TAG CYBER

Connect to the Correct Vulnerability Data for your Organization

Katie Teitler | June 04, 2020

When it comes to cyber security vulnerability and exploit data, there is no shortage of commercially available and open source tools. From identified vulnerabilities to malware to lists of compromised credentials, organizations are swimming in data. Usually, obtaining this data requires various tools that look at certain parts of the threat landscape. There are internal scanning tools, tools that scan the external web, and those that combine internal and external data so companies can determine prevention and mitigation strategies. Each tool has its place in the security ecosystem, but the number of tools security teams rely on quickly adds up.

Tools management can be a full-time job, especially in larger companies where the attack surface is vast. Yet, the need to understand the threats against company infrastructure has never been more important. While both internal and external threat intelligence are important, gaining

the perspective of a would-be attacker helps security operations teams zero in on key vulnerabilities that can affect an organization's mission.

Despite all these tools and the countless hours security practitioners spend triaging threat information, most companies learn that they've been compromised via a third party—often law enforcement or because Brian Krebs called. A smaller number of companies, generally those with big budgets and large staffs, may be lucky enough to stumble upon or surface anomalous activity via their innumerable logs and alerts.

An early warning system

Arctic Security, a threat and vulnerability management vendor based on Finland, wants to change how companies are made aware of threats and intrusions. Born out of Codenomicon (now part of Synopsis), a security and testing tools vendor, the founders of Arctic Security, David Chartier, CEO, and Teemu Vaskivuo, Head of R&D, wanted to give organizations a better way to learn about a compromise. "Our mission," said Chartier during a recent briefing, "is to help companies that have problems but don't know about them." Which is to say: every company. Cyber security is hard.

Arctic Security automates victim notification by identifying data about the threat landscape. Through external passive monitoring, Arctic Security collects threat data from 100+ sources and maps it to companies' internet presence. Additional integrations can be configured via an API. Using a vast third-party network of data providers, Arctic Security's product finds threat and vulnerability information—compromised machines connected to the organization's infrastructure, infected web pages, leaked credentials, suspicious IP addresses and domains, and more—and "automatically harmonizes the incoming data," in other words, it applies context. Sources of enrichment include DNS, WhoIs lookup data, and geolocation data. Advanced correlation and categorization make it easier for threat analysts and SOC operators to further analyze, process, and map the data so that "companies can focus on what matters to them," said Chartier.

Just enough detail

Through Arctic Security's easy-to-use dashboard, users can view threat data by various factors such as geographic region, industry sector, type/class/name of malware, or observation time, for example. There, users can also view reports of compromised machines communicating outside the network and vulnerable services exposed to the internet so that remediation efforts can begin. The data is presented very cleanly and includes enough detail that allows admins to easily fix problems and/or create prioritized IT tickets, without the effort of getting bogged down in excess data.

But admins don't have to login to the dashboard, necessarily, said Vaskivuo: "Arctic Security is an automated notification factory, so customers are alerted in real time, as issues are found. The point is to notify customers immediately so they can fix compromised computers and vulnerable systems; they don't have to wait until someone else find the problem."

National Cyber Security Centers, service providers, and managed security services are currently the biggest consumers of Arctic Security's products, Arctic Hub and Arctic Node. The tools surface actionable data that the aforementioned organizations can use to alert constituents about high-priority vulnerabilities. Enterprises with sufficient resources would also benefit from the wealth of data Arctic Security collects.

The notification system can work in one of three ways: through portal access, emailed reports, or the organization's other deployed security tools. In the latter case, Arctic Security pushes company- or constituent-specific threat information to the SIEM or ticketing system of choice, making it simple for users to see and investigate the data without having to login to and manage another cyber security tool.

Perfect for ideal-state security

Arctic Security is a wonderful for tool for vulnerability and threat information management, and in the right hands can save companies a lot of pain and suffering. That said, the amount of data provided can be overwhelming. Resource strapped or stressed cyber security teams may find themselves drowning in data they can't do much with. There is also an aspect of "ignorance is bliss." If the company doesn't know about the plethora of vulnerabilities it needs to fix, it can't fix those vulnerabilities. However, in the utopia of security operations, a tool like Arctic Security, especially when combined with security tooling that automates remediation, presents an opportunity to drive down exposures and improve risk.