ATTACKERS STILL HAVE THE UPPER HAND

Despite significant investment in information security, attackers appear to have the upper hand. According to the Verizon Data Breach Investigations report (2013), 97 percent of breaches led to data compromise within "days" or less, whereas 78 percent of breaches took "weeks" or more to discover.

- Attackers are becoming more organized and better funded. But while attacks have become dynamic, defenses have remained static. Today's attacks are designed to exploit the weaknesses of our user-centric, hyper-connected infrastructures.
- IT-enabled organizations continue to grow more complex. Organizations now demand much more open and agile systems, creating incredible new opportunities for collaboration, communication, and innovation. This also results in new vulnerabilities that cyber criminals, "hacktivist" groups, and nation states have learned to exploit.
- There are often not enough skilled security professionals to help organizations protect themselves effectively. The 2013 (ISC)2 Global Information Security Workforce Study found that 56% of its respondents believe that there is a security workforce shortage.

To reverse the tide and protect their organizations better, security teams need a few things. They need:

- Better visibility into what’s happening in their environments, from their networks, to their servers to their applications and endpoints.
- More contextual analytics of what’s going on to help them prioritize issues more effectively and concentrate more resources on those issues that are more likely to impact their business.
- Actionable intelligence from diverse sources, both internal and external, to tell the system what to look for in a more automated way, and help them respond quicker.
- An architecture that scales to support the business as it grows and evolves.

RSA and Pivotal have worked together to create an architecture that truly helps security teams to fulfill these needs, and help speed up attack detection and response times, and reducing the impact of attacks on organizations. Moreover this approach creates a platform that can be used for a myriad of other use case across IT operations and the enterprise.
VISIBILITY IS THE FOUNDATION FOR SUPIOR ANALYTICS

RSA and Pivotal provide unparalleled visibility into user and system activity across the IT environment. RSA Security Analytics provides a collection infrastructure that can provides full visibility into

- **Network Activity** by performing full packet capture, session reconstruction and analysis of packet data
- **Log Data** by collecting log and event data from devices and applications that support business and IT activity.

Collection occurs through the deployment of “decoder” devices topographically close of the systems generating the data, either through a span port or tap (in the case of packets) or through common system protocols including syslog, SNMP, ODBC or proprietary protocols.

RSA Security Analytics also integrates with systems that collect contextual information like

- **Asset data** – this includes the collection of technical configuration data, as well as business context like what business processes the system supports, or the criticality of the system
- **Vulnerability data** – data which can add additional context to an investigation (e.g. when the system was last scanned and what vulnerabilities were present) or to help prioritize response to attacks on vulnerable systems
- **Identity data** – additional contextual information about the user, their location, their job function and the privileges they have.

RSA Security Analytics enriches the log and network data it captures with this contextual information to aid in the “downstream” processing of that data, either in the detection or investigation of threats.

Fig 1. Security Analytics High Level Architecture
RSA and Pivotal combine to provide numerous types of analytics, needed to spot threats at different times in the information lifecycle. The three main types of analytics provided are:

- **Capture time analytics** – to identify interesting characteristics of data right at the time of capture. This includes:
  - Basic characteristics – e.g. source IP, destination IP, username, log action, etc.
  - Interesting characteristics – e.g. such use of encryption, executable files, administrative users, administrative commands
  - Indicators of compromise – e.g. known bad IPs, known bad protocols, watchlist users

  Security Analytics creates “metadata” out of these interesting characteristics that can be used for further analytics or to facilitate investigations

- **Streaming analytics** – to analyze metadata in real time to spot concurrent sessions or actions happening over a short time window that might be an indicator of a threat. This metadata could be log-based, network-based or from another contextual source. Examples include:
  - Basic SIEM-like correlation rules: like 5 failed logons followed by a successful logon
  - Compound indicators of compromise: like a user downloading suspect JavaScript at around the same time as an encrypted session to a blacklisted country
  - Hybrid log & network rules: like malformed traffic bound for a host at around the same time as encrypted traffic to a blacklisted country

  Streaming analytics can be based on combinations of events or deviations from a “baseline” normal count of a piece of metadata. Streaming analytics appliances need not be deployed right at the point of data collection, but can be deployed in parallel throughout the environment for enhanced scalability.

