VITAL CYBER
Provided by MCNC

Blog Series- Cybersecurity 101: Securing Your Digital Environment

Episode 3: Software Asset Management

Question about a term?
Visit our Glossary

In episode three of our blog series, "Cybersecurity 101: Securing Your Digital Environment," we highlight an often overlooked area of cybersecurity—Software Asset Management (SAM), one of the three foundational topics of your cybersecurity program. The other two? Enterprise Asset Management (EAM), which we discussed in Episode Two, and Data Management (DM), the topic of Episode Four.

Like Enterprise Asset Management (EAM), SAM is essential for enhancing your cybersecurity posture. Neglecting SAM can leave your organization vulnerable to unauthorized applications, unaddressed software vulnerabilities, and potentially harmful software. Therefore, understanding and implementing effective SAM is foundational to building a solid cybersecurity program.

What's Software Asset Management?

What do we mean by SAM? If you remember from the last episode, we defined an asset as anything useful or valuable to your organization. When we're talking about software, this would include operating systems, applications, libraries, and scripts. Whether it's a cloud-based service, an app installed locally, or an API tool, all of these are part of your software environment.

A solid SAM process helps you manage the entire software lifecycle—procurement, installation, usage, updates, and removal of software. But SAM isn't just about tracking what's installed on your systems. It's about capturing and maintaining the metadata of your software over time, such as who the software owner is, the vendor responsible for maintaining the software, contact information, versions present in your environment, and support status.

An example in the not-to-distant past when this information was worth its weight in gold was after the disclosure of the log4j vulnerabilities in December 2021. Since this was a product embedded in many applications, it was a heavy lift to identify affected applications without the aid of SAM to provide a clear starting point of what software was present in your environment.

The Framework

Before you begin building out the SAM process, review what safeguards in the CIS version 8.1 framework should be addressed.

- **Basic Cyber Hygiene (IG1).**
    - (CIS 2.1) Establish and Maintain a Software Inventory
    - (CIS 2.2) Ensure Authorized Software is Currently Supported
    - (CIS 2.3) Address Unauthorized Software

- **Additional Safeguards (IG2).**
    - (CIS 2.4) Utilize Automated Software Inventory Tools
    - (CIS 2.5) Allowlist Authorized Software
    - (CIS 2.6) Allowlist Authorized Libraries

Where To Start?

To kick off your SAM process, start by setting clear administrative controls outlining the basic cyber hygiene safeguards and any additional ones needed to protect your organization.

- **Policy.** The first step is developing a SAM policy that clearly defines who oversees the process, handles the daily management of software assets, and what actions should be taken during each software lifecycle phase. Establishing these guidelines ensures consistency and organization in how software is managed across your organization. To kickstart your SAM process, we have a template that covers the essentials.
- **Standards and Procedures.** Standards and procedures are the next step in establishing an effective EAM process. Together, they translate the policy into day-to-day operations, offering a clear roadmap for everyone involved in managing enterprise assets. Here are standards and procedure templates with the essentials you can use as a starting point.

Where Do We Go From Here?

Now that you've established your administrative controls, it's time to implement them by documenting and managing your software assets throughout their entire lifecycle.

Create an Up-to-Date Software Inventory.

With a comprehensive inventory, it's easier to secure your environment. Start by compiling a detailed inventory of all software currently in use. You can automate this process with specialized tools or manually create a spreadsheet. If you're opting for the latter, here's a template to help you categorize your software assets effectively.

Manage Software Through Its Lifecycle.

Managing software effectively involves following established policies and procedures throughout its entire lifecycle. This includes:

- **Procurement.** Evaluate and select software vendors to ensure new software aligns with your organization's security standards and operational needs. After procurement, promptly add the new software to your inventory.
- **Installation.** Ensure software installation follows approved procedures on enterprise-owned or authorized devices. Keep track of all installations and update your inventory accordingly.
- **Upgrade.** Regularly update and upgrade your software to keep it secure and functional. Track these upgrades in your inventory to ensure all versions are up-to-date and authorized.
- **Usage.** Include software in your organizational Acceptable Use Policy (AUP) and clearly define how software is used within the organization. Make sure all users understand and agree to these guidelines. If you don't have a policy, here's a template to help you create one.
- **Discovery.** Identify any software within your organization that may not be listed in your inventory by regularly scanning the environment. Add authorized software to your inventory, and promptly address unauthorized software.
- **Removal.** When software is no longer needed or reaches the end of its lifecycle, ensure it is properly removed from your systems. This step is critical to prevent unauthorized access or data breaches. Update your inventory to reflect the removal.

Where We're At!
Building upon the Cybersecurity Framework in episode one, here is a visualization of the progress made to this point in the series. We recommend you copy this sheet or create your own to visualize your progress.

Take the Next Step in Strengthening Your Cybersecurity
Is your organization ready to enhance its cybersecurity posture? Our team of experts at MCNC is here to help. Whether you need a comprehensive risk assessment, policy analysis, or guidance on implementing best practices, we're ready to partner with you to safeguard your digital assets.

Don't wait until it's too late. Contact us today to schedule a consultation and discover how MCNC's Vital Cyber solutions can protect your institution. Fill out our Contact Us form and let's start building a stronger defense together.

Data Management
Secure Configuration
Account and Credential Management
Network Management
Vulnerability Management
Audit Log Management
Malware Defense
Data Recovery
Security Awareness Training
Service Provider Management
Incident Response Plan