The Intersection of SAM and Cybersecurity

INTRODUCTION

SAM and Cybersecurity Work Best Collaboratively

Risk is a hot topic, especially when security is top of mind for corporations. While this has been the case for a long time, what this means to a business can be murky. This article will work to define both Software Asset Management (SAM) and Cybersecurity (CS), the importance of both in an organization, and the relationship between the two. Software Asset Management practitioners work with every team in an organization, whether directly or indirectly. There are teams that are more closely related than others, in this example, the Cybersecurity team. While this will cover topics that both teams can do, the purpose is really for SAM and CS practitioners to increase communication and improve data sharing. If this relationship is built up, it can be optimized so time and money are not wasted on tasks being done multiple times.

What is Cybersecurity?

Cybersecurity is the application of technology, processes, and controls to protect computer systems and networks from attacks that could lead to a data breach and unauthorized information disclosure; theft of or damage to hardware, software, or data; and the disruption or misdirection of the services provided. A data breach is a security violation in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so. Cybersecurity teams will not be able to negate the risk of a breach entirely. However, there are several recommendations to limit significant risk.

What is Software Asset Management?

Software Asset Management is the practice of managing the purchase, deployment, maintenance, utilization, and disposal of software applications within an organization. Practically, this looks like negotiating software contracts, managing renewals, overseeing departments' software usage, monitoring increases or decreases, and more. An important piece of SAM is the humility to know the limits of what your team can accomplish – by clearly defining the SAM team's role in the organization, it becomes easier to communicate with other teams and see how they can improve your workflow and vice versa.

Where Do CS and SAM Overlap?

We can view Cybersecurity, in part, as the stopping of unauthorized access to data and devices. For example, an organization could use CS to monitor account access and passwords, and SAM to review software updates and device inventory. Or, on the front end, SAM answers questions like:

Do the programs being onboarded meet the organization's security requirements?

How many units are being purchased?

Who will have access?

This work can be done by SAM and shared with CS to accomplish the overall mission of the organization, like balancing bringing in tools to help employees do their jobs within an acceptable amount of risk. As stated above, it can sound like these two teams are doing the same task. While this paper is to examine the relationship between the two teams, it is important to note that the purpose of this relationship is to optimize the organization so the same task does not need to be done twice.

How Can CS and SAM Work Together?

A Mature ITAM/SAM program is a data provider to Cybersecurity. This means the SAM team is providing clean, accurate, regularly updated, and, most importantly, complete data to the Cybersecurity team. It is important to recognize that a mature SAM program is a data provider to the whole organization – SAM should not only be requesting information from CS, Operations, HR, Finance, etc., without reviewing, cleaning, and providing complete information back to these teams, as needed. When an organization has one set of complete, trustworthy data that all teams are working from, risk is well managed and costs are optimized. While this is focusing on CS and SAM, every department should be in direct contact with both CS and SAM for various reasons. Human Resources will use CS measures for account management and incident response. Finance will use CS for risk management and data integrity. They will both use SAM for software purchases and license compliance. This is a limited view but a good look at how departments are all interconnected and direct, open communication benefits all in an organization.

Cementing the Relationship Between SAM, CS, and Cyber Hygiene Best Practices

The full list of all 18 recommended Critical Security Controls are publicly available via the Center for Internet Security (CIS). CIS is a non-profit group responsible for creating and evolving controls and standards to provide safeguards against known and new threats. This group was formed in 2000 by business and government leaders concerned with not knowing how and what to implement in cybersecurity practices. CIS is currently on version eight of its list of controls, according to current best practices designed by private enterprises and government research. Their top five controls, which they call Cyber Hygiene, really fall under what SAM does, even though they are specific to Cybersecurity. Below is a breakdown of the five CIS controls. By implementing these five controls, an organization can mitigate up to 80% risk of breach.

CIS CONTROL 1
Inventory and Control of Enterprise (Hardware) Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

