TAG CYBER

APPLICATION DETECTION AND RESPONSE: AN OVERVIEW OF REVEALSECURITY

DR. EDWARD G. AMOROSO, TAG CYBER

TAG CYBER

APPLICATION DETECTION AND RESPONSE: AN OVERVIEW OF REVEALSECURITY

EDWARD G. AMOROSO

Application Detection and Response (ADR) offers strong cybersecurity support for business applications. It works through automated observation and learning of user activity patterns and behaviors to detect anomalies. The RevealSecurity commercial platform implements ADR using innovative algorithms that work on application logs to review user journeys.

INTRODUCTION

Traditional approaches to securing business applications involve experts manually integrating customized controls into the business logic. While this method can result in highly tailored protections, it often doesn't scale and can sometimes leave applications with insufficient security. What is needed instead is a solution that addresses *Application Detection and Response (ADR)* in a way that can scale across multiple use-cases.

One effective approach to this scaling challenge involves collecting streams of data about application usage. The *user journeys* embedded in the application logs can then be analyzed in detail to learn about normal and abnormal business sequences to develop an accurate means for highlighting violations of policy. User journey analysis thus emerges as a powerful weapon against threats to applications.

In this report, we explain how user journey analysis works and how it provides generalized security support for applications. We show how the approach can be used to automatically learn multiple profiles for users within an application, thus offering high fidelity detection of anomalies. The RevealSecurity platform is shown to implement ADR using a variety of algorithmic techniques such as clustering.

APPLICATION DETECTION AND RESPONSE

Many different taxonomies exist for describing security solutions for software applications. TAG Cyber, for example, tracks dozens of subcategories of application security solutions. The approach followed by RevealSecurity aligns well with ADR. The positioning of the RevealSecurity approach has been carefully delineated by Sounil Yu in his fine Cyber Defense Matrix (see Figure 1).

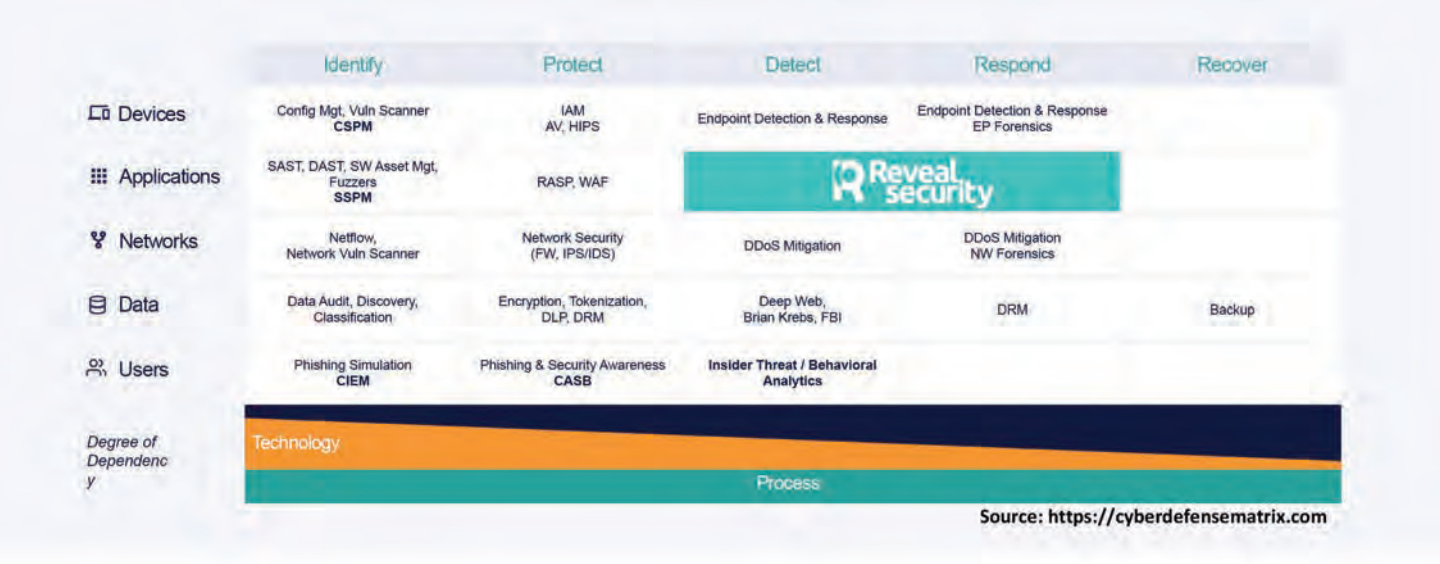

Figure 1. RevealSecurity ADR Positioning

Sounil Yu's analysis of RevealSecurity in the context of his taxonomy positions the solution squarely in the detect and respond categories for applications. Such positioning "to the right" helps explain the overall design goal that the RevealSecurity team has focused on—namely to address these two latter aspects of the user journey. This is different than the attack prevention focus found with other application security tools.

USER JOURNEYS

To implement ADR, cybersecurity systems must collect accurate data regarding user activity and must process this data in an intelligent manner to make sense of what is occurring at an aggregate level. This approach must consider the many different formats, fields, and data included in individual application logs. Making sense of the various concurrent sequences of activity can only occur if this disparate information can be properly resolved.

User Journey Analysis

The method known as user journey analysis involves the collection and aggregation of data from application logs to unravel and interpret logs to determine whether users are behaving in a manner consistent or inconsistent with expected behavioral scenarios. The result of such processing is that application business logic can be monitored for evidence of misuse, fraud, abuse, and other malicious activity.

The RevealSecurity team has positioned their solution and the ADR approach in general in the context of three purported generations of anomaly detection. First generation detection involved rules, whereas second generation approaches extended to include volumetric and frequency analyses. The present third generation employs user journeys as the basis for attack detection (see Figure 2).

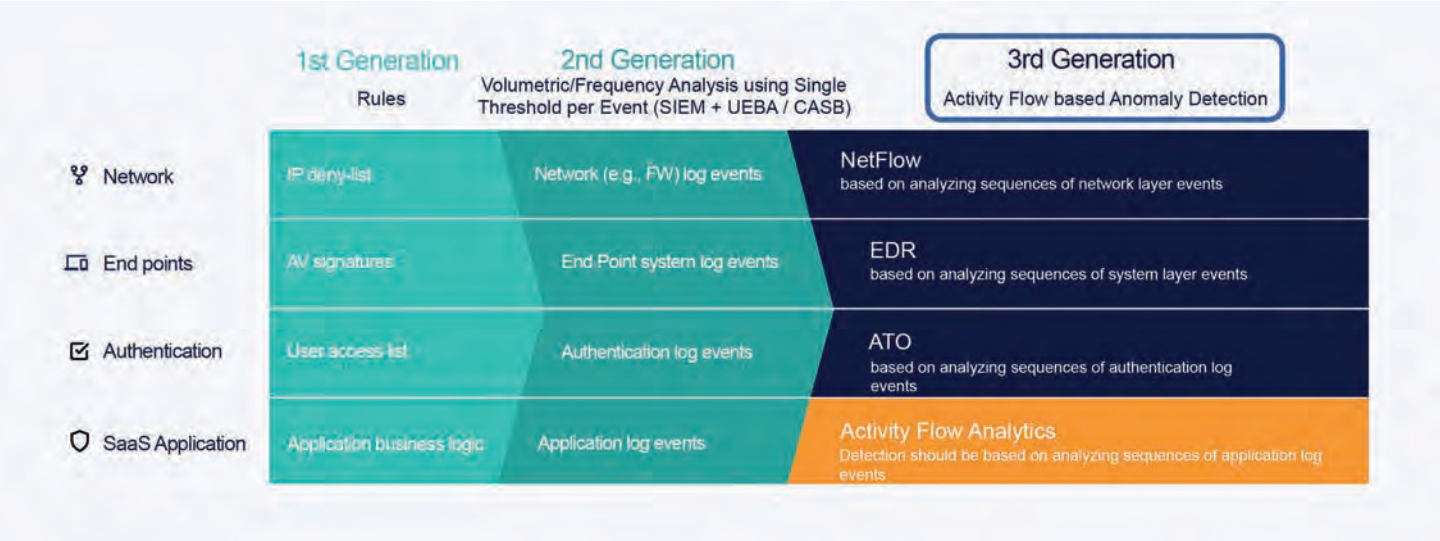

Figure 2. User Activity Journey Analysis

Processing Approaches

The goal of any correlation and algorithmic processing of logs is to create an accurate view of what is occurring at an aggregate level. Two important strategies that help in this regard include clustering and processing of individual user behavior sequences. Both techniques emerged years ago, but when applied to modern resources such as application and API logs, the result addresses many modern and nagging challenges in application security.

Clustering

Clustering involves the dynamic combining of like-resources into groups, which is common in many modern algorithmic design solutions such as K-means clustering solutions on machine learning platforms. The motivation for this approach is to highlight behaviors that do not match the characteristics of a cluster, thus exposing anomalies that should be examined and used as the basis for cyber response actions.

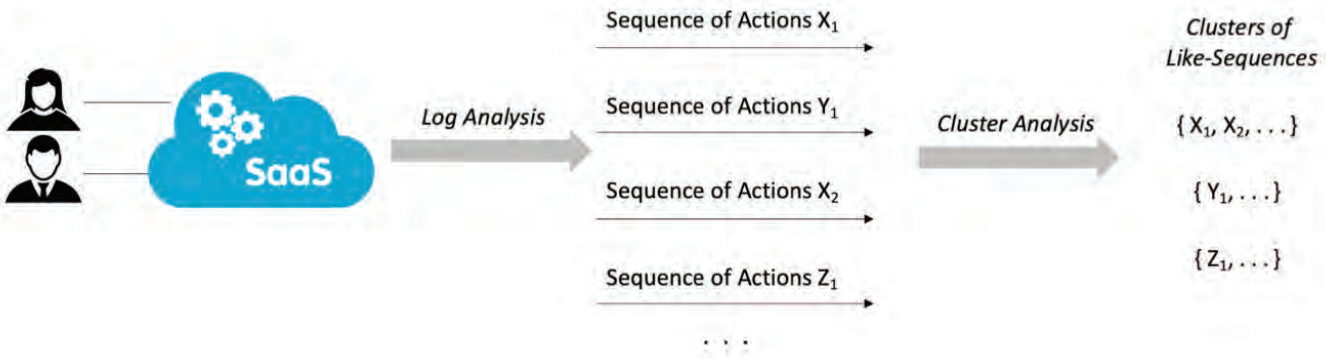

Figure 3. Activity Clustering Approach

The objective of clustering in the context of user activity journey analysis is that indications of misuse, fraud, or other malicious actions might be occurring within an application. This allows for the business logic to be exercised from a security perspective. Profiling is especially useful when signatures are not easily identified, which is certainly true for complex applications with non-trivial business functionality.

Multiple User Profiles

Another key aspect of user journey analysis is that it supports the development of multiple user profiles within an application. The emphasis is on the individual sequences of activity, which can be initiated by the same or different users. This is an essential component of user journey analysis because most attackers will launch multiple threats of attack. Reviews and profiles of each sequence can help identify the attack (see Figure 4 – courtesy of RevealSecurity).

