REAL-TIME PREVENTION OF MALICIOUS ACTIVITIES

Shell Control Box Use Case

"ACHIEVE A HIGHER LEVEL OF SECURITY BY INSTANTLY BLOCKING HARMFUL USER ACTIONS INSTEAD OF JUST MONITORING OR REPORTING THEM!"

The Challenge – Uncontrolled Access of Privileged Users

Your privileged users, such as administrators or developers, are a potential security risk in many situations. Even if your network is properly protected, your critical systems must be made available for maintenance, and this requires remote administrative access. However, if these administrators accidentally - or intentionally - execute harmful commands or programs, they can cause great damage to your IT environment, or even your business.

In addition, despite the best efforts of security experts, credit-card fraud or financial data leakage are still serious threats. Detecting or, even better, preventing such information leaks is also a requirement of the PCI Data Security Standard (PCI-DSS). But implementing that in real life is not always simple. You could easily find many solutions to monitor web, e-mail, IM or FTP traffic, and although these might cover a large portion of user activities, some covert-channels still remain.

The Solution – Real-time alerting & blocking with SCB

The BalaBit Shell Control Box (SCB) is an activity monitoring appliance that controls privileged access to your remote servers and networking devices and records activities in movie-like audit trails. Starting with version 3 F4, SCB can also monitor the network traffic in real-time, and execute various actions if a certain pattern (for example, a suspicious command or text) appears in the command line or on the screen. This functionality helps you prevent malicious user activities as they happen instead of just recording or reporting them! Before a potentially harmful action takes place, SCB can perform the following steps:

Immediately terminate the connection

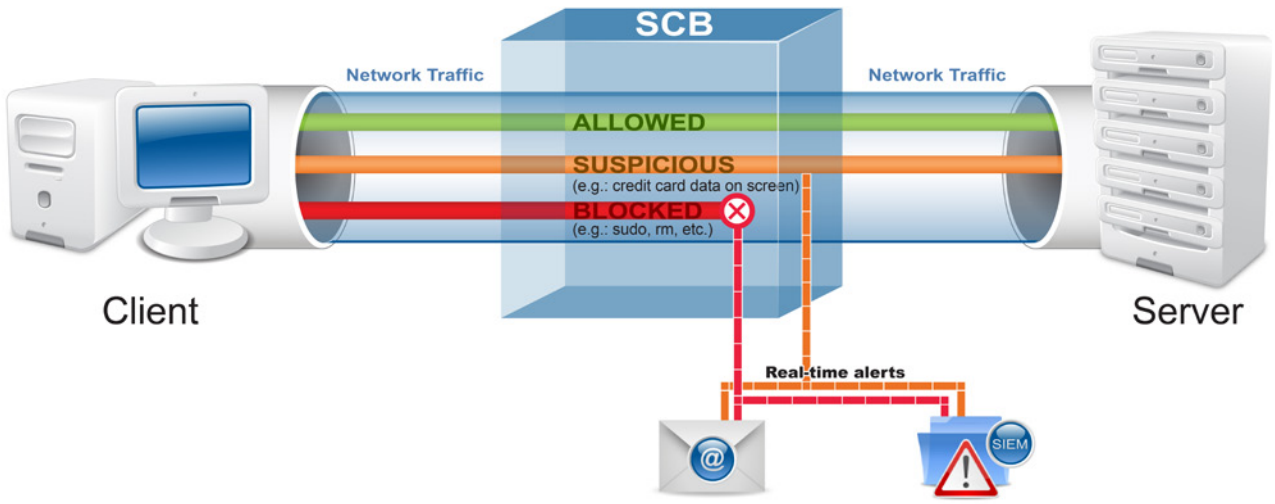
Send an e-mail alert to the auditor

Log the event in the system logs

Send log message to a SIEM application (or SNMP trap to a ticketing system)

Store the event for searching and reporting

Real-time alerting and blocking by SCB



For example, this allows you to:

1. Detect commands and applications

Since content-monitoring is performed in real-time, SCB can prevent harmful commands or applications from being executed on your servers. For example, SCB can block a connection before a destructive administrator command, such as the „delete" comes into effect. In addition, SCB can also prevent starting database manipulation from the command-line, or the elevation of user privileges, such as the "sudo" command. For example, you can configure SCB to alert if any SQL command is used in MySQL, except for the "SELECT" command. Or for example, you can configure the appliance to block the "enable" command, thus preventing the user to enter privileged mode on Cisco devices.

Another example can be defining a policy to immediately block the RDP session if a user opens the 'Administrative Tools' window on a Windows Server 2008 system.

2. Prevent data leakage

SCB can monitor network traffic in real-time, and execute various actions if a certain pattern appears on the screen. As SCB is always in-line of the actual traffic, it checks and analyzes the screen updates received from the server before forwarding the data to the client application for display. The patterns to detect can be defined as regular expressions. For example, if you define a pattern for specific fiscal values, you can prevent leakage of sensitive corporate financial information.

3. Detect credit card numbers

SCB's built-in detection engine finds the valid credit card numbers on the screen, and counts how many unique credit card numbers appear in a given session. Since SCB examines the terminal screen, it can detect the credit card numbers regardless of the accessed application or server. If the number of detected credit card numbers reaches a configured limit, different actions could be triggered, such as sending an e-mail or logging the event to a SIEM system for further correlation or reporting.

Benefits for Your Company

Real-time alerting in privileged sessions allows you to block connections that violate your user-specific rules, and also send alerts in such cases. Overall, this real-time monitoring and prevention functionality is a major step forward in tracking and controlling the activities of users. Instead of just gathering gigabytes of recordings and tons of logs, you can track user activity as it occurs. In many cases you need notification instantly, because recording activities and running forensics analysis later can be already too late. Real-time prevention takes your privileged account monitoring to a new level, similar to how Intrusion Detection Systems (IDS) evolved into Intrusion Prevention Systems (IPS) and next generation firewalls later.

About BalaBit

BalaBit IT Security is an innovative information security company, one of the global leaders in developing privileged activity monitoring, trusted logging and proxy-based gateway technologies to help customers be protected against insider and outsider threats and meet security and compliance regulations. BalaBit, the second fastest-growing IT Security company in the Central European region concerning Deloitte Technology Fast 50 list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Its R&D and global support centers are located in Hungary, Europe.

More information: www.balabit.com

Learn More

- Shell Control Box homepage
- Request an online demo
- Request a callback
- Find a reseller