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

Securonix Journey

Until 2009

Traditional SIEM

- Event correlation
- Rule based thresholds
- Compliance driven

2009

User Behavior Analytics (UBA)

- Identity correlation
- Behavior analytics
- Insider threat

2014

User Entity Behavior Analytics (UEBA)

- Entity analytics
- Threat chains
- Cyber threat

2017 - Current

Next-Gen SIEM

- Unlimited scalability (SDL)
- Intelligent response (SOAR)
- SaaS SIEM

Today's SOC

Collect | Detect | Respond

Data silos, data duplication

Paying by data

Legacy architecture

Too many alerts

Low value threats

New threat surfaces like Cloud, IOT

Limited search

Manual response

Disconnected systems

Costly & limited scalability

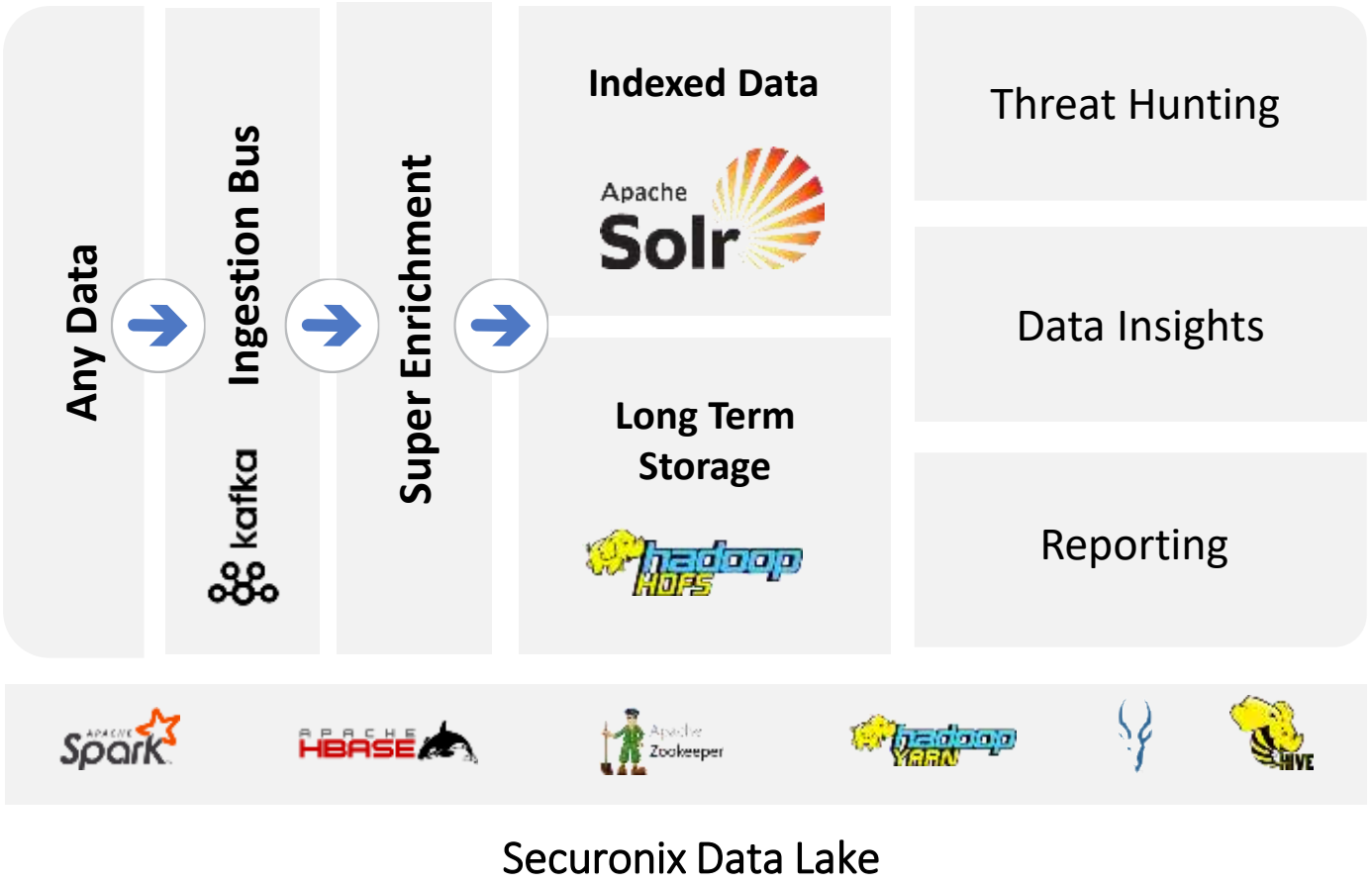
Too Many False Positives

Manual & Incomplete Response

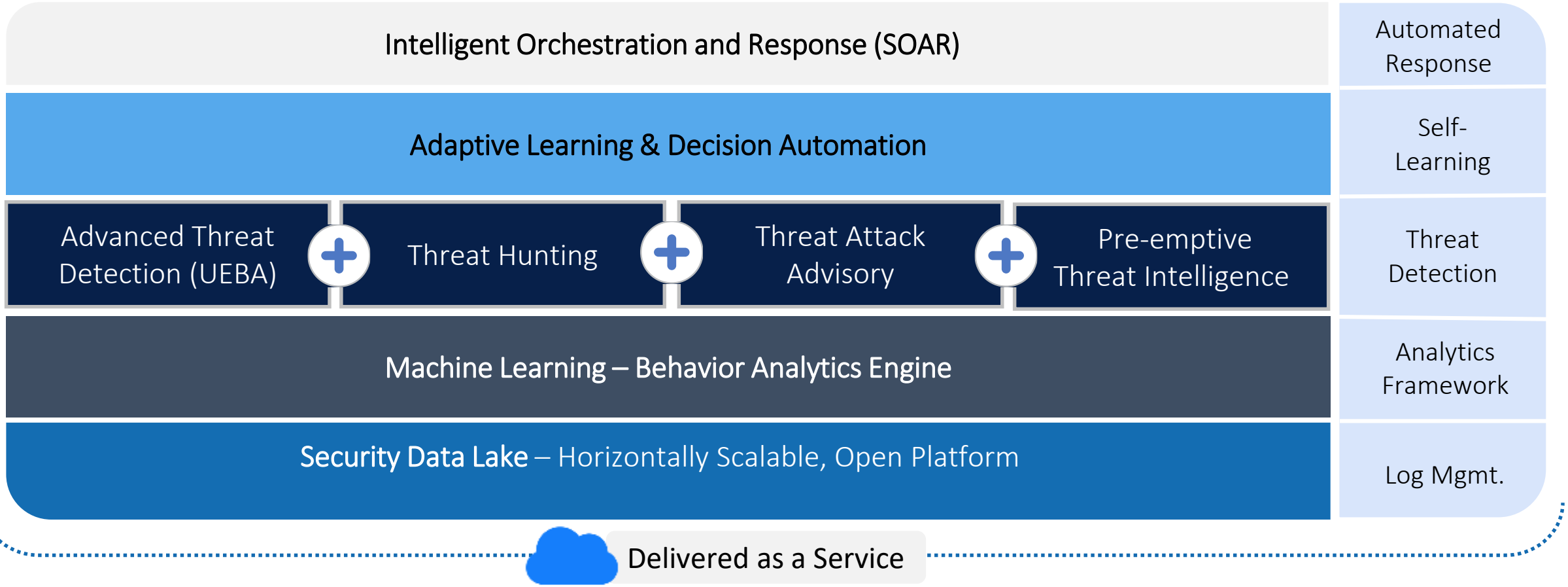
Hadoop Platform - Unlimited Scalability

- 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

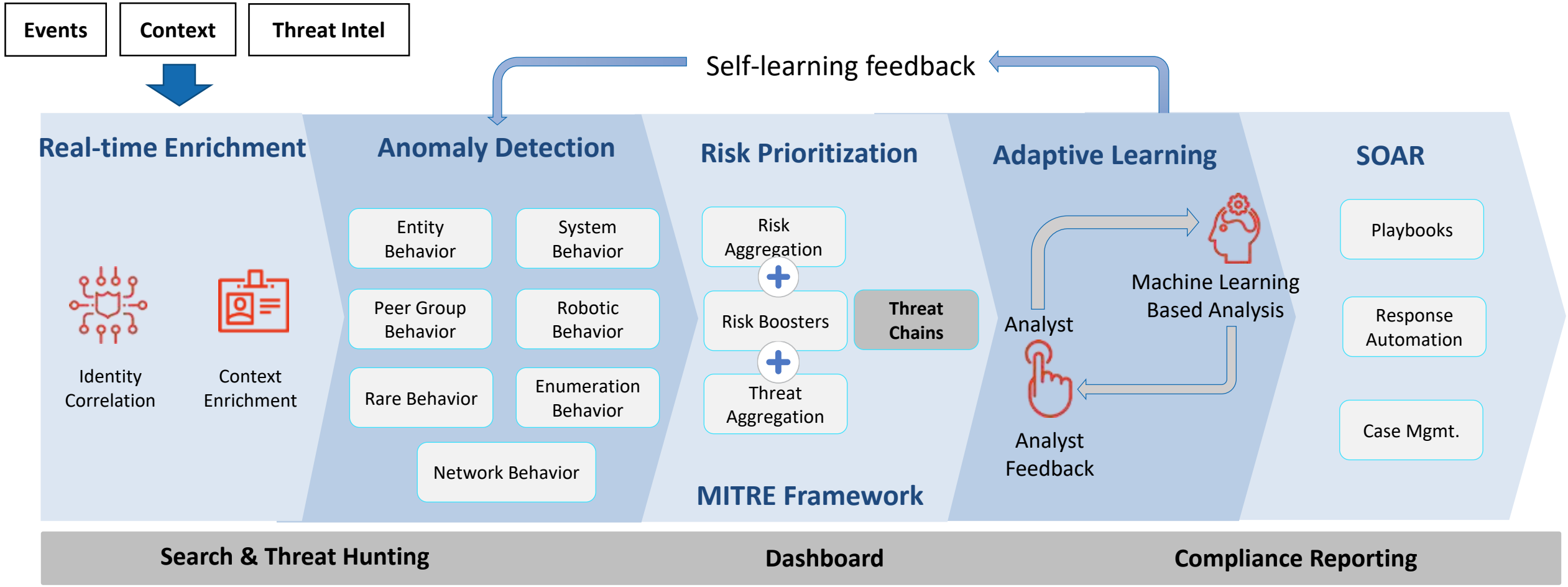


Components of Next-Gen SIEM



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

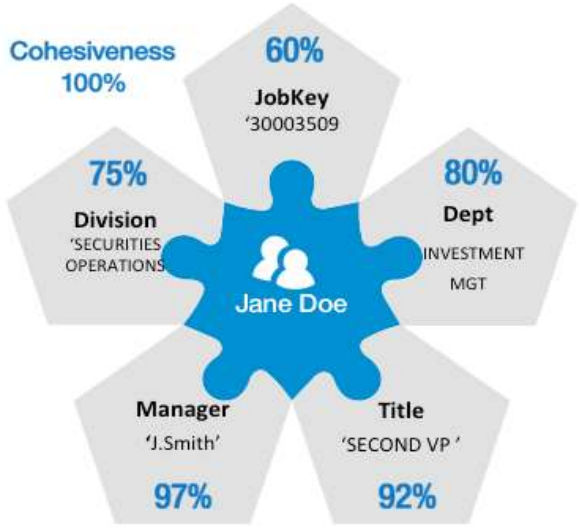
How does it work



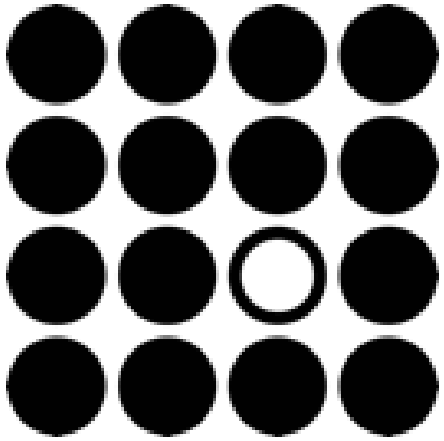
Use Cases

Samples

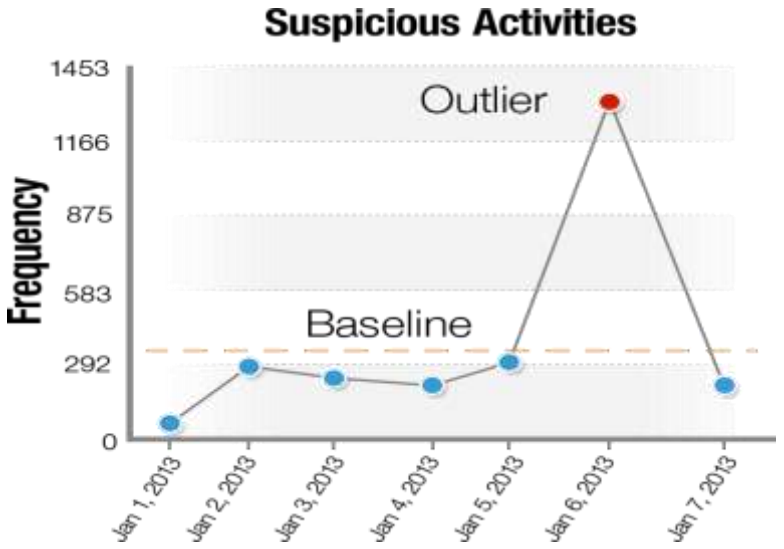
- Patient Data Snooping (EMR)
- IT employee accessing patient records not accessed by peer
- Access patients from unusual location (state/country) never seen before
- Spike in break the glass violations
- Rare outpatient activity when the doctor typically performs only inpatient activity



