CLICK SECURITY

DATASHEET

RtSA Tracker

Traditional Security Defenses are Insufficient

Traditional security defenses like firewalls, intrusion detection/prevention systems, anti-X product and web proxy servers are necessary, but at best – insufficient. Security event management and forensic tools are inherently designed for "after the fact" post-analysis of what has already occurred. Security analysts are asking for a solution that lets them find and investigate the unknown – which is at least anomalous, and potentially malicious – before it is too late.

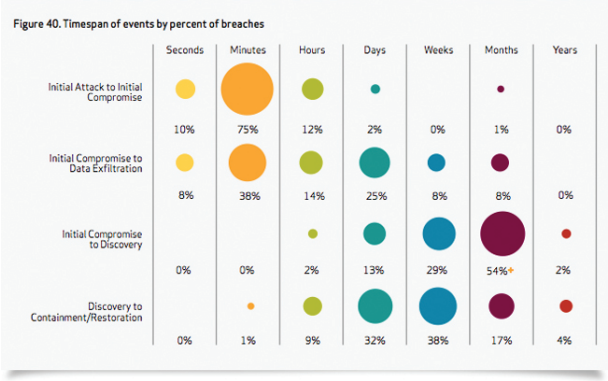
Consider the findings within the Verizon Data Breach Investigations Report, 2012 – which shows that 85% of the time it takes hackers minutes or less to move from initial attack to initial compromise. Yet, 85% of the time it takes organizations weeks to months, even years, to discover the compromise.

A New Approach is Needed

Click Security's RtSA Tracker application – which runs on our revolutionary Real-time Security Analytics (RtSA) platform – provides automated visibility into early stage kill-chain activity – enabling organizations to piece together anomalous and malicious actor activity before exfiltration or damage occurs.

RtSA Tracker is equipped with trigger analytics, a purpose-built user interface, and playbooks that allow analysts to:

- **Rapidly perform freeform contextual queries**
- **Sharply reduce the time and energy required to isolate anomalous and malicious activity**
- **Pinpoint anomalous actor behavior, as well as the exact progress each actor has made over time and distance – before it is too late**



2012 Data Breach investigations Report (DBIR), Verizon.

KEY FEATURES

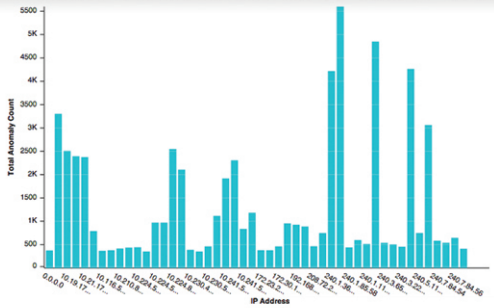
- **Intelligent Protocol Interpretation**
  Traditional log collection and alert management products collect and retain data in raw format, except where obvious alert trigger data can be easily normalized. RtSA Tracker automatically ingests, parses and organizes specific user, device, server, flow, and security alert telemetry - freeing the analyst from spending loads of time sifting through raw logs to create meaningful source information that can then be analyzed.
- **Automatic User ID Correlation**
  Log records coming from different sources create a "jigsaw puzzle" of identifiers about a given user, including multiple IP addresses – depending on where the product sits relative to NAT/PAT boundaries – and spotty user ID data from web proxy logs. Other products force the analyst to piece together data into a form where it becomes contextually meaningful. RtSA Tracker intuitively associates identity elements across different data sources into a complete picture of the user identity – automatically.
- **Auto-Contextualization into Actors**
  A lot of recursive time and energy is required to piece together a contextual picture of big data representing user, device, server, and event data before considering analysis. Traditional log and event management products – and even newer map reduce/fast search products – have no notion of pre-contextualization. RtSA Tracker encodes the intelligence of Click Labs research into "automated situational awareness". Hundreds of thousands, even millions, of telemetry logs and events are automatically contextualized into a meaningful actor population.
- **Hotspot Revelation**
  Given a large attack surface, every event can appear to have equal importance at the outset. Something must point your eyes to initial areas of interest. Other products present the network as a "flat earth" picture with no investigative start point. RtSA Tracker visually highlights activity clusters – drawing focus to areas of interest quickly.
- **Dynamic Playbooks**
  Once a hotspot or anomaly has been highlighted, RtSA Tracker paints a situational awareness picture through playbooks – complete with graphic visualizations that enable the analyst to intuitively explore. The laborious, frustrating work of investigation is now streamlined. You are operating as a security analyst/"investigator", and not as a generic "data scientist".

