RSA SILVER TAIL®

Innovative and Effective Online Threat Detection

THE EVOLVING THREAT LANDSCAPE

The threat landscape is ever evolving and increasingly challenging. Some of the threats today's organizations are vulnerable to include:

- Account Takeover via robotic attacks, password guessing, Man-in-the-Middle or Man-in-the-Browser and HTML injection
- Business Logic Abuse or the use of website functionality for malicious or exploitative purposes (e.g., abuse of loyalty point programs or shopping cart functionality, fraudulent account set up)
- Distributed-Denial-of-Service or DDOS attack on the application layer where a deluge of page requests coordinated by a bad actor overwhelms the server and brings the site down
- Site or Architecture Probing to gather as much information about site structure and security vulnerabilities as possible to prepare for an attack on that site
- Site & Inventory Scraping or data theft perpetrated by copying large amounts of data from a website, typically via automated script
- Mobile Channel Threats such as mobile session hijacking

IDENTIFYING CRIMINAL BEHAVIOR ON LINE

Complex online cyber attacks and fraud schemes cost organizations billions of dollars annually. Many of these attacks exploit the legitimate functionality of web and mobile channels to take over user accounts, steal money, scrape information and perpetrate other types of fraud.

When you have so many people interacting with your website on a daily basis it can be difficult to tell the difference between legitimate and criminal users – after all it is virtually impossible to monitor what every individual is doing at all times.

Cybercriminals exploit this lack of visibility into user behavior by hiding themselves and their activities among legitimate users and legitimate activities - making it extremely difficult for organizations to detect these types of attacks in real time. Rather, they must rely on log and other retrospective data to investigate the cause after an attack has become a reality.

This results in low fraud detection rates, high costs of manual review and increased exposure to threats.

RSA Silver Tail helps identify potentially criminal use of a website by detecting anomalous online behavior - behavior that is out of the ordinary from general population of web visitors. This allows the information security and fraud teams to focus their attention on the users that have exposed themselves as potentially disruptive rather than trying to identify the cyber equivalent of a needle in a haystack.

RSA SILVER TAIL HELPS YOU TELL THE DIFFERENCE BETWEEN CUSTOMERS AND CRIMINALS

RSA Silver Tail can help organizations meet the challenges posed by an ever evolving and increasingly challenging threat landscape through the use of web session intelligence to distinguish between legitimate and disruptive users.

Web session intelligence is actionable information gleaned from click stream data, created each time a user clicks on any object on a web page. It provides visibility into how users are interacting with your site in real time so that you can respond to potential threats in real time.

SOLUTIONS BRIEF

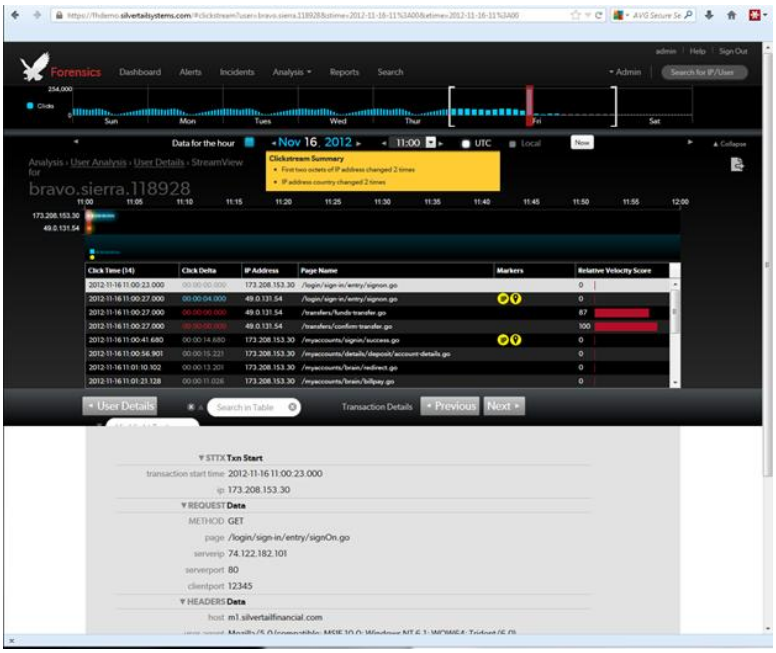
CRIMINALS IDENTIFY THEMSELVES THROUGH THEIR ONLINE BEHAVIOR

Criminals do behave differently than legitimate site users.

