

Securonix – Harnessing the Power of Behavioral Analytics

10th October, 2019

Ralph Kreter

About Securonix:

Company:

- Founded 2008
- 350+ employees, 200+ customers worldwide
- Privately held. \$29M Series A funding in Sept, 2017

Products:

- Next-Gen SIEM
- Security Data Lake
- User and Entity Behavior Analytics

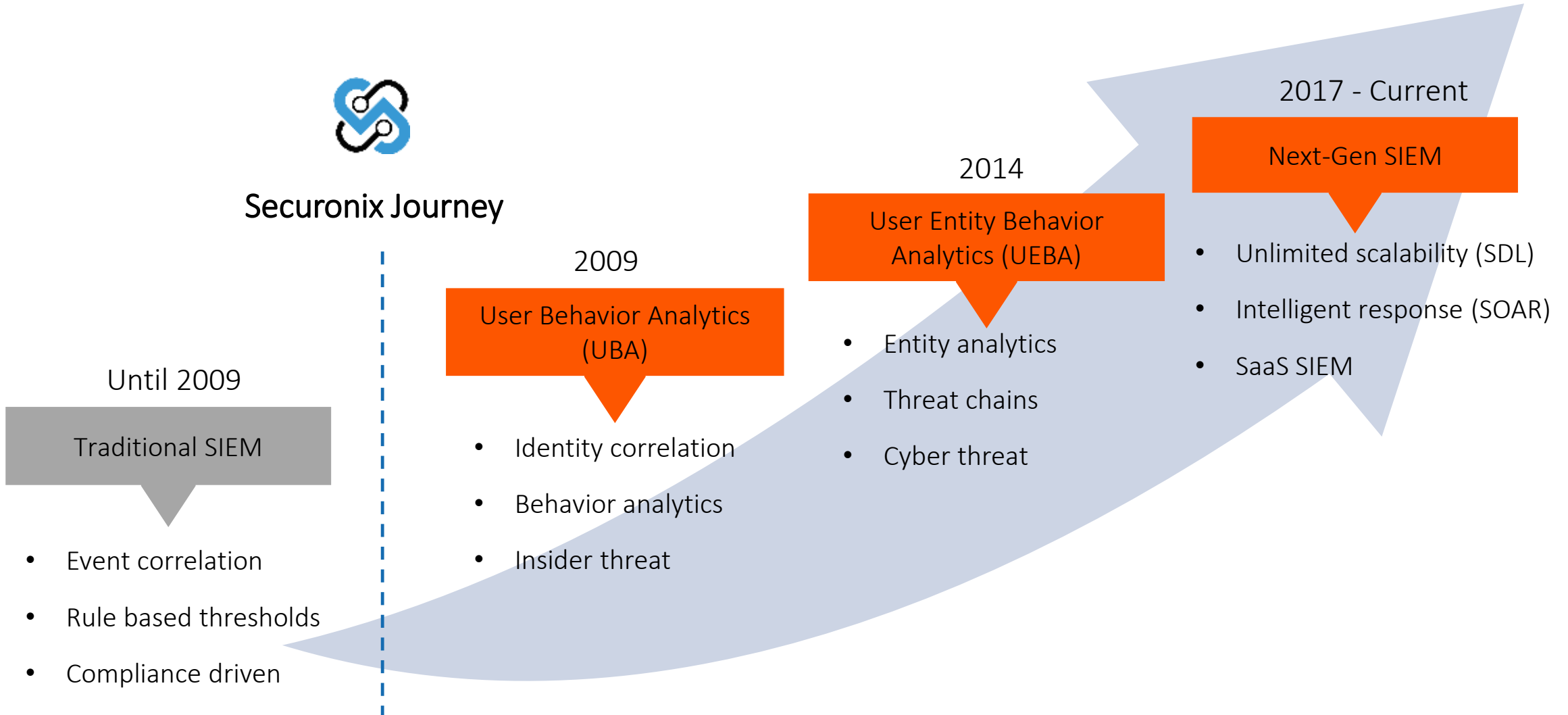
