ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (21-22), Month: October - December 2020, Available at: www.researchpublish.com

Security Configuration Management Process, Implementation and Integration

Ziad Alomair, Mohammed Alfraih

Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **This paper will explore the overall concept of security configuration management, its implementation and integration with the change management process. Furthermore, the paper explains the security configuration management life cycle and why it matters. The paper provides an approach to detect and mitigate future risks if proper methods and tools are used. Furthermore, this paper proposes an approach to utilize existing inventories to detect unauthorized changes captured by security configuration management monitoring tools.**

Keywords: **Baseline, SCM, Security Configuration Management, NIST, CIS.**

Security Configuration Management (SCM) is considered one of the top 10 controls in major cybersecurity frameworks, such as National Institute of Standards and Technology (NIST). The main goal of security configuration management is to enable security through consistently checking for any deviations to a known state of an information system. This approach is crucial to manage risks and fix any misconfiguration or default configuration across information systems. In addition, security configuration helps organizations to detect and mitigate any future hacks due to default configuration. SCM identifies misconfigurations that make systems vulnerable, and also identify changes to critical files or operating systems keys.

SCM relies on a gold standard configuration. By setting a gold standard configuration for systems, and continuously monitoring for signs of compromise, a breach is identified quicker and an incident response is triggered faster. Then the cybersecurity personnel team have the leverage to be in control of the risk at an early stage. Early prevention of internal or external threats helps to mitigate the damage of a cyber-security breach. The gold standard configuration is a known baseline or known system status that can have either a hardening standard — the Center for Internet Security (CIS) and NIST — or vendor security best practice. It should be a general rule in organizations to have a dedicated baseline for every critical system that resides on their network.

Organizations with large infrastructure should invest in having a bare minimum of security controls to be applied to most applications that have no known reference, by either security frameworks or vendor recommended security controls. When a new system is received, it is a requirement to establish a baseline. A baseline submitter must start with benchmarks from trusted establishments like CIS or NIST for guidance on how devices should be configured.

The baseline is then reviewed by the SCM team and other related security entities, such as accounts management, log management, etc., to assess the baseline. Once the baseline is fully reviewed and the system is in a production status, a compliance assessment is carried out to verify that all security controls mentioned in the baseline are compliant. If any misconfiguration is found, then it is reported and escalated to the system owner to remediate any findings. This practice should continue to control the risk of running critical applications on the network.

The SCM process can be overwhelming if the right tools are not at your disposal. With the right tools and expertise, the bulk of the work is handled through automation. The SCM team can search the market for tools that are compatible with their infrastructure. The tool must have enhanced reporting capabilities, ease of automation, and APIs to integrate with the event log management system and threat analysis management systems. This can assist the incident response team to develop threat cases to be triggered, if for example a certain line configuration is changed without an approved change

request. Automation can be possible if the SCM tool has an approach to view system configuration. This can be accomplished by either having a software agent deployed across information systems or agentless approach such as accessing information system through known secure ports/protocols, such as SSH.

SCM can also be integrated with the change management process. If organizations have a central inventory for all assets and the inventory is integrated with a proper change management application. API calls from the SCM application is then utilized to detect any changes that have no approved change request. For example, if a change is detected by an SCM tool, an API call with an asset ID is then sent to a change management tool, to verify if there is an approved change request related to this asset ID. If not, cybersecurity personnel are notified to start an investigation. This process is only possible if the security configuration team have visibility over system configurations.

In conclusion, it is vital to ensure that defensive security controls are in place to assist security personnel to be in control of organizations' networks. Therefore, it is recommended for organizations to adopt technologies that help protect business and ensure compliance to defined baselines.

REFERENCES

[1] Brian JacksonFollow @infosecNW!function(d, S. (2018, September 05). Why Security Configuration Management (SCM) Matters. Retrieved October 14, 2020, from https://www.tripwire.com/state-of-security/security-data-protection/security-configuration-management/why-security-configuration-management-matters/

[2] BUCHANAN, I. A. N. (n.d.). Configuration management: definition and benefits. Atlassian. https://www.atlassian.com/continuous-delivery/principles/configuration-management

[3] Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2011). Guide for Security-Focused Configuration Management of Information Systems [E-book]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf