GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Curcurto, Sam

"Asset Management for the Digital Age"

Darkreading.com

informa tech Technology Group

18 March 2019

URL: https://www.darkreading.com/vulnerabilities---threats/asset-management-for-the-digital-age/d/d-id/1334177
Accessed: 31 May 2019

Synopsis: For today's security challenges, organizations need a global perspective to ensure their IT and security operations teams have an accurate, up-to-date inventory.

Asset Management for the Digital Age

For today's security challenges, organizations need a global perspective to ensure their IT and security operations teams have an accurate, up-to-date inventory.

The foundation of any robust security program is a complete understanding of everything that needs to be protected. This is validated by nearly every security framework, including NIST or the CIS controls. They all begin with one thing: the necessity of maintaining an accurate inventory of assets.

Unfortunately, the decentralization of information technology systems has cracked this foundation, because there is no central point through which all assets flow in order to accurately inventory and track what must be protected. As a result, the rest of your security programs are built on incomplete or incorrect data, likely inherited from past generations of security or asset management staffs. People come and go. Assets are procured and decommissioned. Mergers, acquisitions, and divestitures happen. All of these changes result in gaps in accuracy and completeness.

Which brings us to the ultimate question: How confident are you in the asset list that you're operating from? The answer stems from how (or if) your team continuously manages your IT and Internet-connected assets.

Assets Are born. Or made. Or bought.

In a perfect world, when new assets are purchased they flow through a central IT department where they are recorded, tagged, and tracked through their useful lives. But this isn't a perfect world.

Many IT organizations are still operating off the same asset spreadsheet–or, worse, multiple spreadsheets–started a long, long time ago. Even if you have an asset management system, chances are, data about your assets is not complete or centralized in one system. Additionally, because of disparate information between systems, they require heavy manual overhead to maintain and update, and they don't take advantage of modern technologies that exist to track their existence in near-real-time. An additional challenge is that new types of assets, like domains and certificates, are not types of assets that can even be tracked using some of the old technology.

Decentralized IT and purchasing mean that anyone with a credit card and an email address can create a cloud account and deploy a server, software, and infrastructure without ever having to speak to anyone in IT.

Similarly, commissioning assets that flowed through a central point allowed IT and security to configure and set up systems and ensured that the correct software was deployed and appropriate security policies were applied before the asset entered service. IT operations teams knew what the asset did, who was responsible for it, what was on it, and where it was.

Under the decentralized model, IT and security operations teams rely on the people procuring assets to be security-minded and configure them properly, as well as capture and report information about what's on them.

There's a Critical Patch Available. Now What?

Do you even know where all of your affected Internet-assets are? Responsibility for assets not only enables security and IT to direct questions about an asset to the right group or person, but also allows for appropriate monitoring of what that asset is doing, by understanding how it should be behaving, what it should be talking to, and who should be accessing it and for what purpose.

Centralizing and automating your Internet-facing asset inventory also ensures that you've appropriately accounted for each asset so that security teams are monitoring, securing, and testing only those that belong to you. It also assures that time is not wasted in the process of chasing alerts or issues related to assets that aren't yours.

Start from Scratch, Every Single Day.

Most security operations teams aren't as confident as they would like to be–or *should* be–in their asset list. Given all of the changes we've listed above, self-reporting of assets is incredibly messy and unreliable.

Critical things to look for in a framework or platform that can help you manage the lifecycle of Internet-exposed assets include having a continuously updated and validated list of everything Internet facing, generated from real observations, with deep inspection of each asset. It should also be able to assign responsibility for assets and remediation tasks assigned to key groups or individuals, as well as surface exposures or misconfigurations that can be identified from the outside.

These things together are a good start to improve the effectiveness of asset management programs in the age of digital transformation. And you can do that every single day. In a zero-trust model, it's actually important that you do. Just because something was legitimate or accurate or authorized yesterday doesn't mean that it hasn't been changed or compromised today.

For more information about how you can manage your Internet assets with a global Internet perspective, please visit the Expanse web site.

About the Author

Sam Curcuruto, Director of Product Marketing, Expanse

Sam Curcuruto is the director of product marketing at Expanse, an Internet asset lifecycle management company. Sam focuses his day-to-day efforts on working with network and security teams to help them defend their infrastructure from constantly changing cyberattacks via the Expanse platform, which enables IT and security operations to refresh Internet-connected assets so that teams are always operating from a solid foundation. Sam has previously held product marketing positions at network and Internet security companies and is currently pursuing his CISSP certification.