Geo-location



Rarity



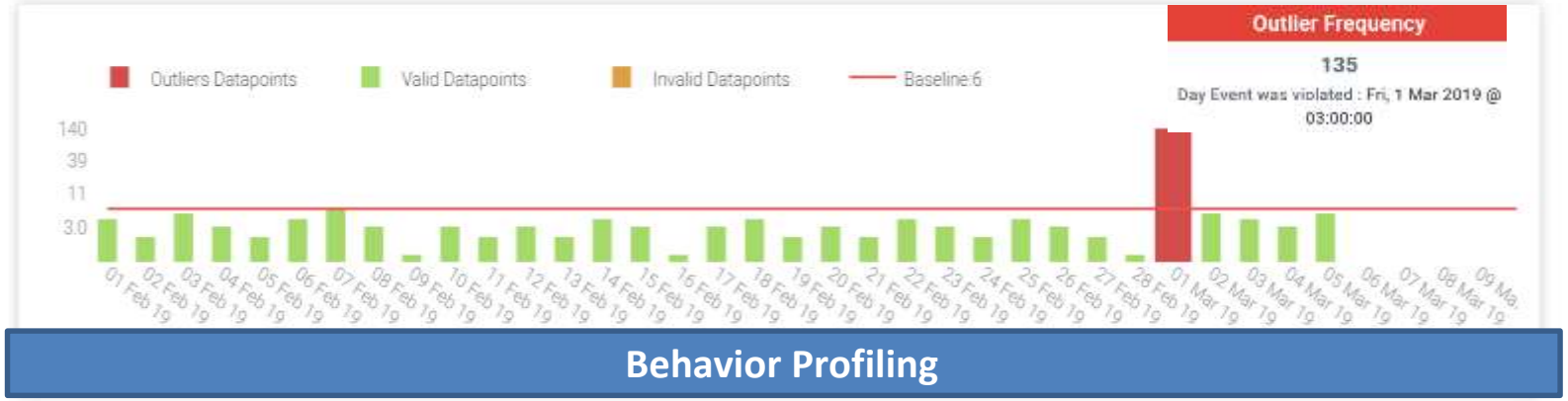
SECURONIX

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

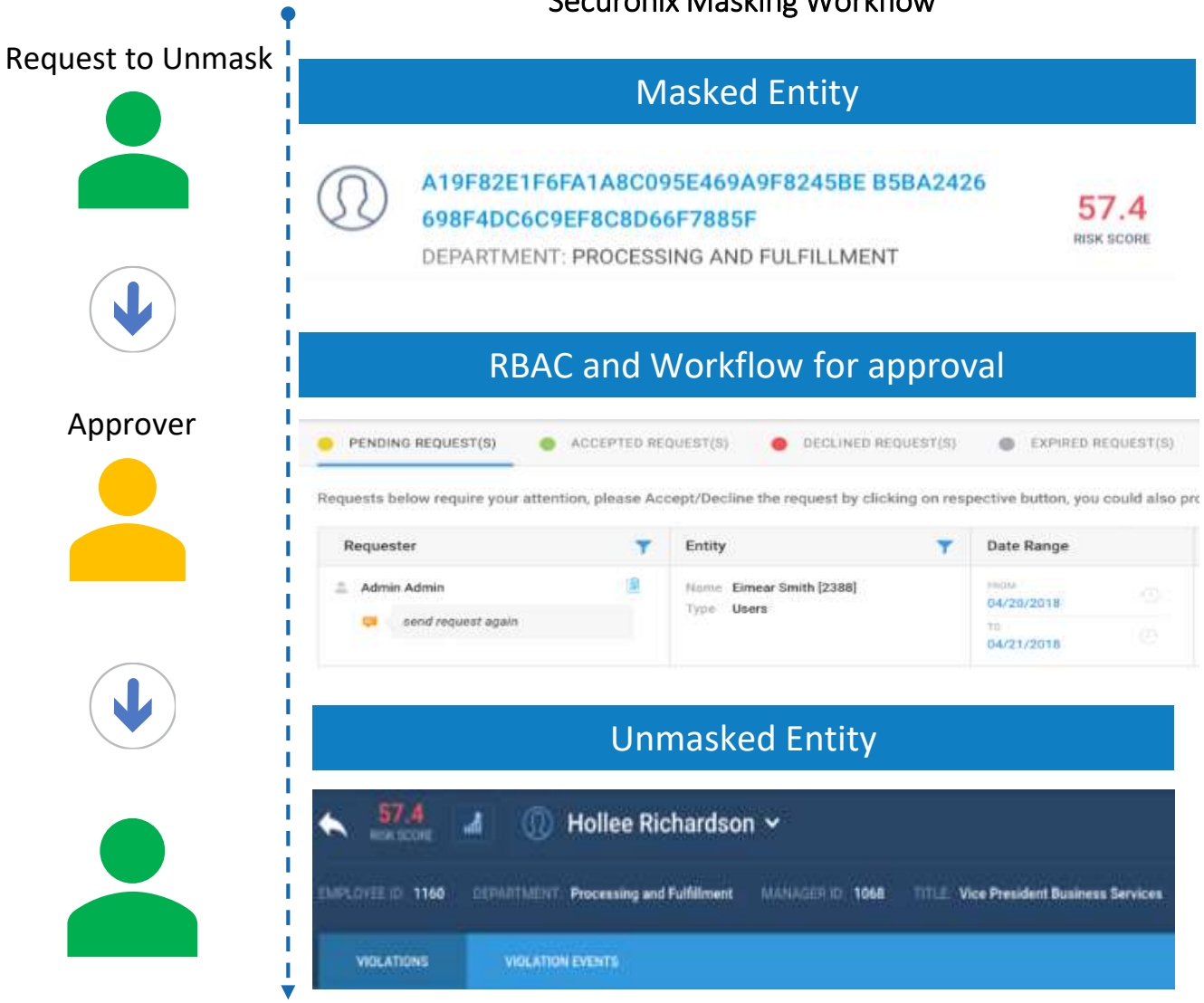
Data privacy can be a key requirement to protect employee privacy and other sensitive data

