REPORT REPRINT

Darktrace is immune to old security ideas

ERIC OGREN

14 MARCH 2016

The vendor applies unsupervised machine learning to detect significant drifts in user, device or network activity that signal an attack. Its Antigena offering extends behavior analytics detection to fight infections with automated network actions.

451 Research®

 |

Imagine security technology acting as an immune system to prevent infections from thriving in your network. Such a system would have to recognize normal network behavior, align itself as your business shifts, and act to contain deviations. Darktrace applies unsupervised machine learning to detect significant drifts in user, device or network activity that signal an attack. The company's Antigena offering extends behavior analytics detection to fight infections with automated network actions. Antigena enhances Darktrace's behavior analytics security system by allowing enterprises to take automated actions to protect their business. It is an important prelude to the potential of probabilistic products that reduce exposures by acting on intrusions that slip by preventive technologies.

THE 451 TAKE

Enterprises deploy behavior analytics to detect intrusions that evade preventive technologies. Unlike firewalls, intrusion-prevention systems and antivirus software that look to match attack fingerprints, behavior analytics detects changes in endpoint, server and communications that indicate the presence of an attack. In many ways, a behavior analytics process powered by machine learning mimics the human immune system where defenses take action only when normal operations are disrupted. Darktrace applies mathematical models to create statistically significant views of user, device and network behaviors – an approach that makes it adept at detecting attacks that are already within the enterprise.

For instance, Darktrace can recognize a process walking through a file share encrypting data as it goes, but simply alerting security teams is far too slow of a response. By the time a human can respond, the ransomware attack will have been successful and the organization's data will be inaccessible. Antigena can stop the attack, limiting the damage to just a few files. We believe it represents an important step in behavior analytics evolving to an active defense that traditional systems cannot match.

CONTEXT

All large networks are already infected. The problem is that security teams do not know where the infections are living, how long they have been affecting the business, or how to find and eradicate them. Attacks would have been filtered at the perimeter, in the network or on the endpoint if exploit pattern-matching approaches were totally effective, or analysis of SIEM data had proved fruitful. However, experience tells us that as good as preventive technologies are, they cannot catch everything.

Behavior analytics vendors crunch large amounts of data to learn the normal behavior of users, servers and network connectivity. Real-time behavior-processing engines then ingest these models of normal behavior to detect outlier activity that frequently indicates a spreading infection seeking data and credentials to steal. Security teams can then choose the highest-priority alerts to remediate to protect business assets, or in some cases choose automated response procedures to further reduce the time-to-contain cycle.

Cambridge, UK-based Darktrace, which is comprised of a team of mathematicians from British government intelligence agencies, has jumped from its founding in 2013 to become one of the faster-growing behavior analytics providers. The company reports a 450% hike in revenue year over year, more than 200 employees and 750+ installations. Darktrace has quickly become one of the behavior analytics firms to watch.

PRODUCTS

The company addresses market needs with a comprehensive package to analyze large chunks of data, create mathematical models of normal behavior, interpret activity, and concisely report findings to security teams. The technology processes all network traffic in creating models of each user, device and communications path.

Darktrace is based on unsupervised machine learning and probabilistic mathematics. There are no a priori assumptions about what behavior is normal or what constitutes an attack. The immune system derives a baseline of how everything in the business works, applies machine learning to adapt to changes in the business without declaring false security incidents, and rapidly identifies significant problems requiring IT's attention. The company has several offerings:

- Darktrace's flagship product is Enterprise Immune System (EIS). EIS consists of network appliances hanging on span ports and endpoint software, and applies more than 300 measurements of user, device and network activity to detect attacks in the network. The key, of course, is the Bayesian mathematical models grouping views into sets that can be analyzed and statistically processed in real time. The algorithms start defining behaviors with an analysis of big data, and then come to life with real-time dynamic checking of activity against acceptable behaviors. Importantly, the math models work to distinguish acceptable new business practices from suspicious activity to enhance accuracy and reduce false alarms.
- We like the concepts behind Darktrace's Industrial Immune System (IIS). Many Internet of Things-oriented systems are characterized by an inability to support an endpoint agent, well-placed fear of patching and software upgrades, and well-defined communication tendencies with very little daily drift in activity. A retail point-of-sale (POS) system with tablet or mobile POS devices communicating in real time to designated payment servers is a typical scenario that's tailor-made for behavior analytics. IIS supervises authorized business behavior by recognizing a security incident from deviations in network activity. It is a nuanced approach for application environments with requirements that cannot be easily satisfied by traditional hosted security wares.
- Antigena provides an inline appliance and programming interfaces to connect Darktrace to existing security infrastructures. It is our belief that this ability to drive security actions based on observed behavior is critical to protecting organizations against sophisticated threats. For businesses where alerting operations staff is too passive and slow, the Antigena API allows security teams to automate responses via firewalls, endpoint software and management consoles.
- Threat Visualizer is the administrative interface for the Darktrace behavior analytics system. It presents complex mathematical models as perceptions of business flows and the impact of security trouble spots. Darktrace offers its products as a monthly subscription service. This allows enterprises to address critical application environments before committing to extensive deployments. For the vendor, the subscription model provides a level of forward revenue visibility with an easy mechanism for selling advanced behavior services.

COMPETITION

Behavior analytics is becoming a highly competitive space as enterprises evaluate mechanisms to detect penetrating attacks and prevent significant disclosure incidents. Still, we find it to be an immature market loaded with many new entrants. We have identified more than 35 vendors actively competing in the behavior analytics sector, all applying mathematical models that categorize behavior to identify attacks in the network that defeated the best traditional defenses money can buy.

Darktrace can expect to vie with legacy SIEM providers as well as the hot contender du jour for every proof of concept (POC), though so far behavior analytics is a formative area where POCs are usually lightly contested. Players focusing on insider threat use cases include E8 Security, Forcepoint, ObserveIT and RedOwl Analytics. Meanwhile, LightCyber, Niara and Vectra concentrate on network flow data in developing models of behavior without dependencies on other products reporting events. Exabeam, Fortscale and Securonix rely on existing SIEM deployments in treating behavior analytics as a big-data-mining problem. Finally, larger players such as LogRhythm, Rapid7, RSA and Splunk have evolved security information-oriented product lines to offer more complete behavior analytics services to large enterprises.

SWOT ANALYSIS

STRENGTHS

Darktrace taps a sense of urgency within enterprise accounts by targeting a specific segment of the business to secure, typically a key datacenter or facility. This, combined with a flexible subscription pricing scheme, is contributing to early customer wins that can grow to become substantial strategic deployments.

WEAKNESSES

Proving the efficacy of advanced mathematical profiling to catch attacks is difficult, and it is also challenging for enterprises to evaluate and differentiate rivals' claims. Focused POC efforts are required to demonstrate value for important use cases.

OPPORTUNITIES

By virtue of seeing all account activity, behavior analytics has the unique opportunity to initiate security responses. Darktrace is well positioned to expand behavior analytics from a highbrow detection tool to an active prevention and incident response capability that no security-conscious organization can be without.

THREATS

Enterprises will have to carve out budget exceptions to fund new behavior analytics deployments in 2016. This might drive up the cost of ferreting out opportunities and extend sales cycles.