CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

Special Report:

Warning Signs for Managing Cyber Security

JUNE 2018

MORE INSIDE!

WARNING SIGNS FOR MANAGING CYBER SECURITY

In 1997, the NSA attacked the Department of Defense information infrastructures and attempted to breach their network. The attack was codenamed Operation Eligible Receiver 97 and was intended to test the defense capabilities of the DoD against a cyber attack. Results from the exercise were alarming. The NSA took complete control over many of the Department of Defense information infrastructures and gained superuser access to critical systems. The exercise highlighted the unorganized and poorly governed computer infrastructures of the DoD and armed forces.

After two years of hearings and review, three recommendations were made; recommendations that cybersecurity professionals are well aware of today. These are Configuration Management, Patching Vulnerabilities, and the implementation of Controls. Though best practices were not formally codified, compliance frameworks were developed and these may be reviewed. They are Security Technical Implementation Guides (STIGs), the National Vulnerability Database (NVD), and the controls within NIST 800-53. Surprisingly, while the recommendations were made over twenty years ago, many organizations still struggle with implementing them today.

All professionals know benchmarks and accountability are a hallmark of good management. A project may not proceed until the target is formally described, processes are implemented, and milestones are validated. Unfortunately, for many professionals in the cybersecurity field, the tools and process have been developed over the years in a hodgepodge manner.

Certain beliefs and procedures are implemented because “that’s how it has always been done.” There are even occasions when milestones are merely guesses. For example, how many times have you heard the question, “What percentage of CVEs do we have patched?”, answered with, “Probably 75%.” This inability to provide consistent or accurate data creates an unmanageable cybersecurity process.

THE DEVIL IS IN THE DETAILS

While all plans start out logical, over time the complexity of implementation, requirement of changes, and opinions of others can introduce problems. This article describes a technique used by managers to notice warning signs and determine if there is a problem with their cybersecurity processes. By reviewing the metrics they receive, managers can determine the health of their group. Likewise, inconsistencies in the security metrics may be used to justify reviews or upgrades to tools and training for parts of the process. What is needed to find the warning signs? What every manager looks for: reliable, consistent, and usable data (RCU).

Reliability ensures security teams are utilizing real data. Organizations operating without real data often misunderstand their current security posture or rely on guesses. For example, an understanding of vulnerabilities can only be accomplished when there is an understanding of asset inventory and IP leases. Many organizations use DHCP servers to discover these IP leases, but this number will vary over time and is inaccurate. If a manager learns developing reliable data by his team member is difficult, they know an underlining tool or process is incomplete. With a focus on reliability, the security process becomes based on reality.

Consistent data ensures security professionals are able to view data, return at a later date, and analyze the same data. More importantly, it allows different members of the team to get the same results. If a manager determines security metrics are inconsistent, they know there is an issue with the organization and retention of data by the team. Maintaining a detailed history of changes is crucial for an accurate security ledger detailing what security risks an organization has, what procedures are in place, and ultimately reporting to the board.

Usability allows data to be used in different ways. This is the measure of the flexibility that a security team has in determining problems, forensically exploring issues, and developing a novel and unique procedure. If a manager suspects the metrics developed by their team are silo-ed, or limited in scope, they know there is an issue with team members being too regimental in their performance.

Access to actionable items that apply to multiple security functions differentiates organizations from an inefficiency where time is being spent searching through data instead of being used to remediate issues. For example, when looking at configurations, usable data clearly shows when drift has occurred along with who caused it. This allows security teams to efficiently discover who was responsible for changes and what the reasoning was. Linking data from behavioral information into usable metrics for security functions, such as configuration management, helps organizations manage cybersecurity.

THE RED FLAG OF POLICIES

Organizations will often attempt to manage cybersecurity with specific policies. These policies will cover various IT functions such as USB usage or local admin rights. Unfortunately, these policies can take on a life of their own and specific answers to the compliance of policies will be met with statements such as “We’ll have to ask IT” or “ We won't know until the next audit.”

When following the principles of RCU, answers to the coverage of policies will be nearly instantaneous. The continuous checks provided by RCU determine if specific policies are utilized rather than simply existing. A manager can quickly tell their organization is at risk if their team is more focused on whether the policy is being followed rather than if there is a policy in place.

Reliable, consistent, and usable data is important for the security process as a whole. For example, conducting an audit every six months does not follow the principles of RCU. In order to be reliable and consistent, data needs to be analyzed continuously. Security events that occurred six months ago will not be relevant or usable for security professionals. When organizations have reliable, consistent, and usable data to manage security processes, their processes become more efficient and robust.

As an example of utilizing the reliability, consistency, and usability principle to configuration management, organizations have immediate answers to questions such as:

- How are devices configured?
- How are they supposed to be configured?
- Who made changes and when did they make them?

The answers to these questions provide valuable information for not only configuration management, but for all security functions.

The recommendations from Eligible Receiver 97 are critical to any organization's security posture, but there is far more to consider before implementing a process.

The processes implemented must provide reliable, consistent and usable data so a robust and dynamic security team is supported. Managers watching for simple indicators can determine if their group is working in a productive manner.

Utilizing the revolutionary UDAPE® technology, AristotleInsight collects reliable data from the process level across all devices on an organization's network. A unique Bayesian Inference Engine sorts through the kernel level data to highlight actionable items that help security teams identify risk, direct the remediation process, and document results. This helps security teams save time and better manage their cybersecurity posture.

If an organization is building their security process, AristotleInsight is the perfect solution to collect data that is reliable, consistent, and usable. For organizations with a mature cybersecurity process in place, AristotleInsight is an effective hunt tool.

To learn more about AristotleInsight: Visit - www.aristotleinsight.com

Email - info@provecompliance.com Call - 866-748-5227