
HAY SIEM
PA' TODOS
SNYPR
by Securonix

Muy Caro…

Modelo de Precios

Costo de la Operación

No identifico el Time to Value

Complejo!

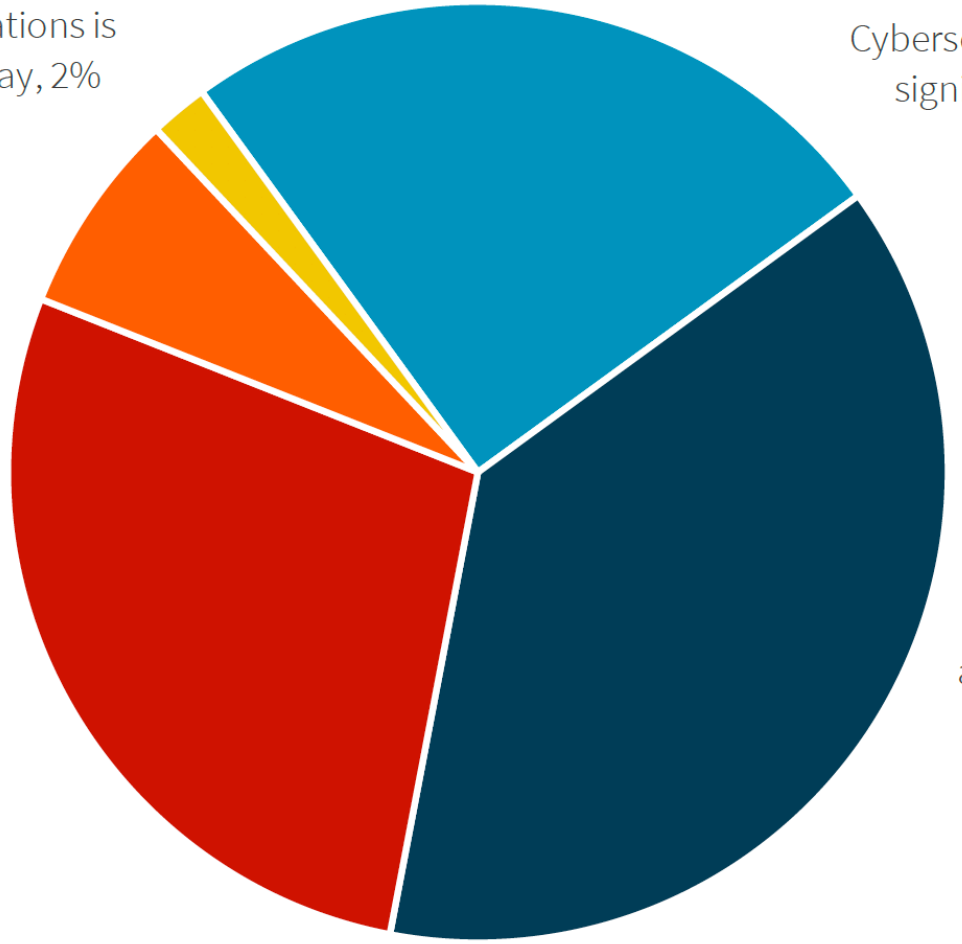
Infraestructura

Mantenimiento

Operación

No le veo la utilidad

Which of the following best describes your opinion about cybersecurity analytics and operations? (Percent of respondents, N=406)

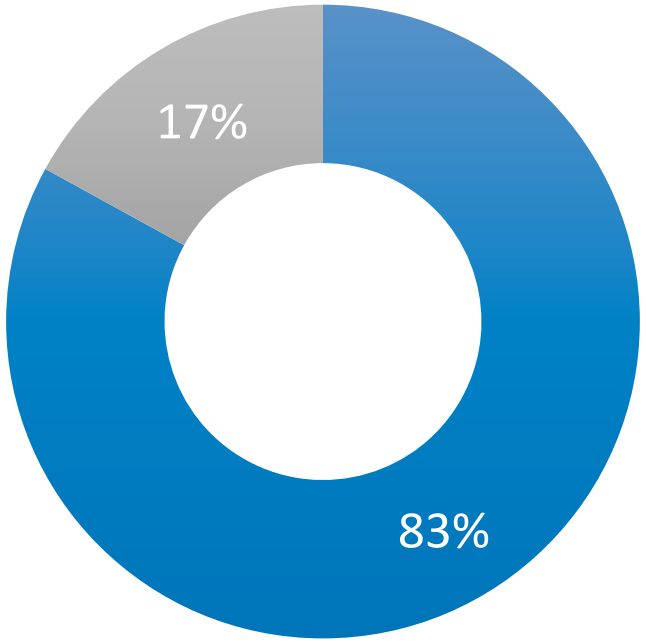


Source: Enterprise Strategy Group

Cifras, datos y hechos

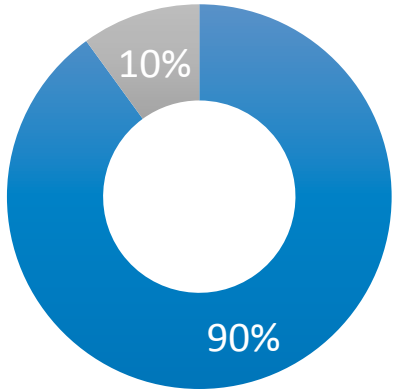
Los atacantes buscan Identidades e Información

Casos de Exfiltración de Datos



Credenciales Legitimas

Otros



Porcentaje de casos con usuarios comprometidos

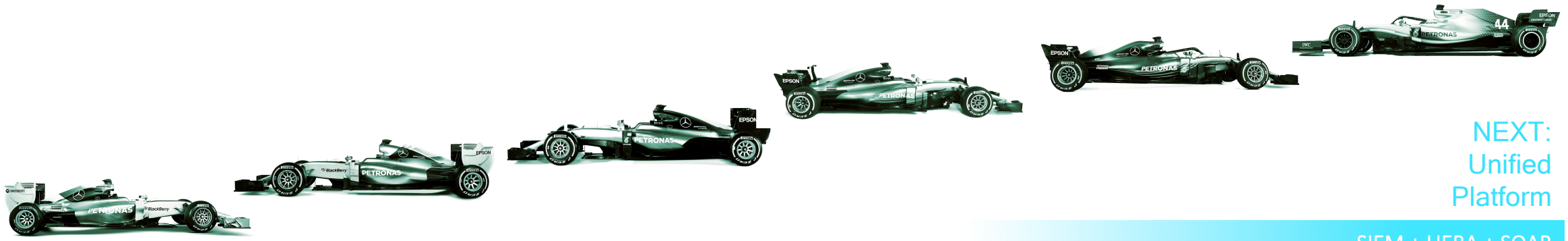
Otros Indicadores

98% de la evidencia de las violaciones investigadas y la actividad de los atacantes está disponible y contenida en los logs de seguridad*

Source: Gartner 2017

SECURONIX

Evolución en las operaciones de Seguridad



NEXT:
Unified
Platform

SIEM + UEBA + SOAR

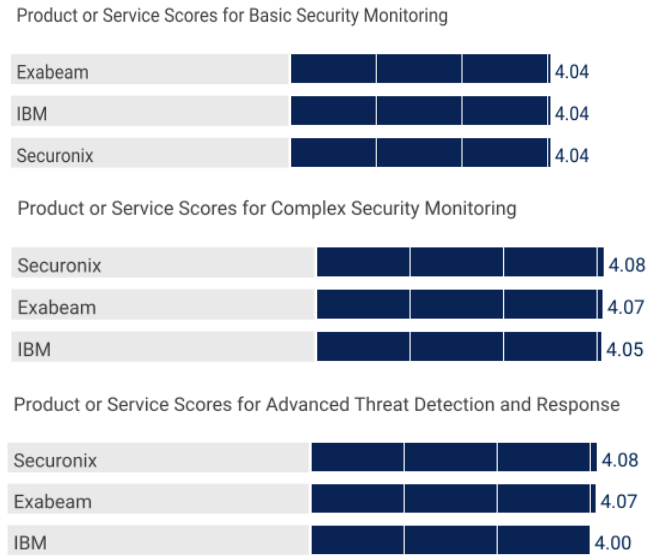
Orchestration & Automation — SOAR

Machine Learning — User & Entity Behavior Analytics

Threat Hunting — Search, Visualizations, Ad-hoc reporting

Tools Alerting — Security Information and Event Management

Logging — Log Management



Source: Gartner (February 2020)

