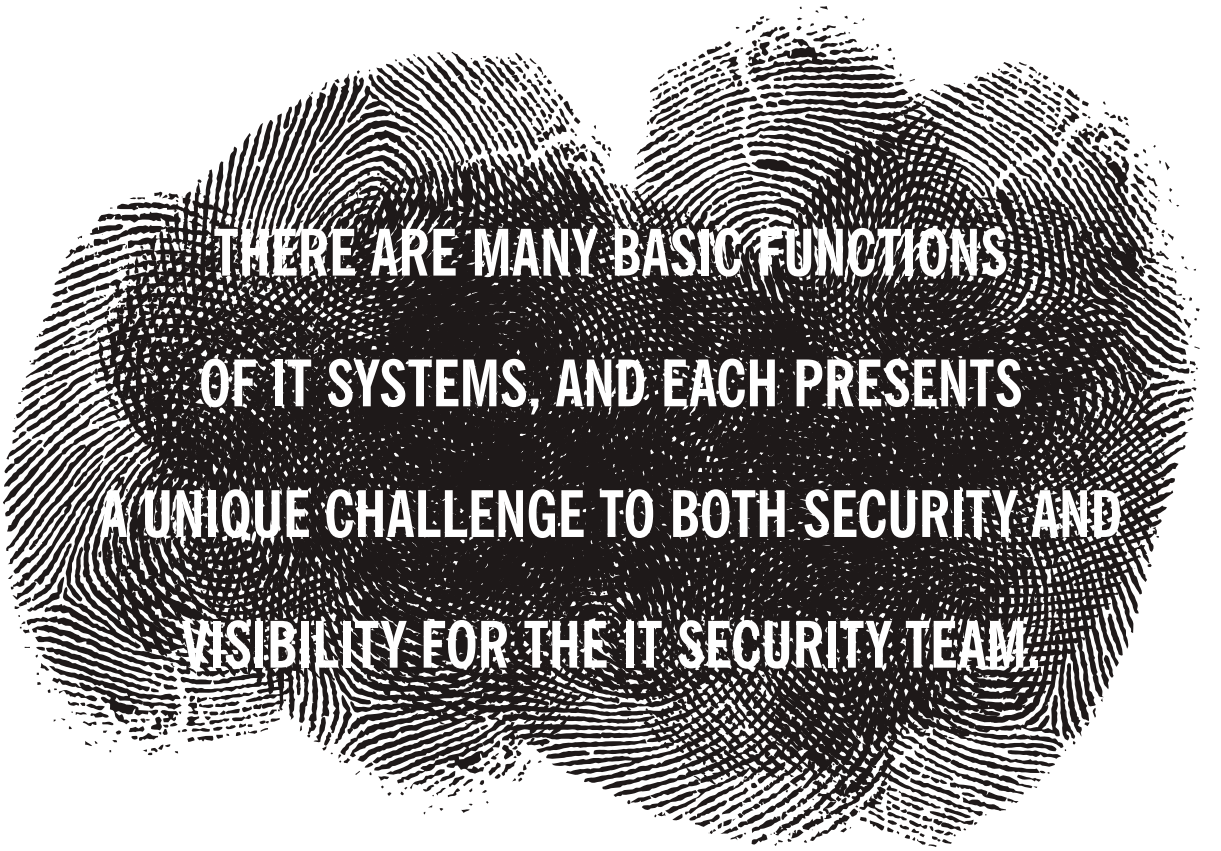
The Importance of Monitoring for Enterprise IT Security Pitfalls

Enterprise Security IT teams face enormous challenges in securing their infrastructure environments. Network Architecture complexity, volume of servers and users, along with simply finding available time to audit existing systems are all obstacles to effective security. Currently, there is no single, integrated tool that will provide you with this ability.

There are many basic functions of IT systems and each one presents a unique challenge to both security, as well as, visibility for the IT security team. In all of these functions, the goal is to minimize the number of people with access and monitor IT activities for odd behavior. An example of odd behavior would be monitoring system logs for remote access requests by accounts that should have been deactivated. In addition, wherever possible, do not include private or sensitive information where anyone can easily view it. Finally, if there is no other option, ensure that information is encrypted before storing it in a public location.