Automating the analysis is the key to finding, understanding, and proactively addressing early stage kill chain activity.

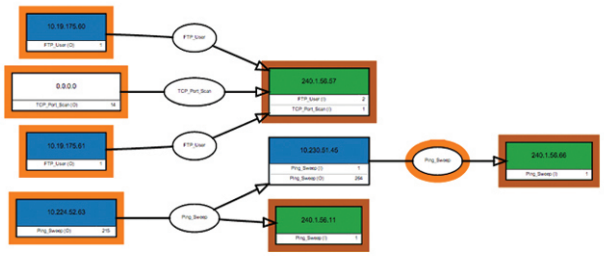
RtSA Tracker in Action

Click Labs has developed advanced trigger analytics driven by internal and external telemetry sources, augmentation enrichment data, easy-pivot visualizations, and ready-to-use playbooks that simplify the job of finding and understanding anomalous activity in your network.

Analytics include threat-anomaly detection (Top N, Policy Violation, Vulnerability + Attack, etc.), integrated threat anomaly augmentation (Security Zone, Blacklist, Vulnerability Scan) and unique threat visualizations (Fanout, Top N, Actor, Maps, etc.) – giving the analyst real-time, contextual insight into network activity – as a situation of interest is developing – well before damage or exfiltration occurs.



First, analytics and workbooks present all network actors in a histogram view – instantly showing the analyst which actors – and it could be just a handful within a population of thousands – are registering the most anomalous activity.



Second, each actor can be further tracked with our unique fanout view – showing every machine on your network the actor has connected to by protocol – instantly revealing how broad and deep his reach is into your world.

Finally, as shown below, playbooks assimilate specific, context-rich 'leads' so analysis work results in root cause repair – as opposed to continually treating symptoms, which will never scale.

Example suspicious leads revealed through analyst playbooks:

- Thousands of systems from Iran continue to send HTTP requests to "Company.com". Thought to be associated with the Pushdo trojan.
- Blacklisted spider/cracker bots from the Netherlands are combing the Company internet-facing servers.
- a.b.c.d is receiving inbound probes from international systems, and connecting to blacklisted servers and suspicious cloud servers.
- The "suzyq" user is logged in from China and is generating a high event count including a lot of IIS OWA errors.
- The "johndoe" user is logged in from a non-portable address in China and performs a large data upload and generates a lot of IIS OWA errors.
- The IIS OWA server is generating "500 Internal Server Error" responses to almost all "POST /EWS/Exchange.asmx"; the issue involves many clients.
- The IIS OWA server is sending an unrecognized server response code: 441
- There is a mysterious relationship between the Company DNS server at e.f.g.h and the systems s.t.u.v and w.x.y.z. The two latter systems are sending a lot of suspicious UDP traffic to the former.
- r.t.s.u is sourcing IIS OWA authentication requests for thousands of usernames, all but one of which are rejected as "unauthorized". This system also attempts to perform a PDF download via a redirect through the OWA server as a Yandex bot, and is observed sending requests with the "Crazy Browser" user-agent.
- These four servers are being heavily probed by international actors using a variety of remote access protocols including telnet, SSH, and RDP: 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4

RtSA Tracker's unique ability to automate the analysis accelerates time-to-detect, time-to-understand, and time-to-action – reducing business risk by thwarting early-stage kill chain activity.

CLICK SECURITY

6500 River Place Blvd.
Building 1, Suite 350
Austin, Texas 78730

+1 512 637 8500
info@clicksecurity.com
www.clicksecurity.com