Awards



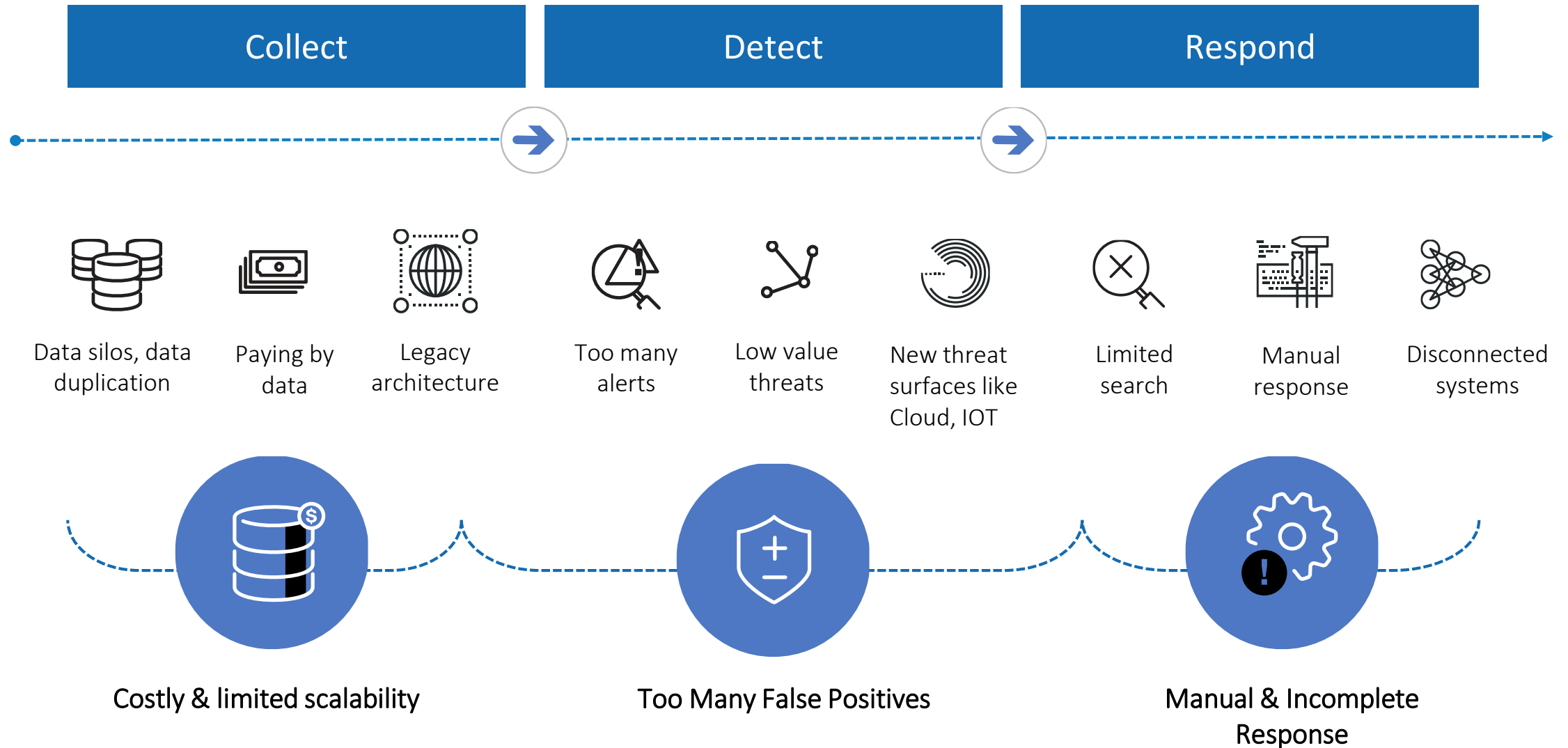
Evolution to Next-Gen SIEM



Securionix Journey



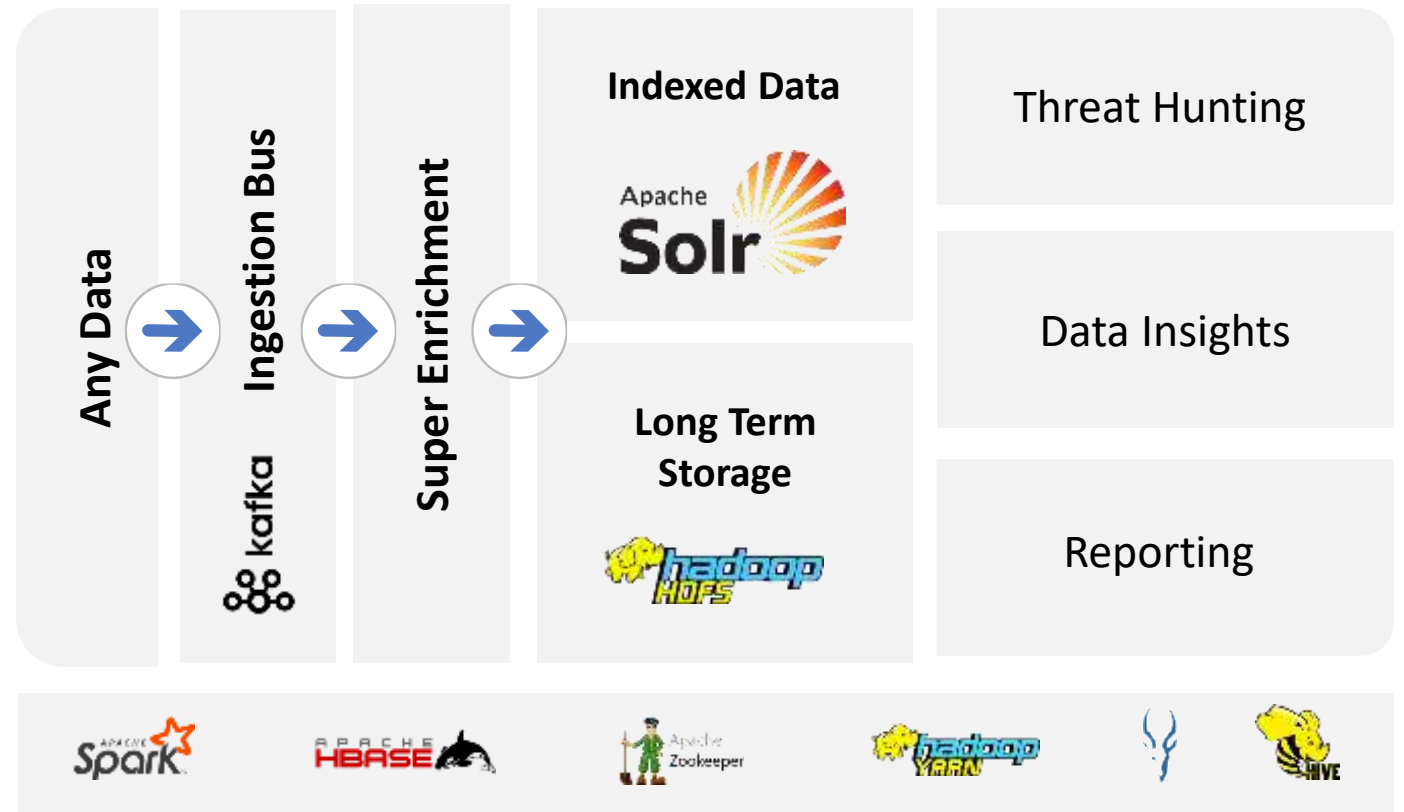
Today's SOC



Hadoop Platform - Unlimited Scalability

- Own your data - built on native Hadoop platform with no proprietary components
- Not priced by data – Identity based pricing [+ hosting cost for SaaS SIEM]
- Unlimited scalability

-
- Tested to over 600,000 EPS in our lab
 - In production @ 350,000 EPS
-



Securonix Data Lake

Components of Next-Gen SIEM

Intelligent Orchestration and Response (SOAR)

Automated Response

Adaptive Learning & Decision Automation

Self-Learning

Advanced Threat Detection (UEBA)