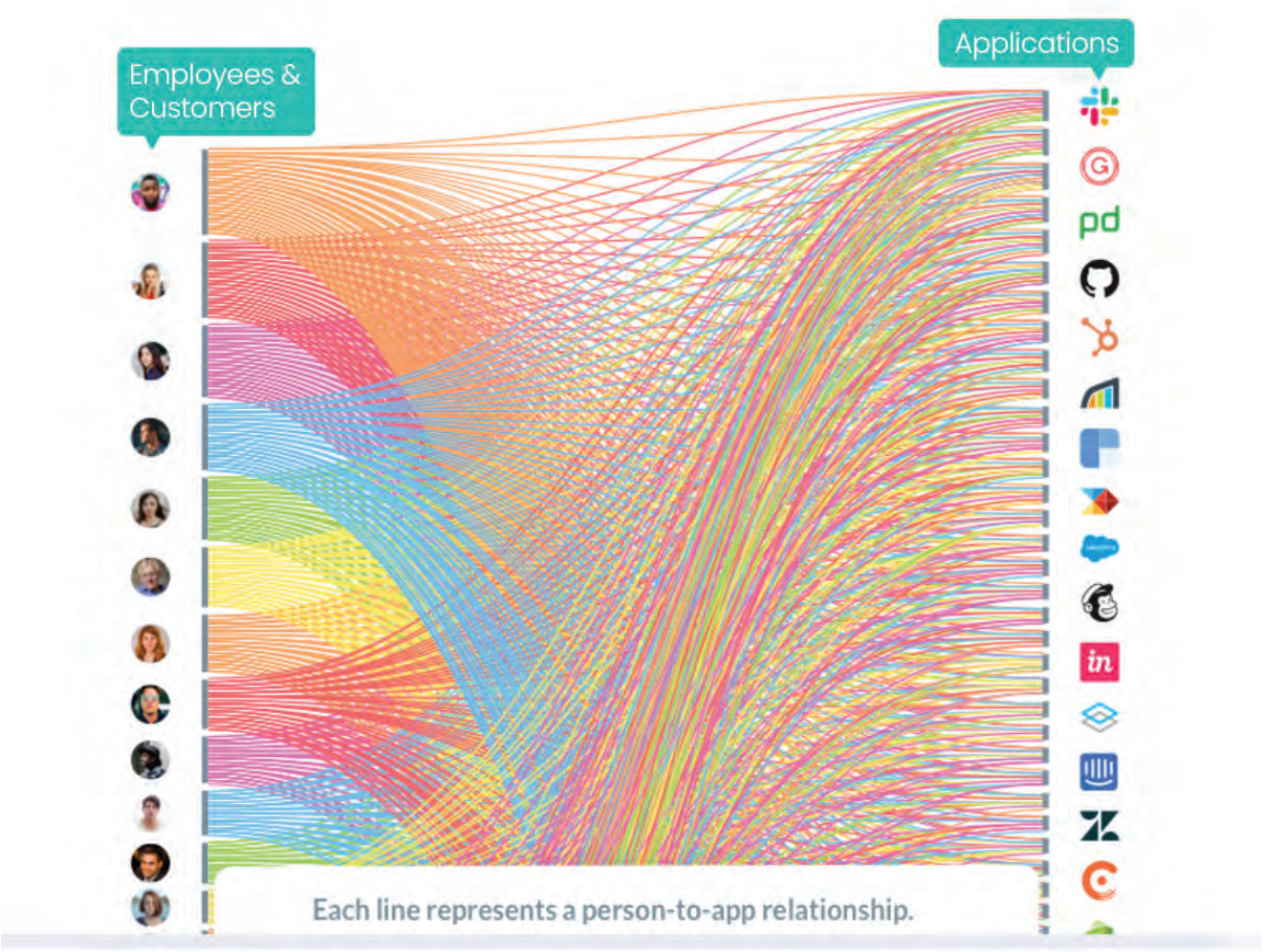

Figure 4. Multiple User Profiles per Application

As one would expect, when individual sequences of activity are being analyzed, the processing goal is to correlate the various threads based on like-attributes. This type of review exposes patterns between different threads, and this is the essence of the detection approach. The goal is to report an aggregate view of the business logic analysis, activity clustering, and user journeys detected in the application.