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

Securonix privacy capabilities include:

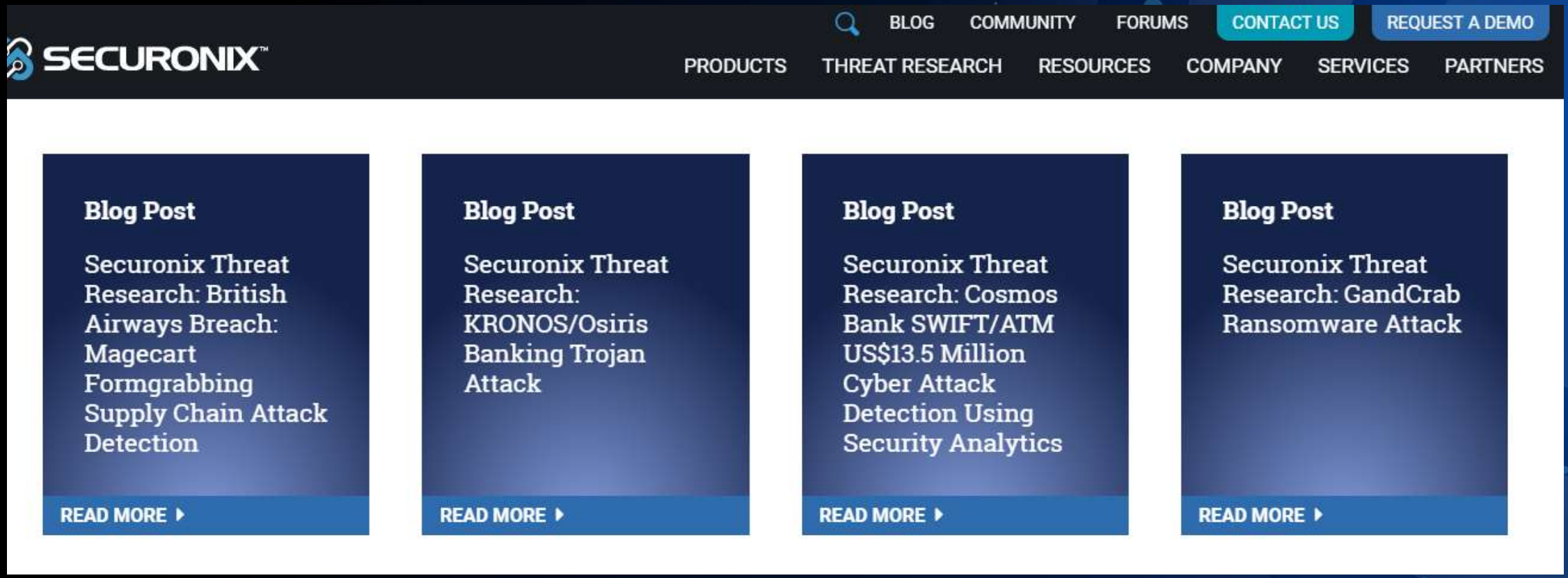
- Data can be anonymized with masking
- Role based access control
- Data filtering or eraser [GDPR requirements]
- Audit trail

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



Securonix Threat Research & Hunt

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



Thank You