2000	2005	2010	2015	2019

INTELIGENCIA ARTIFICIAL

Un sistema que puede imitar comportamientos inteligentes

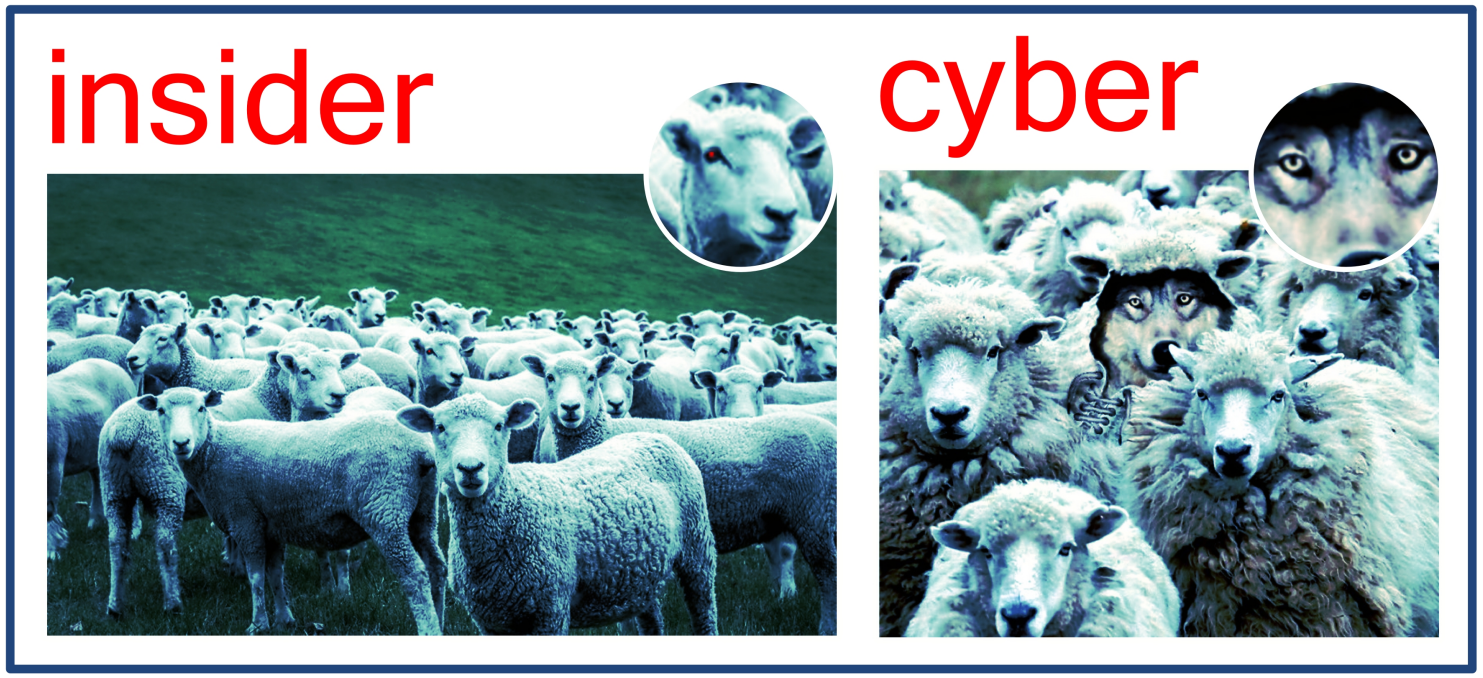
MACHINE LEARNING

Capacidad de aprender - generalización del comportamiento a partir de un conjunto de experiencias

DEEP LEARNING

Aprendizaje en capas - redes neuronales

Detección de ciberamenazas vs amenazas internas



última generación significa:

Automatizar

Mediante el aprendizaje automático

Mejorar

Procesando Millones de eventos en forma simultanea

Modernizar

Madurez: Tecnología + Personas + Procesos

Data Feeds

Customer Cloud

CLOUD CONNECTOR

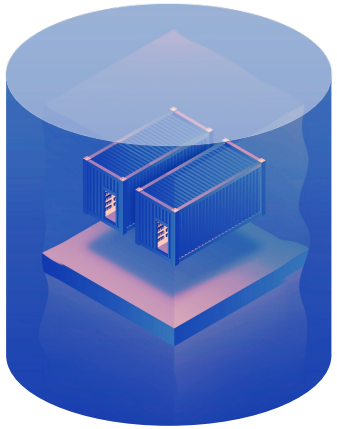
aws

Colector

APP CONNECTOR

SECURONIX API

Customer on-prem



Security Data Lake

Cloud

Analytics

Threat Chains & Risk Scoring

Insider Threat

Cyber Threat

Cloud Security

Fraude

User & Entities Behavior Analytics

SECURONIX

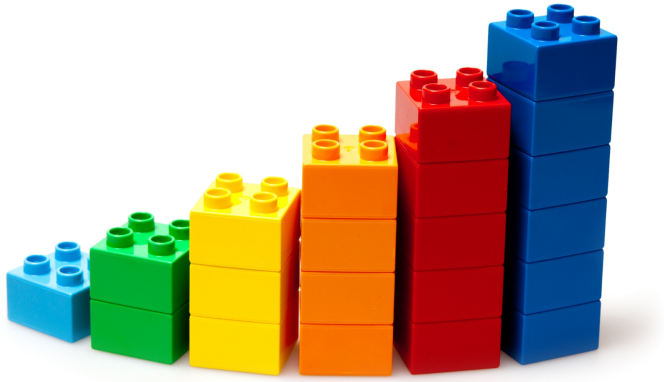
Qué tan Complejo puede ser?