Threat Hunting



Threat Attack Advisory



Pre-emptive Threat Intelligence


Threat Detection

Machine Learning – Behavior Analytics Engine

Analytics Framework

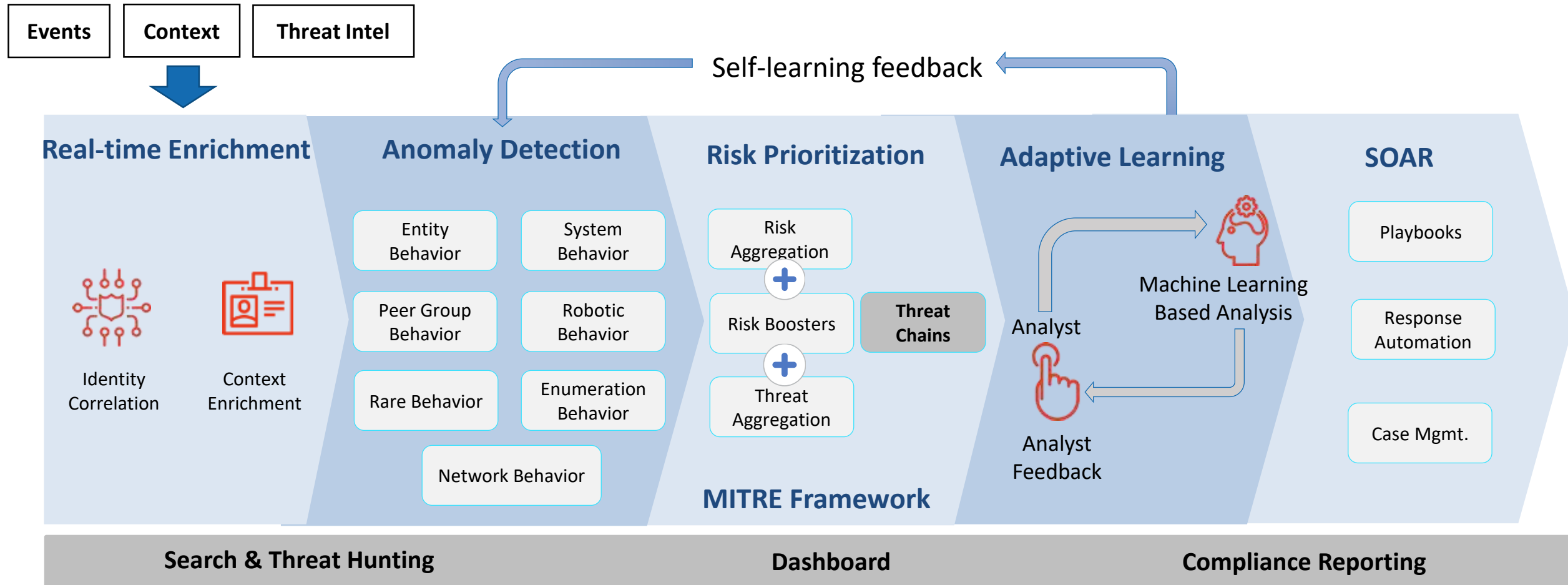
Security Data Lake – Horizontally Scalable, Open Platform

Log Mgmt.

 Delivered as a Service

Add-ons: Vulnerability Risk Analytics, Network Traffic Analytics, End-point Analytics, Continuous Risk and Compliance Monitoring

How does it work



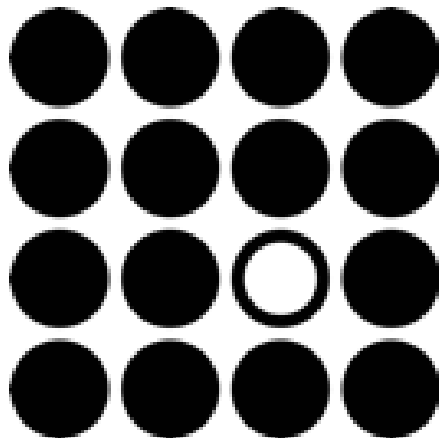
Use Cases

Samples

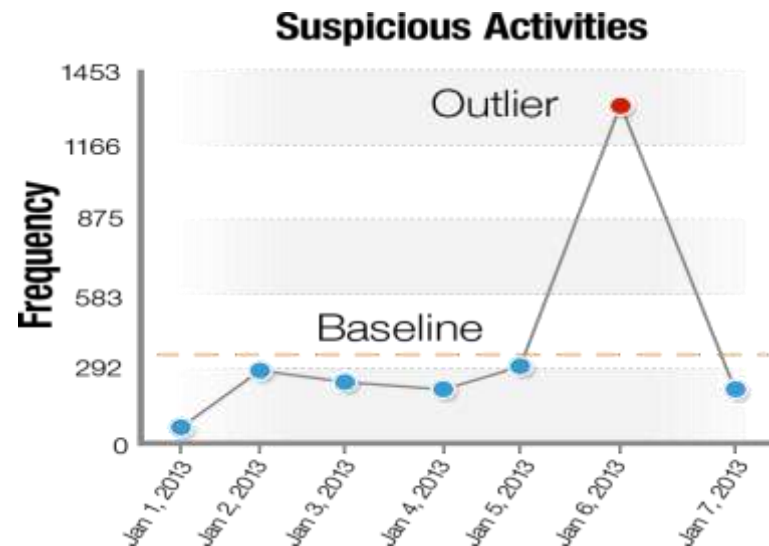
- Patient Data Snooping (EMR)
- IT employee accessing patient records not accessed by peer
- Access patients from unusual location (state/country) never seen before
- Spike in break the glass violations
- Rare outpatient activity when the doctor typically performs only inpatient activity



