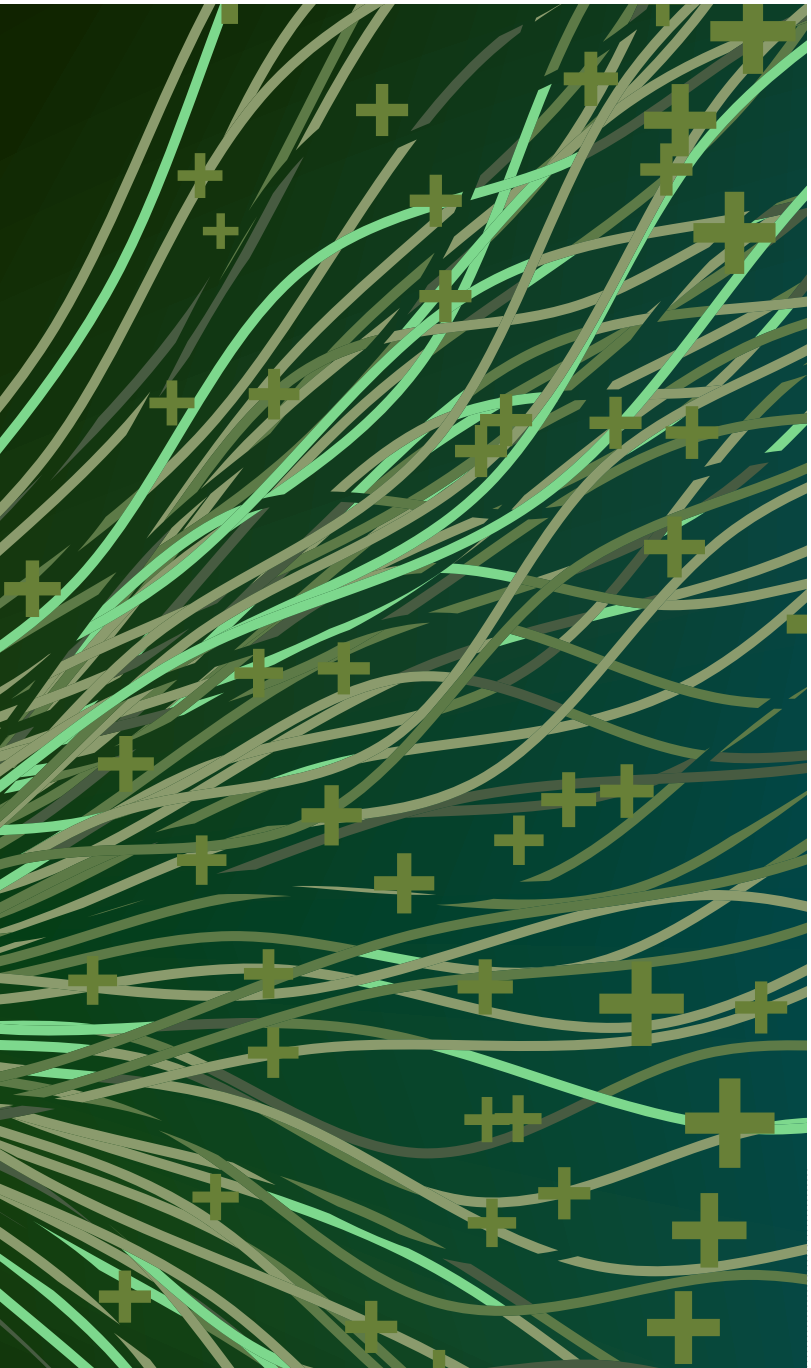
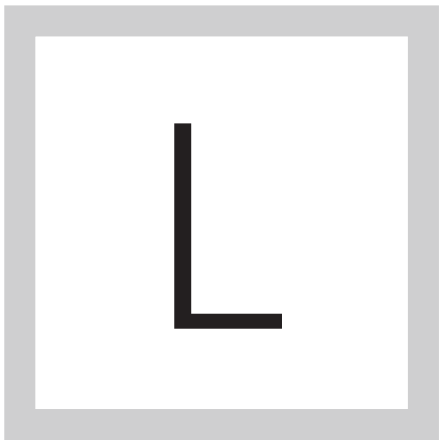


E-Guide

REAL-TIME BEHAVIORAL THREAT ANALYTICS: WHAT IT IS, WHY YOU NEED IT

TechTarget | SearchSecurity



ACK OF QUALIFIED security staff and alarming breach reports got you down? Then it's time to consider a real-time behavioral threat analytics tool.

