CSO
FROM IDG
December 18, 2018 www.csoonline.com

REVIEW

Review: Continuous cybersecurity monitoring with CyCognito

The CyCognito platform studies networks the same way that hackers do, from the outside with no help or internal bias inserted into the process.

By John Breeden II

Back in the early days of networking, a lot of effort went into hiring penetration testers who would come in and try to break security. They would then report on their findings, and, presumably, whatever flaws or vulnerabilities they discovered would get fixed before real attackers could come calling. Everybody did this, even the military, which dubbed its penetration testers "red teams." An experienced red team could find all kinds of previously unknown threats.

These human-centered penetration testing operations became less useful as networks began to grow. Today, even with something like a two-week engagement, most penetration testing teams can only get to a very small percentage, often less than one percent, of a total network. What good is a report about one or two application servers if there are hundreds or thousands of them deployed worldwide? It's gotten even worse with the move to cloud, virtualization and software-defined networking. Assets might appear and disappear within the space of a few hours, and virtual servers are often abandoned and forgotten about. Most internal information technology teams don't even know about all of their assets, so external penetration testers who visit maybe once a year certainly have no clue.

The industry has responded with things like vulnerability scanners to try and automate what penetration testing teams used to do. But they are limited by their programming and can only scan assets that are known to IT teams or that fall within a range of IP addresses. That's not how hackers operate, of course. They are more than happy to compromise an unknown asset, a server outside of a defined IP range, a cloud asset or even a connected server sitting outside of an organization's direct control downstream in the supply chain.

The CyCognito platform was designed to provide the kinds of advantages that old school penetration testing used to, but on a continuous basis and for modern, global enterprise networks comprised of mixed physical and virtual assets. It basically studies networks the same way that hackers do, from the outside with no help or internal bias inserted into the process

How CyCognito works

Unlike most other reviews CSO has done, for the CyCognito platform there was no setup required. Nothing needs to be installed on the host network and there don't need to be any assets on the inside either. The people who designed the CyCognito platform believe that even a simple act like defining IP addresses inserts bias into the testing. And because hackers aren't given any parameters to work from, an attack surface monitoring tool shouldn't either.

CyCognito maintains a network of over 60,000 bots scattered around the internet. The bots are constantly looking for assets connected to the internet and cataloging their findings, sort of like how Google looks for new webpages. Currently, there are about 3.5 billion assets that have been discovered by CyCognito, and that number is always growing. It's pretty much the entire internet.

Once CyCognito is contracted to perform continuous attack surface monitoring of a company's assets, the platform gets to work, collecting what it already knows and adding to that information. Pricing for the service is tiered and based on the number of assets in the organization's attack surface, with yearly subscription models for the continuous monitoring.

John Breeden II/IDG

CyCognito is always watching. Customers who employ the platform gain access to their own personalized dashboard showing security dangers across their entire enterprise.

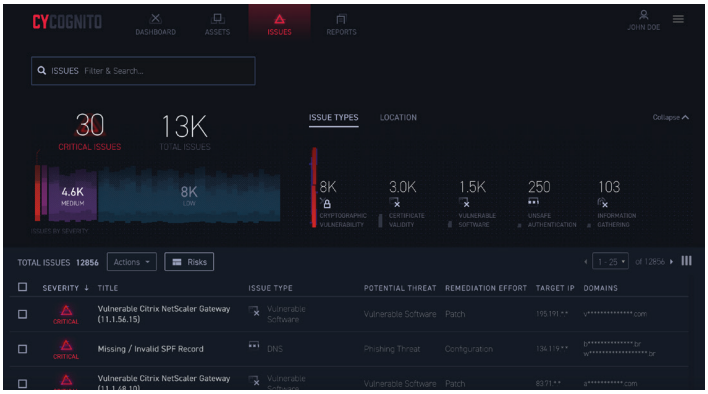
Testing CyCognito

In our testing, CyCognito was able to discover an organization's physical infrastructure including its IoT devices, cloud-based infrastructure, third party assets and several virtual servers that had apparently been abandoned years ago. The engine then grouped those assets into a dashboard that is accessible by the organization deploying the service.

Once it finds those assets, the platform probes them in much the same way that a penetration tester or a skilled hacker would. It moves slowly and doesn't trigger any alarms from embedded security. The platform employs it's 60,000-unit bot network for those tasks.

In our testing, the CyCognito platform not only located thousands of vulnerabilities, but also things like application misconfigurations, weak encryption, assets providing information that could be used in phishing attacks, and critical assets with poor authentication security.

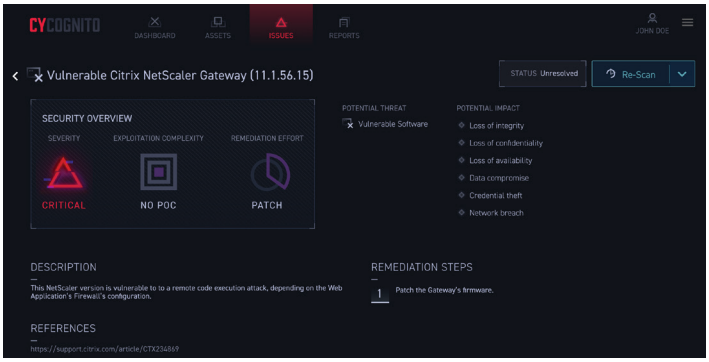
Armed with that information, CyCognito began sorting the thousands of pieces of raw data into useful alerts. For example, alerts were scored based on the amount of real damage that could be done if someone exploited them.



John Breeden II/IDG

Instead of just grouping threats by severity, CyCognito examines every vulnerability in terms of the real harm it could do to an existing network. Only then are they prioritized for users.

The alert score could also be elevated if an exploit were relatively easy to perform over one that required a lot of time and effort from a hacker. CyCognito even prioritized easy fixes ahead of those that would take up a lot of an IT team's time. If there is a critical vulnerability that can be fixed by installing a readily available patch, CyCognito suggests that it be done first before moving on to more complex tasks.



John Breeden II/IDG

Problems found by CyCognito are grouped based on severity, how difficult they are to exploit, how much of a danger they would be to a network, and how easy they are to fix. Here a critical problem can be fixed by a simple patch, so it moves to the top of the to-do list.

Once a vulnerability is fixed, users can trigger CyCognito to immediately rescan that asset from their management console. Or, they can simply wait and let the continuous monitoring nature of the program figure that out.

The dashboard is quite nice, though it is clearly designed to speak to IT teams. To relay network problems and vulnerability-fixing activities to management, you can generate PDF reports that are well-written and graphical. The reports give an overview of network health and the kinds (and number) of vulnerabilities that still exist. Subsequent reports can show how well efforts to secure the entire enterprise are going, and do so in a way that is easy to understand by non-technical people.

John Breeden II/IDG

Because there is often a disconnect between IT teams and company leaders, the CyCognito platform can generate extremely well-written reports in PDF format. The reports describe the nature of problems in a way that anyone can understand.

The last word

The tried and true penetration testing of yesterday has fallen behind modern network infrastructures. But the CyCognito program can help to bring those advantages back in play with its continuous attack surface monitoring. And it can do it with no setup, no humans and no advanced technical knowledge required.