That becomes apparent when you compare how quickly they move through the site, where they access your site from, even how they navigate through the site. They also leave tell-tale signs such as IP addresses and user-agent strings that indicate their presence.

Silver Tail identifies these anomalies in real time so that you can respond in real time.

For example, if an individual logs in from a certain IP address, that IP address should be the only one that appears during the web session. If the session is hijacked, however, a second IP address will also be present during that same session.



Similarly, consider the case of a known user who always accesses an account from one of two IP addresses, both of which are associated with the United States. If that account is accessed from a third IP address in China, especially if it is accessed shortly after the US IP address has initiated activity, it may be indicative of an account takeover.

An atypical page navigation sequence can also indicate potentially disruptive behavior. Visitors to an ecommerce site, for example, typically browse from product page to product page interspersed with visits to their shopping cart. A web session in which pages are visited in alphabetical order is likely one initiated and controlled by a bot.

Likewise, unusual interaction with a new account registration page can indicate business logic abuse. Usually only one or two new accounts will be established from a single IP address and it takes at least a minute or so, depending on the amount of information requested, to complete the form. If during a single web session hundreds or even thousands of accounts are established within a few minutes, it is a sure sign of robotic activity.

Silver Tail identifies behavioral anomalies such as these so that threats can be stopped before they become realized attacks.

USING WEB SESSION INTELLIGENCE TO IDENTIFY BEHAVIORAL ANOMALIES

Silver Tail constructs behavioral profiles to support the identification of anomalous behavior. These behavioral profiles reflect what constitutes legitimate behavior on your site and are built dynamically based on how users actually interact with your site. This enables potentially fraudulent or disruptive behavior to expose itself.

Silver Tail captures and analyzes click stream data to build these profiles. Behaviors that don't conform to the profiles are flagged as suspicious – Silver Tail's rules engine allows you to respond to different levels and types of threats.

Similarly, Silver Tail can compare current behavior against past behavior for individual known users. So for example if an authenticated user always logs in from one of two IP addresses in the greater Boston area but suddenly logs in from an unrecognized IP address in Eastern Europe a red flag is raised.

This is all done in real time so that you can respond in real time.

The use of dynamically created profiles to help identify online threats represents a critical divergence from the traditional approach – rather than trying to intuit activities or sequences of events that would indicate disruptive behavior, Silver Tail allows anomalous behavior to expose itself.

This is imperative in an environment where what constitutes legitimate use may look slightly different from site to site and even from day to day on the same site.

STREAMING ANALYTICS DRIVE INTELLIGENT THREAT DETECTION

Silver Tail is self-learning so it can adapt to changing user behavior – because it collects so much data profiles respond rapidly to new behaviors.

Silver Tail compares individual user session behavior to the profile and calculates a threat score. Threat scores are a tangible indicator of anomalous activity that may carry an associated risk.

Threat scores are calculated for each click and in real time. Threat scores for IPs and users are graphed and ranked so that you can identify emerging threats at a glance and respond quickly.

Because the scores are calculated in real time, they can also be used in rules. So, for example, you could automatically send an alert when a Man-in-the-Browser or parameter injection score exceeds a certain threshold.

Comparing user behavior against behavior that characterizes legitimate use of the site allows you to focus your attention on anomalous and potentially "bad" behavior – with Silver Tail, fraudulent or threatening activity stands out like a sore thumb.

Silver Tail's real-time threat detection capabilities are powered by streaming analytics, a platform that enables the calculation of threat scores in real time on a click by click basis.

With streaming analytics, info sec and fraud teams can get the information they need to focus their attention on potentially disruptive users, enabling faster threat detection and mitigation.