OVERVIEW OF REVEALSECURITY PLATFORM

Founded in 2020, Israel-based RevealSecurity offers a commercial platform called TrackerIQ that provides an ADR solution. The security platform works across a diversity of application logs and supports increased visibility into these resources. Cybersecurity protection is achieved using activity sequences and advanced behavioral clustering to detect potential application misuse.

RevealSecurity detects security indicators using two methods. First, the use of user journey analysis (as described above) supports review of multiple journeys and sessions to piece together a picture of what is occurring across a range of different applications. The resulting real-time visibility into diverse applications is unique for most cybersecurity settings which cannot connect different usage streams.

Second, the RevealSecurity solution creates and supports multiple profiles per entity that are learned automatically by a unique clustering engine. Once typical journey profiles are defined, the solution compares them with every new session. This is especially valuable for enterprise teams that would expect to be attacked by an adversary through a home-grown, custom-built application. The specific commercial offerings are listed below.

TrackerIQ ADR
The TrackerIQ platform uses anomaly detection based on context and indicators in applications. User journey modeling and profiling detect known and unknown patterns of employee, partner, and client behaviors that deviate from expected application models. This can be applied to behaviors in traditional enterprise applications as well as SaaS and cloud. The platform integrates with log management and SIEM tools such as Splunk and ELK.

The advantage of profile-based analysis has been well-established in the cybersecurity community for insider threat detection. The trick for commercial organizations has been to find ways to minimize false positives while also improving accuracy. The clustering approach used in the TrackerIQ platform provides for both goals through user journeys and models of business applications (see Figure 4).