Geo-location



Rarity

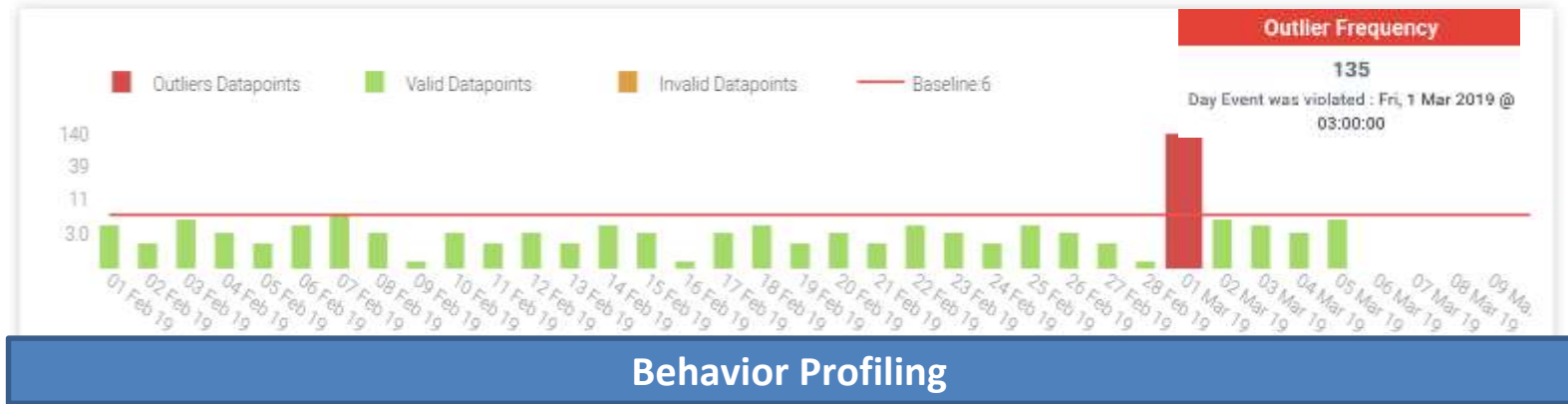


Behavior Analytics -> Threat Chains

Securonix uses behavior analytics to baseline normal and flag outlier activity. The baselines are created for all entities – users, machines, IP addresses over different time slices (weekdays, weekends, time of day)

Behavior Profiling/Anomaly Detection Models

1. Rare behavior detection
2. Frequency/Amount spike detection
3. Enumeration detection
4. Peer outlier detection
5. LandSpeed detection
6. Phishing analyzer
7. Network Traffic Analyzer
8. Domain age detection
9. Threat Intelligence lookup



Most, if not all modern day threats are perpetrated over a period of time. Securonix uses threat chains to stitch related alerts to prioritize low and slow threats



Meet Data Privacy Requirements

Data privacy can be a key requirement to protect employee privacy and other sensitive data

Securonix supports capabilities to maintain data privacy [and meet GDPR requirements]

Securonix privacy capabilities include:

- Data can be anonymized with masking
- Role based access control
- Data filtering or eraser [GDPR requirements]
- Audit trail

Securonix privacy capabilities have been approved by customer work councils across EMEA and APAC

