CalCom

Domain Controller Hardening Automation

DOMAIN CONTROLLER HARDENING CHALLENGES

Active Directory (AD) requires a special approach to protecting it since it holds the "keys to the kingdom" of the IT infrastructure. Domain Controllers (DC's) which are serving as the infrastructure layer for Active Directory are a critical attack vector. Enforcing robust security baselines for DC's is an essential security task, yet, the operational sensitivity of this infrastructure carries significant challenges. Hardening the DC's is time-consuming, costly and has an operational impact that can be devastating. Long hours are spent testing target policies in a lab environment before promoting them to production. Unfortunately, even the best lab environments fail to fully simulate production server activity. It is impossible, through testing alone, to ensure that production will not be impacted by hardening efforts. Due to limited testing resources, and out of concern for production stability, organizations rarely harden more than a small subset of recommended configuration settings – this is a detriment of the organization's compliance and security posture. Once implemented, maintaining hardened settings is an upstream battle. Multiple privileged users in an enterprise environment all but guarantee configuration drift, requiring additional work to determine gaps, re-establish baseline standards, and ensure audit readiness.

BOOST COMPLIANCE WITH CHS AUTOMATED HARDENING

CalCom Hardening Suite (CHS) is a solution for automating and managing server configuration hardening. CHS offers the unique ability to 'Learn' where desired hardening changes will adversely impact production activity. CHS determines the impact of baseline changes before they're implemented, and in doing so prevents outages. CHS eliminates time consuming testing, dramatically improves compliance posture, and reduces the cost and impact of hardening.

LEARNING MODE

Simulates the policy impact on production

ENFORCEMENT MODE

Custom server hardening mode

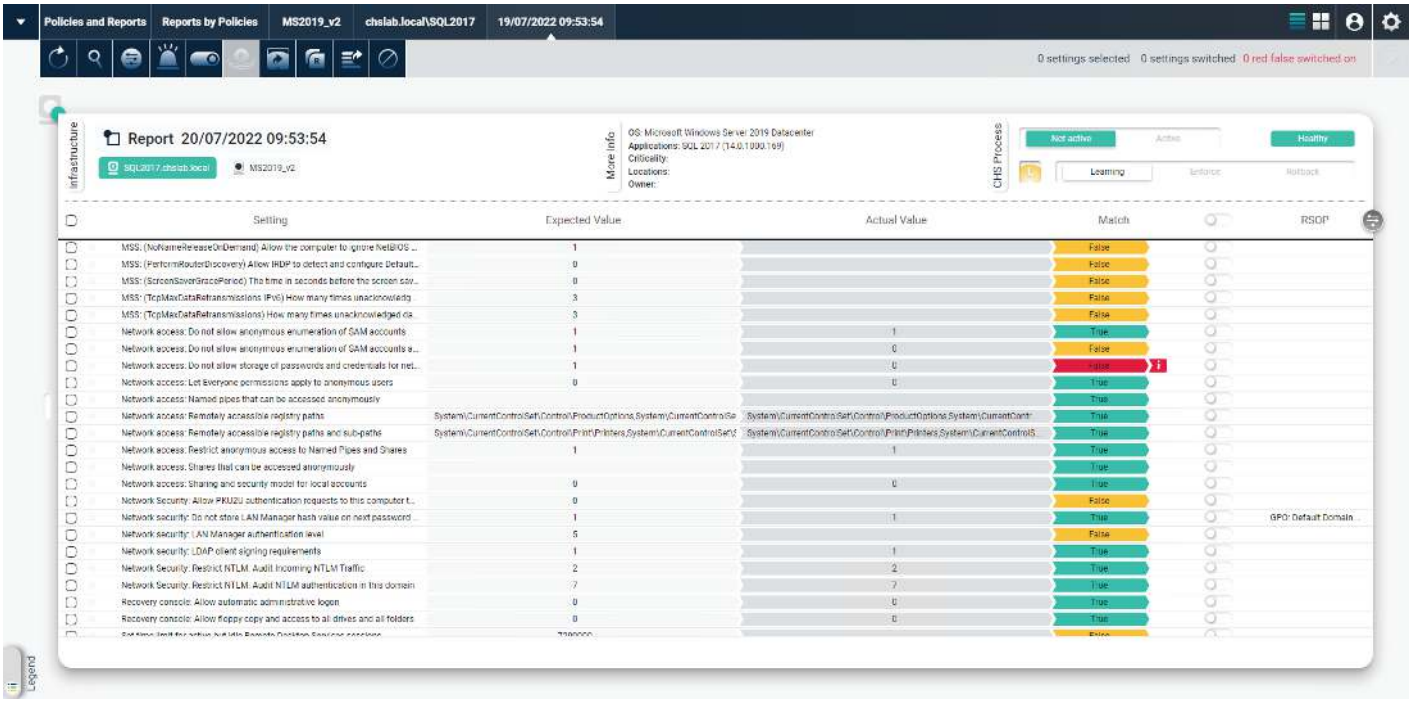
MONITORING MODE

Real time access control protection

rollback

The CHS Automated Hardening Solution implements an on-going automated approach that dramatically improves the breadth of baseline coverage with respect to hardening standards, while reducing time and money spent. Only CHS eliminates the need to manually test baseline changes prior to promotion, effectively automating the very expensive and time-consuming test process. How does CHS do this? For each server in your environment, CHS's proprietary 'Learning' mode observes production activity over time with respect to the desired policy. CHS automatically builds an understanding of production activity that will be impacted or broken by a proposed configuration change – without manual testing. From this understanding, CHS builds, deploys and enforces the optimal 'non-impactful' policy for each server in the enterprise!

THE CHS POLICY CENTER



1. Expected Value

Displays the desired policy value

2. Active Value

Determines the object's current status shows its "actual values"

3. Match/Impact Indication

True: The expected values and actual values are identical

False: The value will be changed when enforcing the policy – with no impact on server operation

False: The object is used by the production system and the actual value is valid, therefore, hardening the policy will cause damage to servers in production

The above Impact Analysis Report is generated by CHS at the end of the learning period. This report projects the impact of the target policy on production activity. The desired value for each object to be hardened is shown in the "Expected Value" column. Actual values observed during Learning Mode are shown in the "Actual Value" column. Finally, the projected impact on production of hardening per the target policy is shown in the "Match" column. From this Gap Analysis report, the optimal "ready-to-go" promotion plan is generated for each server, one that maximizes policy compliance while avoiding impact to production.

THE CHS POLICY ANALYSIS CENTER

The CHS Policy Analysis Center presents each server's compliance and risk posture. The Policy Analysis Center helps IT management prioritize baseline hardening tasks, and assists in documenting and managing unhardened objects as "exceptions" in support of audit requirements.