CIS CONTROL 2
Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

CIS CONTROL 3
Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

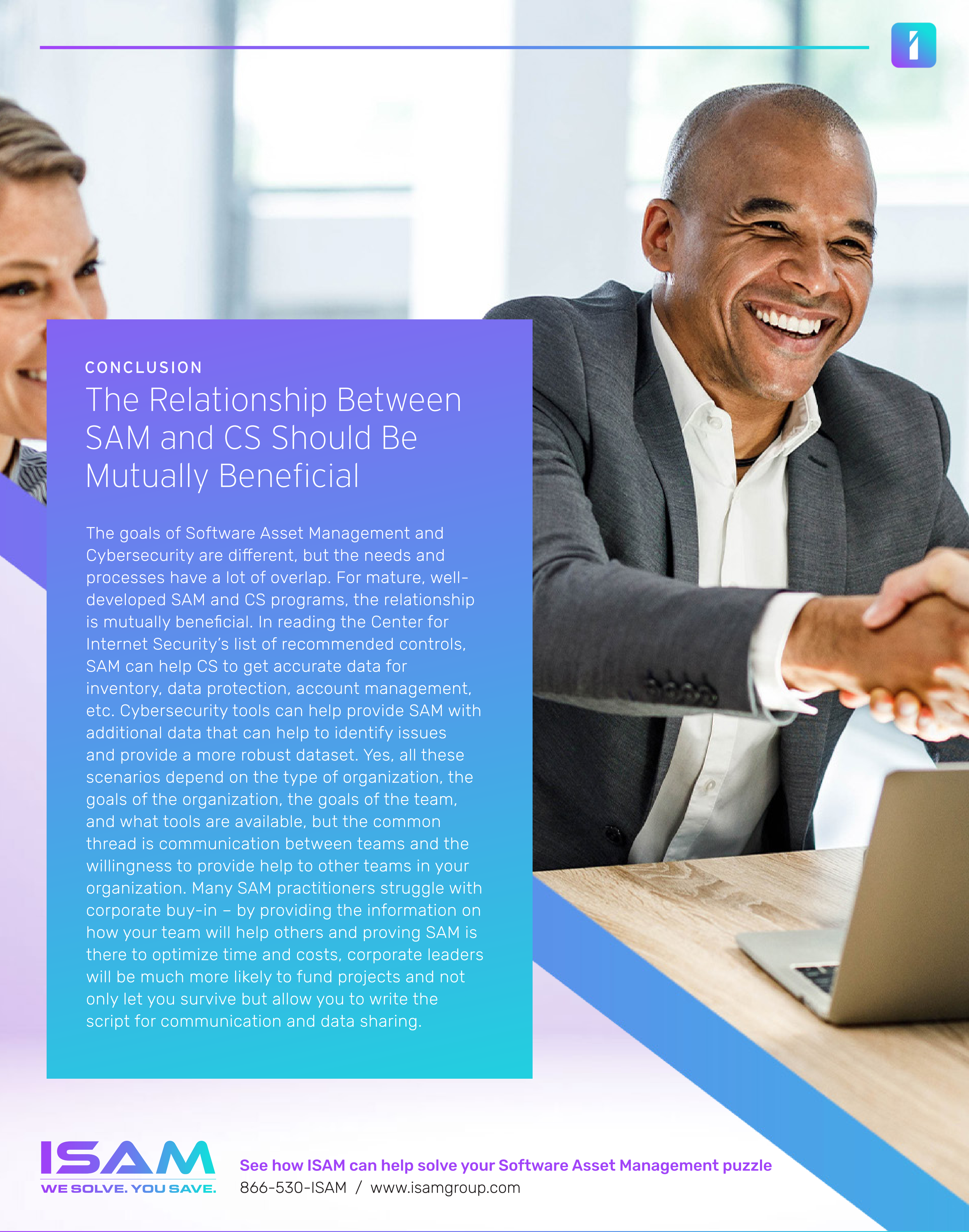
CIS CONTROL 4
Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

CIS CONTROL 5
Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator and service accounts, to enterprise assets and software.

Inventory management, Data Lifecycle Management, on-prem and remote-based secure configuration of Hardware and Software, and account management are all staples of the Software Asset Management strategy.



CONCLUSION

The Relationship Between SAM and CS Should Be Mutually Beneficial

The goals of Software Asset Management and Cybersecurity are different, but the needs and processes have a lot of overlap. For mature, well-developed SAM and CS programs, the relationship is mutually beneficial. In reading the Center for Internet Security's list of recommended controls, SAM can help CS to get accurate data for inventory, data protection, account management, etc. Cybersecurity tools can help provide SAM with additional data that can help to identify issues and provide a more robust dataset. Yes, all these scenarios depend on the type of organization, the goals of the organization, the goals of the team, and what tools are available, but the common thread is communication between teams and the willingness to provide help to other teams in your organization. Many SAM practitioners struggle with corporate buy-in – by providing the information on how your team will help others and proving SAM is there to optimize time and costs, corporate leaders will be much more likely to fund projects and not only let you survive but allow you to write the script for communication and data sharing.