Nadia Short is vice president and general manager of Cyber and Intelligence Solutions at General Dynamics Advanced Information Systems.

Getting Inside the INSIDER THREAT

BY NADIA SHORT

Although "the insider threat" is a common phrase in today's fast-changing cyber threat landscape, it's not a new phenomenon. Before the days of the computer and the omnipresent Internet, government agencies and the private sector have worked to keep insider threats at bay to preserve the integrity of intellectual property and sensitive information.

Whether insider threats are driven by malicious intent, the result of a careless accident or a moment of forgetfulness, as the Internet continues to grow and networks expand, so, too, does the insider threat. What makes the insider threat unique and unlike any other cyber threat is that it originates from a trusted source.

While phishing and malware attacks are often launched by anonymous bad actors, an insider threat originates from an individual who an agency deemed trustworthy. Because the human factor is tightly woven in the fabric of the insider threat, an enterprise must have the right combination of processes, technologies and people in place to successfully combat this dynamic menace from the inside out.

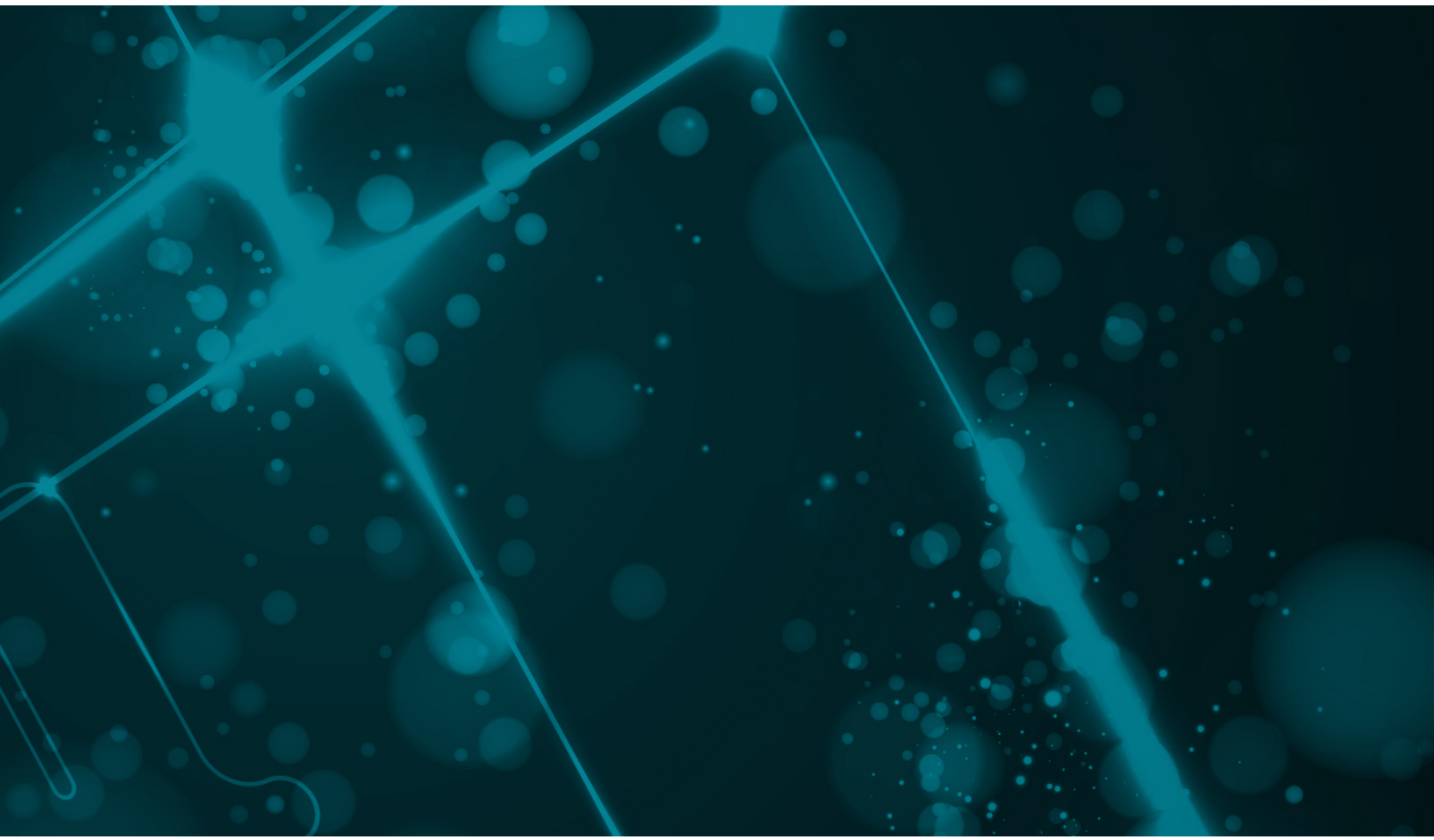
What to do?

So, where should an agency start? The first step in an insider threat detection plan begins with a thorough evaluation of the enterprise. By taking a close look at who has access to the network, where and from what device, an enterprise can work to determine how to monitor access points and associated web traffic. This exercise also serves as a risk assessment, allowing the enterprise to identify areas of vulnerability. Once the baseline of what is normal on the network is established, an agency or company can begin to develop out the processes and programs to keep the enterprise safe.

From aligning with government-driven policies to creating standard operating procedures to developing a policy continuity and maintenance plan, companies need to spend the time and dedicate the resources to building out their formal processes from the ground up to defeat the insider threat.

When it comes to what technologies operate within insider threat processes, that all depends on the customer's mission. As there is no static state in cyber, it is vital that an agency doesn't just go after the latest shiny box, but rather finds a solution that protects, detects and can remediate the threat. Solutions that stand up to the insider threat, and test of time, are truly living, breathing solutions.

But it's also important that these solutions monitor the full lifecycle of a threat – infiltration, command and control communication, propagation and exfiltration – so that data can be tracked as it moves around the network. Additionally, technologies that have real-time updates baked in and leverage threat intelligence from third parties and open source



communities can respond with the agility needed to defeat today's insider threat.

Whether it is the implementation of a digital case management system, or leveraging continuous diagnostic and monitoring solutions, an agency also needs to identify its crown jewels – that data which is most important to protect – and then build the necessary safeguards around it.

Watching the Insiders

One of the most critical pieces of an insider threat detection plan is people. As previously mentioned, people and the insider threat are irrevocably linked – without people, there would be no insider threat, and vice versa. When developing the people aspect of an insider threat detection plan, education should serve as the foundation. Insider threat education includes a variety of awareness campaigns (e.g., signage and posters, best practices, case studies, etc.), general population briefings and formal, classroom-style instruction.

By delivering this critical information via a few different channels, agencies will help raise awareness about the threat while educating their employees about how they can help effectively deter, deny, defend and defeat the insider threat.

In addition to education, agencies can help defend against an insider threat by leveraging behavior modeling analytics to readily identify high risk personnel. With psychology playing a significant role in an insider threat, agencies can work to determine what his/her motivation is, thereby gaining valuable insight into the outside factors influencing the insider threat.

Analysis

Although there is no one-size-fits-all solution when it comes to an insider threat, placing an increased focus on the people aspect and the psychology behind it will help agencies keep pace - and ultimately get out in front of the insider threat.

As our world continues to move towards the Internet of Things and becomes more interconnected via the Bring Your Own Device to work revolution, the insider threat is not going away.

However, if government agencies and the private sector continue to develop robust cybersecurity plans that include the right blend of processes, technology and people, they will be able to continue to make progress towards defending against, and lessening the far-reaching impacts of, the insider threat.