Privileged Access Management Processes and Procedures

Anonemis Research
Simenona Martinez
AnonemisResearch.com

Privileged Access Management Processes and Procedures

PAM is a more in depth version of IAM, they work together in a enterprise environment. Concerning IAM, identity references persons, which in this case must be maintained, monitored and verified. PAM is broadening umbrella in the sense where it manages various types of privileged accounts, where as IAM is more specific.

PAM currently has a large amount of dormant and unaccounted privileged accounts which require managing. This can be mitigated through incorporating A.I. operated machine management.

Including features which consistently update and mange complexities within passwords, repurposing accounts, monitoring those accounts on a separate cyber-security interface which would notify the I.T. administrator of in abnormalities, indicating a breach whether internally or externally. The I.T staff can easily manage and monitor these accounts which would ultimately eradicate cyber-attacks to a certain extent within enterprise.

This would also include automatically disabling inactive accounts by removing them from the queue and rendering the inaccessible, with only retaining records. When accounts become utilized less that alerts the management team and that account is then added to queue in that category to be monitored and effectively disabled.

Default accounts or otherwise will all be accounted for and therefore managed. This software operates on a different server to avoid breaches and to further afford security measures. These accounts are higher risk for breaches and need to be maintained, accounted for, monitored and deactivated effectively.

This all can be achieved with software used for primary management but in this case, applied to the management of privileged accounts for managing and flagging for abnormal behaviors for review. This is essential for early detection and preventive measures.

The monitoring of abnormal behavioral sequences is important, particularly in the cases of Man in the Middle attacks. If the privileged account is acting in different sequences, which is cause for alarm, regardless of if it is managed by a human or non-human entity, it can be detected with efficiency, isolated and mitigated effectively.

In even the instances of Hide and Observe tactics, managing these accounts and their access controls more efficiently reneges any vehicle for the those attackers to learn. You can’t learn what you cannot access.

This would include the system constantly monitoring the geographical locations of all accounts when they access certain elements within the system to observe; folders, files, documents, and downloads.

Monitoring the keystrokes. Considering the time, date and length of view-time is also critical. It’s about knowing what these accounts are viewing and in what sequence. This can be helpful in combating various types of attacks.

Behavioral trafficking analysis is also effective in employee impersonation instances and constantly reconfirming the identity of the user access on all accounts at all times is critical. Having software which manages these accounts makes that requirement achievable.

Protecting critical data is key, and that can be achieved by early detection of a breach. Installing the proper use of firewalls, effective monitoring, consistent anti-virus configurations, intrusion detection, access controls management, and overall encryption is essential in this process. Again, passwords can and should be change frequently.

This is essential the foundational blueprint to your organization, and it is the projected capabilities, the groundwork so to speak. This is the most important practice, and this concept of awareness should always be at the forefront of any operation; tactical consideration or planning.

It crucial in terms of consideration, which is essentially an extension of the previous statement. It is setting the basis and boundaries of an operation, which takes heavy planning and accountability.

Critical operational tactic and precision of execution is non-negotiable. This requires forethought and planning but there’s little room for trial and error in these ever-changing parameters.

Response is everything in cyber-security, it is the defense and offense in the realm of real life, which is no game.

Anonemis Research
Simenona Martinez
AnonemisResearch.com