User activity monitoring

In the field of information security, **user activity monitoring** (UAM) is the monitoring and recording of user actions. UAM captures user actions, including the use of applications, windows opened, system commands executed, checkboxes clicked, text entered/edited, URLs visited and nearly every other on-screen event to protect data by ensuring that employees and contractors are staying within their assigned tasks, and posing no risk to the organization.

User activity monitoring software can deliver video-like playback of user activity and process the videos into user activity logs that keep step-by-step records of user actions that can be searched and analyzed to investigate any out-of-scope activities.[1]

Contents

Issues

The need for UAM rose due to the increase in security incidents that directly or indirectly involve user credentials, exposing company information or sensitive files. In 2014, there were 761 data breaches in the United States, resulting in over 83 million exposed customer and employee records.[2] With 76% of these breaches resulting from weak or exploited user credentials, UAM has become a significant component of IT infrastructure.[3] The main populations of users that UAM aims to mitigate risks with are:

Contractors

Contractors are used in organizations to complete information technology operational tasks. Remote vendors that have access to company data are risks. Even with no malicious intent, an external user like a contractor is a major security liability.

Users

70% of regular business users admitted to having access to more data than necessary. Generalized accounts give regular business users access to classified company data.[4] This makes insider threats a reality for any business that uses generalized accounts.

IT users

Administrator accounts are heavily monitored due to the high-profile nature of their access. However, current log tools can generate "log fatigue" on these admin accounts. Log fatigue is the overwhelming sensation of trying to handle a vast amount of logs on an account as a result of too many user actions. Harmful user actions can easily be overlooked with thousands of user actions being compiled every day.

Overall risk

According to the Verizon Data Breach Incident Report, "The first step in protecting your data is in knowing where it is and who has access to it."[2] In today's IT environment, "there is a lack of oversight and control over how and who among employees has access to confidential, sensitive information." [5] This apparent gap is one of many factors that have resulted in a major number of security issues for companies.

Components

Most companies that use UAM usually separate the necessary aspects of UAM into three major components.

Visual forensics

Visual Forensics involves creating a visual summary of potentially hazardous user activity. Each user action is logged, and recorded. Once a user session is completed, UAM has created both a written record and a visual record, whether it be screen-captures or video of exactly what a user has done. This written record differs from that of a SIEM or logging tool, because it captures data at a user-level not at a system level – providing plain English logs rather than SysLogs (originally created for debugging purposes). These textual logs are paired with the corresponding screen-captures or video summaries. Using these corresponding logs and images, the visual forensics component of UAM allows for organizations to search for exact user actions in case of a security incident. In the case of a security threat, i.e. a data breach, Visual Forensics are used to show exactly what a user did, and everything leading up to the incident. Visual Forensics can also be used to provide evidence to any law enforcement that investigate the intrusion.

User activity alerting

User activity alerting serves the purpose of notifying whoever operates the UAM solution to a mishap or misstep concerning company information. Real-time alerting enables the console administrator to be notified the moment an error or intrusion occurs. Alerts are aggregated for each user to provide a user risk

profile and threat ranking. Alerting is customizable based on combinations of users, actions, time, location, and access method. Alerts can be triggered simply such as opening an application, or entering a certain keyword or web address. Alerts can also be customized based on user actions within an application, such as deleting or creating a user and executing specific commands.

User behavior analytics

User behavior analytics add an additional layer of protection that will help security professionals keep an eye on the weakest link in the chain. By monitoring user behavior, with the help of dedicated software that analyzes exactly what the user does during their session, security professionals can attach a risk factor to the specific users and/or groups, and immediately be alerted with a red flag warning when a high-risk user does something that can be interpreted as a high-risk action such as exporting confidential customer information, performing large database queries that are out of the scope of their role, accessing resources that they shouldn't be accessing and so forth.

Features

Capturing activity

UAM collects user data by recording activity by every user on applications, web pages and internal systems and databases. UAM spans all access levels and access strategies (RDP, SSH, Telnet, ICA, direct console login, etc.). Some UAM solutions pair with Citrix and VMware environments.

User activity logs

UAM solutions transcribe all documented activities into user activity logs. UAM logs match up with video-playbacks of concurrent actions. Some examples of items logged are names of applications run, titles of pages opened, URLs, text (typed, edited, copied/pasted), commands, and scripts.

Video-like playback

UAM uses screen-recording technology that captures individual user actions. Each video-like playback is saved and accompanied by a user activity log. Playbacks differ from traditional video playback to screen scraping, which is the compiling of sequential screen shots into a video-like replay. The user activity logs combined with the video-like playback provides a searchable summary of all user actions. This enables companies to not only read, but also view exactly what a particular user did on company systems.

Privacy

Some companies and employees raised issue with the user privacy aspect of UAM. They believe employees will resist the idea of having their actions monitored, even if it is being done for security purposes. In reality, most UAM strategies address these concerns.

While it is possible to monitor every single user action, the purpose of UAM systems is not to snoop on employee browsing history. UAM solutions use policy-based activity recording, which enables the console administrator to program exactly what is and isn't monitored.

Audit and compliance

Many regulations require a certain level of UAM while others only require logs of activity for audit purposes. UAM meets a variety of regulatory compliance requirements (HIPAA, ISO 27001, SOX, PCI etc....). UAM is typically implemented for the purpose of audits and compliance, to serve as a way for companies to make their audits easier and more efficient. An audit information request for information on user activity can be met with UAM. Unlike normal log or SIEM tools, UAM can help speed up an audit process by building the controls necessary to navigate an increasingly complex regulatory environment. The ability to replay user actions provides support for determining the impact on regulated information during security incident response.

Appliance vs. software

UAM has two deployment models. Appliance-based monitoring approaches that use dedicated hardware to conduct monitoring by looking at network traffic. Software-based monitoring approaches that use software agents installed on the nodes accessed by users.

More commonly, software requires the installation of an agent on systems (servers, desktops, VDI servers, terminal servers) across which users you want to monitor. These agents capture user activity and reports information back to a central console for storage and analysis. These solutions may be quickly deployed in a phased manner by targeting high-risk users and systems with sensitive information first, allowing the organization to get up and running quickly and expand to new user populations as the business requires.

References

1. "What is User Activity Monitoring Software?" (https://activtrak.com/user-activity-monitoring/). *ActivTrak*. 17 February 2019. Retrieved 5 March 2019.
2. "Data Breach Reports" (http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf) (PDF). *Identity Theft Resource Center*. 31 December 2014. Retrieved 19 January 2015.
3. "2014 Data Breach Investigation Report" (http://www.verizonenterprise.com/DBIR/2014/). *Verizon*. 14 April 2014. Retrieved 19 January 2015.
4. "Virtualisation: Exposing the Intangible Enterprise" (http://www.computerweekly.com/feature/EMA-announces-key-findings-from-virtualisation-report). *Enterprise Management Associates*. 14 August 2014. Retrieved 19 January 2015.
5. "Corporate Data: A Protected Asset or a Ticking Time Bomb?" (http://info.varonis.com/hs-fs/hub/142972/file-2194864500-pdf/ponemon-data-breach-study.pdf?&__hssc=&__hstc&hsCtaTracking=c771f50d-6a90-42c2-97d0-868ac3bcfc5b%7Cd2b8c2bf-07bc-4329-b1f9-c6ff2cd88980) (PDF). *Ponemon Institute*. December 2014. Retrieved 19 January 2015.