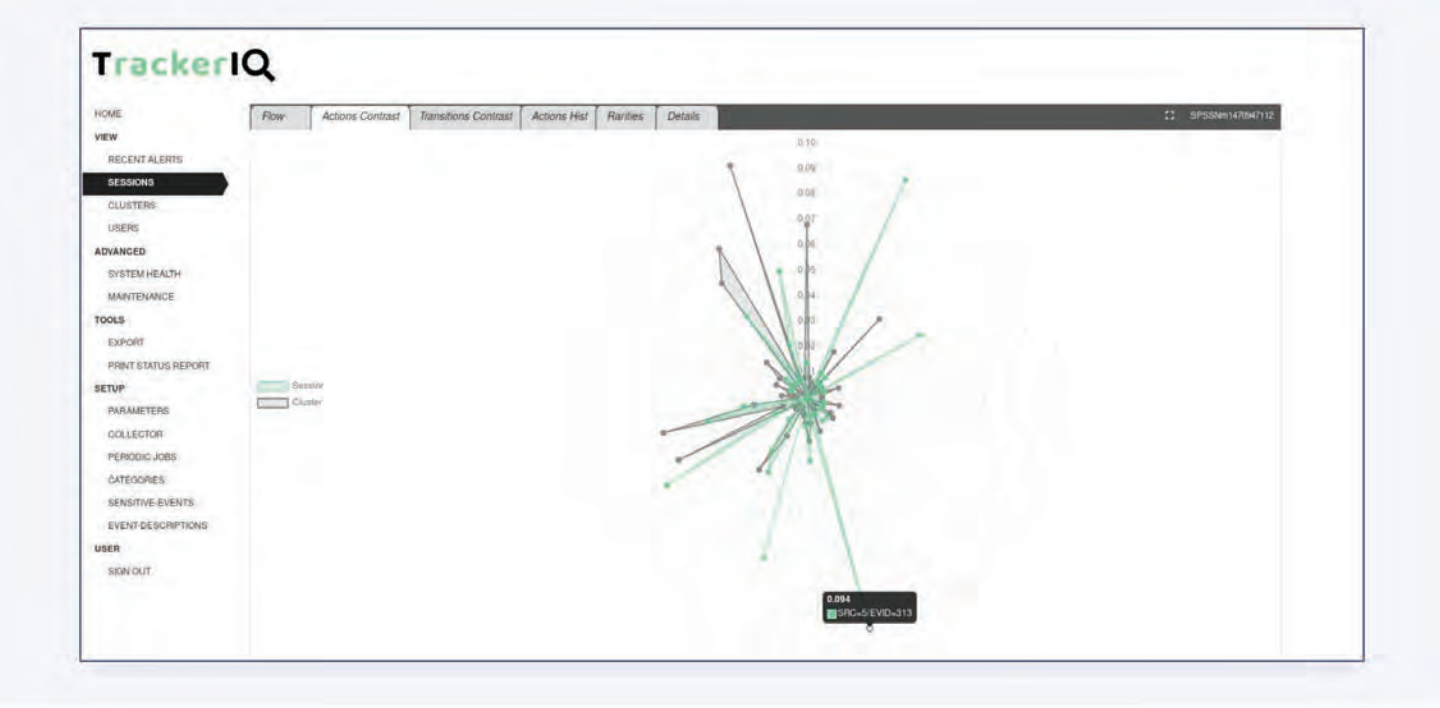

Figure 5. Detecting Anomalies

TrackerIQ Business Challenges
The RevealSecurity platform enables the following tasks for the enterprise security team related to insider threat detection:

1. Signal to Noise Ratio: The platform addresses the problem of too many false positives for operations teams.
2. Detection of Unknowns: Traditional rule-based detection solutions rely on finding what's known and are hence outdated and restrictive.
3. Using Operational Profiles for Detection: This approach involves defining what is correct and inclusive for a given profile.
4. Large Number of Applications: The platform is designed to handle the complexity of monitoring a growing number of applications.
5. Lack of Qualified Security Analysts: Modern automated platforms help deal with the skills gap in cybersecurity.

PROPOSED ACTION PLAN FOR ENTERPRISE

CISOs and risk officers should immediately engage in a management action plan designed to take advantage of activity flow capabilities in their application layer. This plan should be designed for integration into larger strategic and tactical programs. It should also complement other security programs that may be focused more on the prevention of cyberattacks in applications.

The action plan should begin with an investigation into the landscape of application security vendors. Obviously, TAG Cyber has worked with RevealSecurity, and we view their solution as being consistent with the type of controls that should be present for ADR. Nevertheless, enterprise security teams should contact TAG Cyber for assistance in their vendor research. TAG Cyber offers Research as a Service (RaaS) support for such work.

Once suitable vendors have been selected, a proof of value (POV) trial is recommended to determine the suitability of the ADR security processing for select application activity logs. The good news is that application detection solutions are well-suited to POV because they can collect and process data off-line if preferred, and this makes it much easier to implement a trial using actual production output.

[1] *https://www.reveal.security/*

[2] *Sounil Yu is the CISO and Head of Research for commercial cybersecurity vendor JupiterOne, which offers cyber asset attack surface management, cloud security posture management, and DevOps security solutions for enterprise customers. His Cyber Defense Matrix is described in a book recently published by JupiterOne Press.*

[3] *See the 1999 book, Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response, by E. Amoroso. (https://www.amazon.com/Intrusion-Detection-Introduction-Surveillance-Correlation/dp/0966670078).*

[4] *https://towardsdatascience.com/how-does-k-means-clustering-in-machine-learning-work-fdaaaf5acfa0*

ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner's perspective.

IMPORTANT INFORMATION ABOUT THIS PAPER

Contributor: Dr Edward G. Amoroso

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman, (lgoodman@tag-cyber.com), if you'd like to discuss this report. We will respond promptly.

Citations: This paper can be cited by accredited press and analysts but must be cited in context, displaying the author's name, author's title, and "TAG Cyber". Non-press and non-analysts must receive prior written permission from TAG Cyber for any citations.

Disclosures: This paper was commissioned by RevealSecurity. TAG Cyber provides research, analysis, and advisory services to many cybersecurity firms mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.