SECURESTRUX
Cyber Smart | Cyber Secure

Data Transfer Auditor

INSIDER THREAT AUTOMATED SOLUTION

HIGHLIGHTS

- Monitor behavioral analysis of priviledge user activity is critical in fighting Insider Threat.
- Automated solutions that monitor data transfer activity help reduce the strain on human resources, and provides real-time actionalable alerts to leadership.
- Solutions that leverage tools alread native to the operating systems reduce the cost, maintenance and compatibility concerns that arise with third-party products.
- DTAuditor provides the DoD community with a flexible optionto meet todays complex requirements in a time of constrained budgets ans sequestration.

BACKGROUND

Unlawful disclosures of classified information have substantially impacted our national security. They have required leadership to take a harder look at policies and oversight mechanisms for protecting our nation's most sensitive data. Employees and contractors with the boundless privilege to access sensitive data present a greater risk of intentionally, accidentally, or indirectly misusing that privilege and potentially stealing, deleting, or modifying data. Humans are often the weakest link in the intersection of people, process, and technology, the three tenants of security.

Privileged users with malicious intent can cripple a closed system faster and more effectively than the external expert could on an open system. The insider threat has more time and knowledge of the system and its controls and is usually not under any suspicion. The insider often has a network loaded with information that may be stored on removable media. The insider's anonymous misuse and activities many times go unnoticed without the presence of practical audit tools, especially those that can detect the removal of large data quantities to removable media.

Since 2009, and more recently, in July of 2014, United States Cyber Command (USCYBERCOM) mandated various requirements for the control of classified data placed on any removable device in a directive geared towards insider threat mitigation. The directive addresses both authorized and unauthorized users who attempt to copy or move data from a classified system to a removable device. Removable devices can be optical disks such as CD and DVD, storage memory such as USB devices, and PCMCIA Cards. For this paper, only storage memory is considered because optical disks require a different operating system process to "burn" the optical device versus other storage media. Optical disks will be considered in the near future.

THE CHALLENGE

When it comes to user behavior, the threats that organizations typically face, fall into the categories of either policy violations or specific malicious activities. Event management logs are typically focused on who is accessing the system and what they are doing during access; however, further analytics must focus on privileged users to detect anomalies in behavior. USCYBERCOM directives have established more precise policies around established user patterns.

THE SOLUTION

For Windows Operating Systems, SecureStrux has developed a unique and flexible solution combining powerful built-in tools and techniques already native to the operating system to capture file creation, deletion, and change events for all removable storage memory. All of the information collected is easily recorded and sent to Syslog collectors for further analysis and monitoring. The following features are used and executed within the native Windows Operating Systems:

- Auto-detection of a removable device

Data Transfer Auditor

INSIDER THREAT AUTOMATED SOLUTION

- Capture all file creation, deletion and update events
- For each file action, capture the following meta data:
  - File name, to include the file path and logical drive
  - Time stamp
  - Action [create, delete, update]
  - User Account
  - System Name
  - Amount of data in bytes (could be negative for deletions and updates)
  - Record meta data to windows event file of choice
- The process runs quietly in the background
- Start the script on boot up
- Maintain one instance of the process running at all times
- Protected process from shutdown using HBSS HIP signatures or another similar method

The Data Transfer Auditor allows leadership to monitor and subsequently control the amount of sensitive or classified data moved to removable devices by authorized users to detect the possibility of security violations and reduce the risk of insider threat. Additionally, the Data Transfer Auditor demonstrates adequate and consistent compliance with the requirements and intention of USCYBERCOM Directives.

SUMMARY

With sequestration in full effect and despite the growing need for cyber innovation, USCYBERCOM will take a 7% hit in spending in 2016, meaning the Command as a whole, will have to do more with less. Most agencies and organizations are understaffed; therefore, effective automation can reduce the strain on human resources, and yet still provide valuable, actionable information to reach leadership quickly. Data Transfer Auditor can also enhance an organization's security posture by providing more rapid detection and response capabilities that minimize insider threats and prevent future breaches. Research has shown that increased response time reduces the impact and recovery cost of breaches.

Third-party Data Loss Prevention (DLP) solutions are available, but are costly and require extensive training and tuning. For most organizations, these products introduce an additional cost of procurement and maintenance. By utilizing our unique solution, we leverage the built-in Windows Operating System and the tools that are already inherently native to the OS kernel. With no additional software installation, the Data Transfer Auditor seamlessly integrates with the underlying OS making it more cost-effective and less complex than standard add-ons in meeting the intents of USCYBERCOM requirements.

Our team is continuing to enhance and automate cybersecurity within the DoD and Cleared Defense Contractors and brings an enormous amount of creativity and technical skills to this environment. Data Transfer Auditor has widespread applicability for Cleared Defense Contractors, the DoD, and the federal government as a whole. Our SecureStrux team is well balanced among multiple disciplines and is integrated into the existing DoD security realm.

Our Data Transfer Auditor Insider Threat automated solution is just the first in many innovations being developed at SecureStrux to enhance our nation's cybersecurity posture against our global adversaries.

SECURESTRUX
Cyber Smart | Cyber Secure

703-682-6885 | securestrux.com
Arlington, VA & Lancaster, PA