Over the course of dozens of projects, we have observed that the following basic functions are common pitfalls of corporate IT security, and could benefit from applying the security best practices listed above:

- **Remote Access** is the ability for an individual to access a computer or network from another device. Leaving remote access turned on without ensuring the right people are accessing it is like leaving the back door of your house open. Typically, users having remote access are advanced users and it is commonplace to see these same users with local administrative privileges to the environment. Know which individuals have remote access to server assets to help secure a corporate network.
- **Environmental Variables** - Commonly used to store information for applications in an operating system or program, environmental variables are keys or value pairs that are typically stored unencrypted. Due to their ubiquitous nature, it makes them a logical choice as a place to store credentials for applications to use. However, consider a situation where a user's login credentials are stored on a server within environmental variables. If they are unencrypted, any individual with access to that server can see those environmental variables. Storing them unencrypted is like leaving a pair of keys on your doorstep for anyone to copy. Make sure to encrypt all sensitive or private files.
- **Open Database Connectivity Connections (ODBC)**, is a middleware application-programming interface (API) for accessing databases. Similar to leaving a list of addresses out for anyone to read, ODBC connections are created and stored on a server for applications or processes to consume. Like Environmental Variables, ODBC connections are also typically stored unencrypted and may contain user names, passwords and server information.
- **The Windows Registry,** unique to Microsoft Windows, is used for many things, one of which is storing application specific information. Server names, database names, and user credentials may be stored in the registry. An individual with permissions to a given machine's registry could gather a lot of information about a company's infrastructure with a cursory review of the data stored within.
- **XML configuration files,** text files, and INI (configuration) files, in addition to others, are used to store server data and sometimes user credentials in unencrypted text. Typically maintained in a human-readable XML configuration file, this information is easily available to anyone with enough user permissions on the client machine.
- **Databases** by definition store information. This information is commonly stored in tables or files on company servers. A database having a



configuration table containing unencrypted information such as servers and user credentials poses a security risk as individuals having access to the database tables could potentially access this information.

To complicate matters further, a company will typically have multiple servers, multiple client systems, multiple databases, and multiple connections to external applications or systems. Each server or database may be running completely different operations systems, multiple versions, etc.

GAINING VISIBILITY:

Consider the following example of what could be done to help mitigate risks in security or visibility. Suppose a company did not have any formal way to audit the users in its database systems. The company's IT security team is able to gain partial visibility into the security of their IT ecosystem by using freely available scripting tools.

The tools had remote access abilities allowing one to write and run a script on a single server in order to access multiples of other machines. The scripts can consume objects exposed within the Microsoft Windows framework including built-in Active Directory, SQL Server, SharePoint, Exchange, cloud-based Azure, and Office application support.

By using simple scripts, the company is able to feed an Excel-based dashboard. The dashboard shows every single user and group permission to every database server (of one database system type) in the enterprise. This allows the company to maintain its security policy by being able to audit user's server permissions.

In addition to user and group permissions by server, the company is also able to pull in specific Active Directory-based information such as a user's full name, title, manager's name, as well as the last date/time that the user signed into a system.

Now suppose the complexity of the issue grew more apparent as the company discovered it had multiple, nested permission groups. In other words, a user might have had access to a database server simply by being attached to an Active Directory group, which in turn had the proper server permissions. That Active Directory group might then reference another group, which in turn could reference another, and another, and so forth. The scripts are able to handle this by iterating through all nested groups, regardless of how deep the nesting went.

The Excel-based dashboard contains color-coded KPI's to make identification of specific use cases quick and painless. For example:

- Red indicates that a user is no longer a full-time employee or contractor within the organization because the user no longer contained any Active Directory information or they had not signed into the domain for many weeks or months.
- Yellow indicates that user had not used a server. Subsequently, if the user is still in the organization and had not signed into the domain for several days, an email is written to the user's manager to verify if permissions to the database(s) were still required.
- No coloring indicates that there were no known issues with a user's permissions or access.

From the gathering of information stored in the central management server, the reading of Active Directory data, and the creation of an Excel file on the server, it could all be done from within the scripting API framework. The next step for this company would be to tie in other database systems, as well as, other system applications to gain further visibility across the IT ecosystem.

SUMMARY

Enterprise IT teams face enormous challenges in securing their infrastructure environment. Visibility into the security of a company can be like trying to look into a black hole. People, money, time, processes, and technology can be poured in, but without the proper tools in place to see through the darkness, it could be a waste of valuable resources. While there are very few tools that give good insight into the security of a business, by using basic scripting tools, utilizing application programming interfaces (APIs), and understanding how an IT organization's systems are linked together, an organization can begin to gain visibility into its security black hole.

YOSEF BECK
yosef.beck@jabian.com

Yosef applies his expertise in systems analysis to his passion of security optimization

JEFF B.

Jeff specializes in database systems with experience in IT security for the enterprise