sectona

Solution Brief

Analýza hrozeb napříč privilegovanými aktivitami s využitím profilování rizik a behaviorální strategie s vysokou granularitou.

Technological evolution has led to many organizations adopting measures to meet the current industry standards of digitalization. With the sophistication of organizational assets and data, cyberattacks scrutinize the resources' security by adopting more modern and target approaches to penetrate the organization's defences and cause substantial economic losses. And with this, the security controls in line with compliance regulations also keep updating the outdated and inefficient practices, making it difficult for organizations to adapt on a continual scale to these standard rules, making them vulnerable to cyberattacks. Apart from this, any discrepancy/misuse of privileged access or negligence of detecting security event can lead to drastic consequences.

According to **Data Breach Investigations Report** by **Verizon**, 30% of the breaches involve internal actors, of which 8% of the breaches were misuse by authorized users. **IDG's Security Priorities Study** offered an insight stating that 66% of the respondents would be spending part of their budgets to adhere to compliance regulations; they felt that was a distraction from executing their strategic plans. Also Concerned are the respondents of the 2020 State of the **CIO study**, where 34% of them felt that security and risk management was the number one driver of their organization's overall IT spending.

Session Recording & Threat Analytics is an integrated Sectona PAM feature that ensures organizations' safeguarding by recording sessions for all the privileged sessions at different capacities for enhanced auditing purposes. This capability points to specific logs of a privileged activity in a session, then analyzes user actions from multiple data points, detects anomalies and malicious activities of critical Risk, and develops a mitigation strategy to strengthen the security paradigm of an organization.

Challenges

Incident Identification

Identifying the Security Incident which can happen due to many reasons can be difficult. With factors like unauthorized access or unusual user behaviour, the timeliness of the incident, which plays a significant role in assessing the Risk, goes unnoticed, making it susceptible to security risks, owing to the poor practices followed in an organization.

Insider Threat

Ill-equipped with practices to handle attacks from cybercriminals inherent to the organization, can wreak havoc to the Infrastructure. These attackers can be in the form of disgruntled employees, employees or vendors with standing privileges or employees who unknowingly perform unauthorized actions, potentially risking the organization's security.

Adherence to Compliance Regulations

Organizations are responsible for adhering to compliance regulations outlined in the standards specific to a region and industry. Although it is challenging to comply with stable laws and regulations, the compliance standards keep updating their compliance requirements with the rising threat surface, making it more difficult for organizations to maintain and constantly adhere to these security controls.

Use-cases

- **Session Recording**
  Sectona Security Platform's Session Recording and Threat Analytics facilitate recording activities for different sessions at various capacities giving an auditor a granular overview of the user's actions, with search capabilities that include finding activities by a user, asset, or privileged account. It supports recording the sessions in a video format in RDP, SSH-Based Sessions in Over-Browser and Launcher-Based Interfaces to Telnet, Browser (URL-Based), Thick-Client Based in Launcher- based and RDP Client/Browser-Based Session in Jump Server Based Interface. Session Recordings provide a detailed overview of the log with an option of filtering activities based on the timeframe, source IP, and session launch types. Sectona PAM has four components falling under the Session Recording module defined as follows:

  - **Live View**
    Facilitates live monitoring of a session in real-time while also monitoring command inputs and the source details and terminating a session if there is unusual activity

  - **Session View**
    Comprises the consolidated list of all the access and log entries to the target servers and devices.

  - **Risk View**
    Facilitates activity logs based on Risk-Based Filtering, which provides a list of Top 10 High RiskLogs entries by Asset and User accordingly, which assists auditors in prioritizing review of the entries.

  - **Activity View**
    Comprising a list of activity logs segregated by a filter option of Asset Category and Asset Type.

- **Risk Scoring**
  Risk Scoring is a standard process that detects and reviews suspicious activities with Intelligent Threat Analytics, exploring and analyzing anomalies based on user behaviour. The user activities in each Session are analyzed, and the risk factor associated with each one of them is calculated based on 27 different events. These events falling under categories like Identity Theft, Unusual Account Activity, Privileged Account Abuse, Leapfrogging, and Data Theft and Exfiltration have four adjustable configuration values from low to high, depicting the critical nature of the activity. This process helps us identify, prioritize incidents, and develop a risk mitigation strategy to tackle any anomalies.

- **Immutable Administrable Logs**
  The Recorded activity logs of the privileged sessions are available only to an administrator and an auditor, receiving access when he intends to review specific log entries for auditing purposes. With the scope of protecting the integrity of these Log Entries, they are encrypted and stored in an Immutable Storage that employs practices to prevent the tampering of log entries.

- **Enforced Session Review**
  All the Session Recording entries have a System Trail embedded feature that presents a detailed overview of a Target Asset activity. When an auditor wants to analyze a session activity in detail to comply with confidence, the designated access to the log entries allows them to enforce session review. Reviewers can delegate incident analysis to another auditor or incident manager to confirm the review through the re-review feature, ensuring thorough scrutiny.

The key benefits

Granular Visibility
Log all the privileged activities, facilitating a detailed overview through Session History Log and the Session Recordings, simplifying compliance and incident response.

Reinforced Governance
Real-Time Monitoring of all the activities while recording all the privileged sessions for enhanced auditing purposes.

Enforcing Risk Assessment
Analyze the privileged sessions, asses the associating Risk based on the user behaviour, and if critical, prioritize the review and act on it with a mitigation strategy.

Exploring Sectona PAM's Capability of Session Recording & Threat Analytics

Sectona Privileged Access Management Solution provides the inbuilt capability of Session Recording & Threat Analytics, facilitating administrative control over a privileged user's activities and trails throughout a session. Protecting access to the organization's resources and sensitive data is of utmost importance. With Advanced session recording capabilities for all privileged activities with risk-profiling & behaviour-based analytics, the activities are prioritized and dealt with, mitigating any mishaps.

Features

Contextual Capturing
Recording all the activities performed in a session by a privileged user for RDP, SSH, thick clients, web, and cloud consoles at different capacities in video and command/text formats.

Intelligent Risk Scoring
Analyze the Risk associated with each Session by profiling user behaviour based on a pre-packaged library of high-risk events and determine a score and risk level associated with each Session.

Simplified Auditing
To ensure compliance with confidence, the administrators can review the logs or enable re-review by delegating it to auditors or incident managers and getting the sessions audited

Storing the Logs
Independent of the device logs, the session logs are encrypted and stored in a designated Tamper proof Log Storage.

Playback Speed
For ease of use, auditors have the facility of viewing the recordings of enormous length at a faster speed of up to 32x speed or granular and detailed analysis of an event at up to 0.5x speed.

Filtering Metadata
The Session Recordings have a search filter, enabling them to search for specific metadata/ command inputs and pinpoint the specific time in the recording to its execution.

Session Search Capabilities
Allowing you to find activities using user, asset, privileged account, source IP, timeframe, and session launch types.

Session Collaboration
Share a Live session can with another user through a link, accessible under the Live tab, which moves to Session Tab after the Session terminates.

sectona

Sectona se zabývá správou privilegovaného přístupu a pomáhá firmám snižovat riziko cílených útoků na privilegované účty v datových centrech a cloudu. Sectona dodává integrované komponenty pro správu oprávnění pro zabezpečení dynamického přístupu vzdálených pracovníků, napříč lokálními nebo cloudovými pracovišti, koncovými body a komunikací mezi zařízeními.

Pro více informací navštivte www.sectona.cz