- **Batch analytics** – to identify “low and slow” type attacks, and patterns that occur over extended periods of time. Batch analytics is performed by the RSA Security Analytics Warehouse, which has Pivotal HD at its core. Pivotal uses proven Hadoop and other Big Data technologies, and the Pivotal Data Science Labs team to enable different analytic techniques including:
  - Rules based pattern matching
  - Cluster analysis
  - Anomaly detection
  - Machine learning

  Batch analytics and these advanced methods facilitate use cases such as malicious domain detection, beaconing host detection, and anomalous user behavior detection.

In addition, RSA Security Analytics provides a log **archiving** capability to allow organizations to satisfy retention and reporting requirements, but store the data in a cost-effective manner.
ANALYTIC METHODS COMBINE TO FACILITATE ADVANCED SOC ACTIONS

Threat analysts need a combination of capture time, stream and batch analytics to detect and investigate a full range of threats. Each of these methods combine to support a number of workstreams common in a security operations center, like:

- Visualizing heat maps of issues across an organization by business unit or profile
- Profiling systems or devices for indicators of risk
- Prioritizing alerts when a particular critical business asset or user exhibits multiple suspicious characteristics over a week-long period
- Providing investigative context after an alert gets triggered to determine the cause or impact of an issue, e.g. if the user downloaded an executable prior to the alert, or the IP accessed a critical asset after triggering the alert

In addition, using Pivotal and Hadoop, and the Pivotal Data Science Labs team offers the potential to add additional capabilities like:

- **Predictive modeling** – using visibility and context to predict where issues are likely to occur
- **Analyst feedback loops** – allowing analysts to provide feedback whether they think a particular alert warrants follow-up, and allowing the system to learn that for future alerts

DISTRIBUTED ARCHITECTURE ALLOWS FOR ENTERPRISE SCALABILITY AND DEPLOYMENT

Many systems have claimed to offer this functionality, but have failed. This is because older architecture using old database technologies and proprietary data stores don’t work. More analytical compute power than ever is needed to analyze the data, but this needs to be provided cost effectively.

Pivotal and RSA have teamed up to create a Security Analytics platform that provides an architecture that deploys components throughout the environment in order to provide superior scalability and deployability, and the ability to deploy the platform in a modular way to suit an organization’s unique use cases.

- **Collection and Capture-Time Analytics** get deployed close to where the activity occurs. This allows the system to scale across locations more effectively. This also minimizes the impact on WAN connections, since the system can be configured to transfer only metadata, not raw data across these connections.
- **Streaming Analytics and Archiving** get deployed centrally or in a federated way. Architects can decide to deploy the system in a more central way, or in a federated way. This gives maximum flexibility to take into account compliance regulations around cross-border data transfer requirements or network constraints.
- **Batch Analytics** gets deployed in a Hadoop cluster that takes advantage of the resilient nature of a Hadoop distributed computing environment
- **SOCs** operate where the best talent resides. With this architecture, the Security Operations Center can access the data and perform analytics from anywhere across the organization.

A sample multi-location architecture diagram is included below.
PIVOTAL EXPANDS USES OF COLLECTED DATA ACROSS IT AND ENTERPRISE USE CASES

The combined Pivotal and RSA platform allows IT organizations to gain greater value from the data collected through the use of the collected data for non-security use cases. The open architecture gives IT organizations flexibility to leverage Hadoop tools, or Pivotal tools like HAWQ and Spring XD to develop applications and analytics for adjacent use cases like:

- Capacity planning
- Mean-time-to-repair analysis
- Downtime impact analysis
- Shadow IT detection

Moreover, outside of security and IT operations, there are a myriad of options for incorporating security into a wider Enterprise Data Lake allowing the data to be used for uses such as customer experience monitoring and billing. This allows customers to gain much wider benefit across their organization from their investment in Pivotal and RSA.
BENEFITS OF RSA-PIVOTAL APPROACH

The joint RSA-Pivotal offering provides customers with:

- Reduced risk of compromise by using the latest analytic and detection techniques and threat intelligence to aid in the detection, investigation and response to security incidents
- Reduced deployment risk and quicker time to value through proven, validated architecture for collection, analytics of data that produces actionable intelligence at enterprise scale
- Less reliance on Data Science expertise to leverage cutting edge analytic techniques
- Take better advantage of existing security expertise by adding analytic firepower
- Enterprise-wide benefits as collected data integrates with the Enterprise data lake