AN INTERVIEW WITH DAVID MOVSHOVITZ, CO-FOUNDER & CTO, REVEALSECURITY

APPLICATION DETECTION AND RESPONSE

Current application security mechanisms detect and protect against the exploitation of application layer vulnerabilities. However, the actual use of applications isn't monitored, which enables internal and external users—users who have legitimate application access—to use them in ways that may cause damage, whether intentionally or unintentionally.

RevealSecurity is a cybersecurity startup that offers unique detection of misuse, abuse and malice conducted in business applications by authenticated users. We wondered how its platform protects applications from human error and targeted abuse by malicious users.

TAG Cyber: Why should we monitor what users do in business applications?

REVEALSECURITY: There are plenty of excellent products that identify and protect against the exploitation of application vulnerabilities, but ultimately people are the most serious threat to business applications. RevealSecurity monitors what people do. Our solution assumes that all applications are perfect and have no vulnerabilities. We then ask risk and security officers whether they have full visibility into how their business applications are being used. Do they know when misuse, abuse or malice takes place? The answers we get are in line with market research, which is that it usually takes months.

TAG Cyber: Why can't rule-based solutions effectively detect behavioral anomalies?

REVEALSECURITY: Enterprises currently try to monitor user behavior and detect malicious activities with rules, but rules suffer from several deficiencies. Here are three. It's almost impossible to define all the allowed scenarios with rules, so rules usually define forbidden scenarios, which means they can only detect *known* forbidden scenarios. You've got to fully understand an application's business processes in order to write rules that apply to it, which is not trivial; and you have to do this for each of the many applications in your organization, and they're all just a click away. Finally, maintaining rules properly is labor intensive and takes time, but rules that aren't properly maintained generate endless false positives and an impossible signal-to-noise ratio. The bottom line is that rules are a 20th century concept, which is now simply outdated and very limiting.

Most solutions are based on rules, which in turn are applied to the entire community. We can't write a rule that will be applicable to everyone because there will always be people who have a good reason to behave a bit differently.

TAG Cyber: What is a signal-to-noise ratio, and why is it typically a problem for rule-based detection?

REVEALSECURITY: A problematic signal-to-noise ratio basically means you're experiencing a high rate of false positive alerts, or "noise." We often see customers suffer from alert fatigue due to a 98% rate of false alerts. Analysts just end up ignoring them. This happens because most solutions are based on rules, which in turn are applied to the entire community. We can't write a rule that will be applicable to everyone because there will always be people who have a good reason to behave a bit differently.

TAG Cyber: Why has UEBA not been applied to application layer detection?

REVEALSECURITY: The implementation of user and entity behavioral analytics (UEBA) has been based on standard infrastructure operations. However, there are no standard operations in business applications. Each application has its own set of operations, and implementing EUBA for all applications hasn't been done. But more importantly, EUBA is usually based on statistical analysis, such as analyzing the averages, standard deviations and medians of various operations. But do I have an "average" day? No, each day is a bit different. A focus on "average" or "median" is therefore ineffective. It generates both false positives (i.e., false alerts) as well as false negatives (i.e., suspicious activities go undetected).

TAG Cyber: How can we accurately detect anomalies within and across applications?

REVEALSECURITY: We do this with user journeys and sequencing. Cisco uses the same concept to detect network layer anomalies with NetFlow. Applications have been absent so far, because how do we normalize so many different ones? User journeys provide us with the context required for detection based on sequences and sessions. We normalize with activity-based journey to detect anomalies in applications. We're now applying them to applications precisely because we've seen them effectively detect anomalies on networks.

Our activity flow model is ubiquitous; the actual meaning of each activity is irrelevant. Since each user has differing activity flows per application, TrackerIQ learns multiple profiles per user. A patent-pending clustering engine groups the user activity flows and generates profiles. These profiles are our foundation for accurate detection of anomalous activities. TrackerIQ also assigns a risk score to each anomaly so that we can prioritize detected anomalies.

Once we start looking, we find patterns. And the more data we have, the more repeatable the patterns. These patterns of normal user journey profiles can be used to detect anomalies in a very accurate way.

TAG Cyber: How does your TrackerDetect solution work?

REVEALSECURITY: RevealSecurity proactively uses application logs to detect anomalies and unknown breaches.

Our underlying technologies are based on unsupervised machine learning of user activity flows. These activity flows are then clustered into behavior profiles for individuals, as well as for cohorts of users. The learning is based on analysis of user sequences of operations. We look at which operations were performed; the order in which operations were performed; and the time intervals between the operations in the analyzed sequence.

If we were to analyze three or four months of my daily activity, we would find similar patterns: days dedicated to solving problems… days dedicated to writing specs… days I spend in meetings. Once we start looking, we find patterns. And the more data we have, the more repeatable the patterns. These patterns of normal activity-flow profiles can be used to detect anomalies in a very accurate way.

TAG Cyber: Do you have any predictions about whether application detection will play a role in future global cyberwars?

REVEALSECURITY: Cyberwars have mostly been about access and penetration of the infrastructure layer. However, in the future we will see a second stage of penetration, one that exploits business applications to achieve the attacker's goals. Attackers will impersonate application users to bypass the monitoring of enterprise networks and infrastructure. Three global trends are leading the market toward application detection. First, applications are increasingly cloud-based SaaS for good reason, but that often takes away the control organizations had on-prem. SaaS, in turn, enables a plethora of applications, ostensibly creating a longtail ecosystem of applications, making rules even more ineffective, while, at the same time, expanding an organization's attack surface as APIs opens it to third parties.