REAL-TIME BEHAVIORAL THREAT ANALYTICS: WHAT IT IS, WHY YOU NEED IT

Johna Till Johnson

If yours is like most organizations, it's instrumented your environment to detect anomalous behavior by users and systems. You're logging information and digging through that information to find out what has happened.

And you've probably discovered a couple of whopping flaws with your approach.

First, it's expensive and unsustainable. Very few enterprise organizations can afford to hire dozens of security analysts every year, if they can even find them. (And estimates are that the global market is generating a million unfilled security analyst job openings per year.)

Second, and more important, it's slow. Even if you could staff properly, the backlog of analysis means that the average breach goes undetected for months (according to many breach reports). And as the time to exploit an attack continues to increase, that means trouble.

BTA TO THE RESCUE, IN REAL TIME

The answer? Consider deploying real-time behavioral threat analytics (BTA). Real-time BTA tools come from vendors like Bay Dynamics, Exabeam, Fortscale, Gurucul, LightCyber, Securonix, Splunk (through its Caspida acquisition) and others. Although the algorithms are different from vendor to vendor, real-time BTA solutions provide a layer of analysis on top of existing monitoring and logging solutions.

That is, BTA solutions plug into SIEM, IDS/IPS and other systems (like firewalls) and import their log information. They then perform correlation analysis on that information to determine what behavior is "normal" for users, devices and systems. The next step for BTA is additional analysis to determine whether anomalous behavior is just that—anomalous, but harmless—or represents a true threat. BTA products do all this by applying machine learning to the data streams, so security analysts don't need to program in rules about what comprises "normal" behavior.

That means that one of the huge benefits BTA tools can provide is minimizing the number of alerts and false positives—things that look like threats but aren't. Users that have deployed such systems say they bring the number of false

positives down from 500 or more a day (clearly an unmanageable amount) to two or three real threats.

GETTING BTA LAUNCHED

To get started deploying a BTA, the first thing to do is set up selection criteria, starting with the existing and planned security architecture. What monitoring and logging tools are core to your environment and are the go-forward solutions you'll count on for the next few years? Integration into those systems will be a critical selection criterion for your BTA solution. You should also think about what form factor you'd prefer: on-premises or cloud-based. Most security professionals are uncomfortable uploading security logs to the cloud, so on–premises may be the best way to go.

Then you'll want to set up a proof of concept (POC). Ideally, this will be in a self-contained network with a defined set of users, like a stand-alone department or geographical division. Why? Because you'll be able to get a feel for the BTA tool's capabilities—and if it works out, the business owner of that division or department will be your top evangelist in advocating for the system in the rest of the company.

ASSESSING A BTA TOOL

When you run your POC, look for several factors. First, how long does the BTA tool take to "learn" your environment? Most vendors say the tools begin delivering value in a few days—the sooner, the better.

Second, what's the rate of false positives? Are you seeing a dramatic drop or just a minor reduction?

Finally, how does the solution display information? Are there dashboards that can be used by less technical folks, like business stakeholders? Are threats prioritized clearly? Does the system recommend actions and next steps?

Once you've run your POC, you should have a feel for the business benefits such a tool can bring. In addition to reining in the unsustainable growth of security teams, a real-time BTA can enable you to respond to threats in a far timelier fashion—thereby increasing your security stance (and impressing the board with your new agility). Depending on the system, you also may have a more effective approach to documenting threats and compliance concerns.

The bottom line? If you want to understand the threats occurring in your environment, where they're happening, who's affected and what you should do about them, it is likely time to consider a real-time BTA solution.

JOHNA TILL Johnson is CEO and senior founding partner of Nemertes Research, where she sets research direction and works with strategic clients. Till Johnson has decades of experience in technology design, deployment, and operations. Under her leadership, Nemertes has emerged as a leading trusted advisor to Fortune-50 and other world-class organizations.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.