WHY SILVER TAIL

Silver Tail offers a number of advantages over traditional hardware and software security solutions.

- No disruption of customer experience or site performance - Silver Tail leverages the SPAN port for port mirroring. All of the data collected is directed in real time to a dedicated server for monitoring and analysis
- Self-learning risk engine - Silver Tail's self-learning risk engine continuously updates behavioral profiles according to the site's traffic patterns. What constitutes anomalous (and potentially disruptive) behavior changes over time – Silver Tail keeps pace with these changes by dynamically updating profiles.
- Real time detection of anomalous behaviors - When you can detect threats in real time you can respond in real time. Silver Tail can send alerts within 2 milliseconds to firewalls, SIEMs and authentication tools so that they can take immediate action
- Almost immediate time to benefit - Silver Tail leverages Big Data to detect online threats. Silver Tail monitors and analyzes every click so the software can begin building behavioral profiles almost immediately
- Rapid deployment - in most cases Silver Tail can be deployed in less than a day
- Highly scalable - Silver Tail handles over 330,000 SSL handshakes per second

Silver Tail significantly enhances an organization's ability to prevent, detect and respond to a broad range of online threats and attacks.

BUILT FOR THE WAY FRAUD AND INFO SEC TEAMS WORK

SIMPLIFYING THREAT IDENTIFICATION

Silver Tail's intelligent and interactive user interface enables users to immediately identify threats and understand their causes

- Incident queue includes rule name for immediate identification
- Summary function translates click stream anomalies into easily understood terms
- Interactive geo-spatial maps allow you to visualize where traffic is concentrated

FACILITATING THREAT INVESTIGATION

Silver Tail has task-driven and streamlined workflows to support deeper and more efficient investigation and analysis

- Prioritized and easily navigated incident queue drives rapid response
- One click incident investigation brings everything you need to a single screen for greater insight and more efficient analysis
- Robust transaction search and incident filtering speed investigation tasks
- Cutting edge data visualization and click stream analysis support more sophisticated analysis.

RSA SILVER TAIL PRODUCTS

The Silver Tail portfolio is comprised of three products that work together to identify and mitigate potentially disruptive or criminal behavior.

RSA SILVER TAIL FORENSICS

Forensics lies at the heart of the Silver Tail online threat detection system.

- Forensics monitors each click and all HTTP/HTTPS data for every web session active on your site, providing comprehensive web session intelligence and context in real time. Forensics' self-learning risk engine then uses this data to develop population-based behavioral profiles – individual user behavior is compared to the profile and anomalous behavior is flagged.

RSA SILVER TAIL MITIGATOR

Mitigator is Silver Tail's real-time rules engine.

Mitigator allows you to enforce organizational or other custom policies as well as determine how to respond to different levels and types of threats. Because it integrates with your existing infrastructure, Mitigator offers you total flexibility around responding to both potential and realized threats.

Features of the Mitigator rules engine include:

- Ability to use real-time threat scores in rules (e.g., if the man in the Middle Score is >90, create incident)
- One-Click Rules so that you can deploy rules across all pages of a website without having to code pages individually
- Rule Tags for identifying rule owners, functional group membership, threat type etc. to enhance reporting capabilities

- Automated Alert Generation so that if a behavior trips a rule, an alert can be sent to firewalls, SIEMs and authentication tools as well as your fraud and info sec teams. Response time is within 2 milliseconds to support genuine real-time response
- Time Stamp for more granular control around rules are fired (e.g., only outside of normal business hours)

RSA SILVER TAIL PROFILE ANALYZER

Profile Analyzer helps prevent fraudulent activities perpetrated by someone who has stolen the credentials of a legitimate, non-threatening user or hijacked their web session.

Profile Analyzer constructs behavioral profiles for individual users in much the same way it constructs a profile for the site population. Once a known user logs into his account, current behavior is compared to past behavior and deviations are marked.

Profile Analyzer is integrated with Mitigator so that you can leverage the rules engine to respond to threats generated from the accounts of known users. You can also drill down into individual IP addresses and users for even greater visibility.

CONTACT US

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at www.EMC.com/rsa.