Request to Unmask



Approver



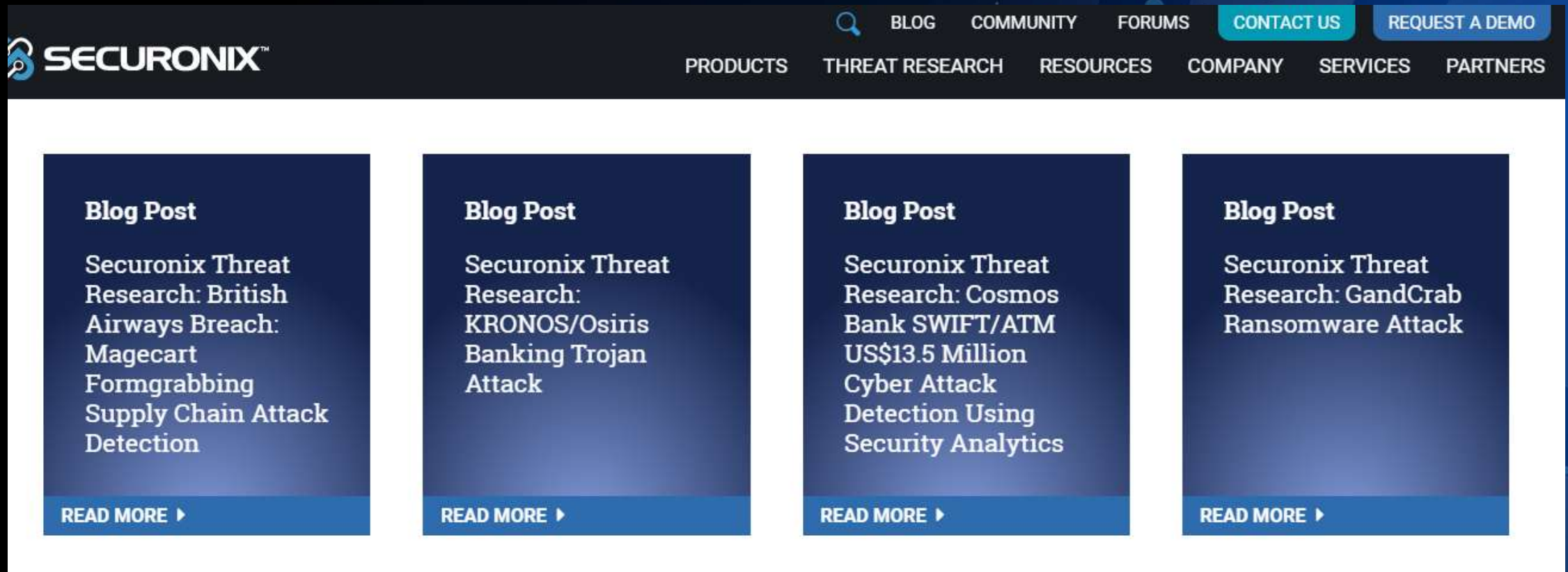
Securonix Masking Workflow

The screenshot displays the Securonix Masking Workflow interface. It is divided into three main sections:

- Masked Entity:** Shows a masked employee record with a risk score of 57.4. The masked ID is A19F82E1F6FA1A8C095E469A9F8245BE B5BA2426 698F4DC6C9EF8C8D66F7885F. The department is PROCESSING AND FULFILLMENT.
- RBAC and Workflow for approval:** A table of pending requests. The first request is from Admin Admin for Eimear Smith [2388], a User, with a date range from 04/20/2018 to 04/21/2018. A 'send request again' button is visible.
- Unmasked Entity:** Shows the unmasked employee record for Hollee Richardson, with a risk score of 57.4. The employee ID is 1160, the department is Processing and Fulfillment, the manager ID is 1068, and the title is Vice President Business Services.

Securonix Threat Research & Hunt

120 people in Threat Hunt, Threat Research, Data Science – providing Behavioral Models / Threat chains



The screenshot displays the top portion of the Securonix website. The navigation bar includes the Securonix logo on the left and a search icon followed by links for BLOG, COMMUNITY, FORUMS, CONTACT US, and REQUEST A DEMO. Below this is a secondary menu with links for PRODUCTS, THREAT RESEARCH, RESOURCES, COMPANY, SERVICES, and PARTNERS. The main content area features four dark blue blog post cards, each with a title, a brief description, and a 'READ MORE' link with a right-pointing arrow.

Blog Post Title	Blog Post Description
Securonix Threat Research: British Airways Breach: Magecart Formgrabbing Supply Chain Attack Detection	Securonix Threat Research: British Airways Breach: Magecart Formgrabbing Supply Chain Attack Detection
Securonix Threat Research: KRONOS/Osiris Banking Trojan Attack	Securonix Threat Research: KRONOS/Osiris Banking Trojan Attack
Securonix Threat Research: Cosmos Bank SWIFT/ATM US\$13.5 Million Cyber Attack Detection Using Security Analytics	Securonix Threat Research: Cosmos Bank SWIFT/ATM US\$13.5 Million Cyber Attack Detection Using Security Analytics
Securonix Threat Research: GandCrab Ransomware Attack	Securonix Threat Research: GandCrab Ransomware Attack

Thank You