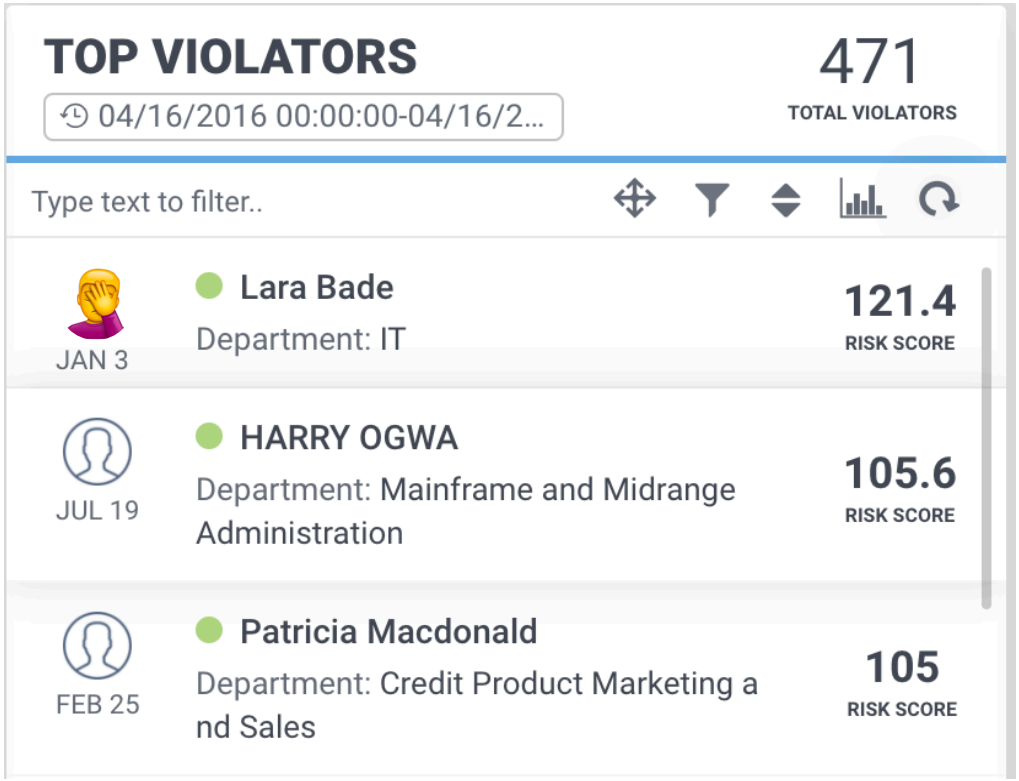
la Data tal
como viene

es clasificada

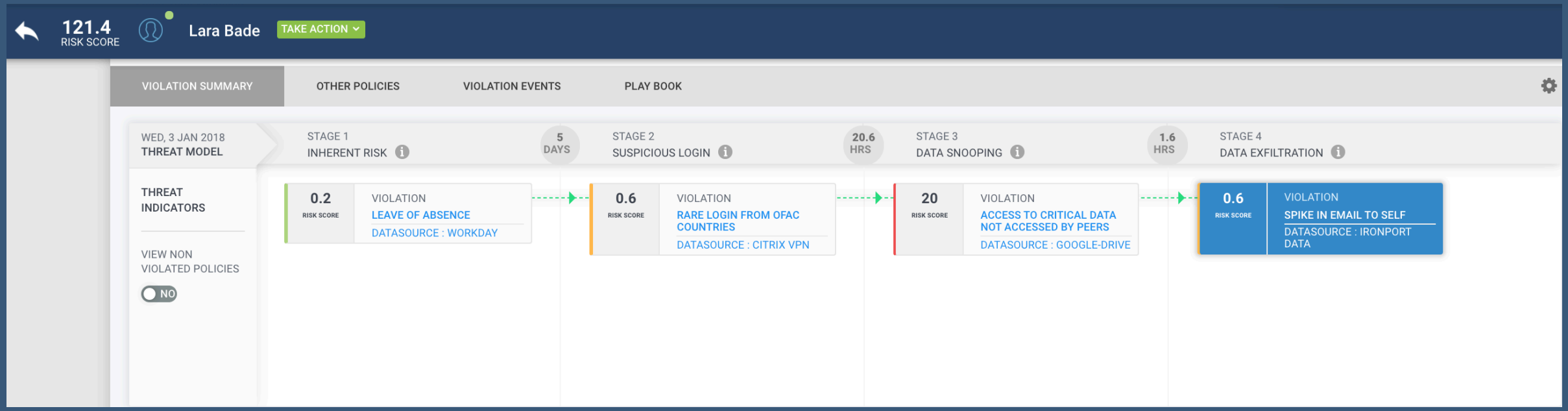
organizada

para entregarla
visualmente presentable





La diferencia entre una alerta y el modelamiento de una amenaza


121.4
RISK SCORE
Lara Bade
TAKE ACTION
VIOLATION SUMMARY
OTHER POLICIES
VIOLATION EVENTS
PLAY BOOK
WED, 3 JAN 2018
THREAT MODEL
STAGE 1
INHERENT RISK
5
DAYS
STAGE 2
SUSPICIOUS LOGIN
20.6
HRS
STAGE 3
DATA SNOOPING
1.6
HRS
STAGE 4
DATA EXFILTRATION
THREAT
INDICATORS
VIEW NON
VIOLATED POLICIES
NO
0.2
RISK SCORE
VIOLATION
LEAVE OF ABSENCE
DATASOURCE : WORKDAY
0.6
RISK SCORE
VIOLATION
RARE LOGIN FROM OFAC
COUNTRIES
DATASOURCE : CITRIX VPN
20
RISK SCORE
VIOLATION
ACCESS TO CRITICAL DATA
NOT ACCESSED BY PEERS
DATASOURCE : GOOGLE-DRIVE
0.6
RISK SCORE
VIOLATION
SPIKE IN EMAIL TO SELF
DATASOURCE : IRONPORT
DATA

La importancia de unificar y estructurar los datos antes de...

0.6
RISK SCORE

SPIKE IN EMAIL TO SELF [RESOURCE GROUP: IRONPORT DATA | ACCOUNT: LARA.BADE]

filename	emailrecipientdomain	accountname	emailsubject	emailrecipient	emailsender
18	1	1	16	1	1

Outlier Details

Datapoints Analyzed for Cluster Formation : 53
Last generation time : Wed, 3 Jan 2018 @ 18:37:35

Transactions message:Send mail

Baseline used for outlier

10

5 x Deviation From Baseline

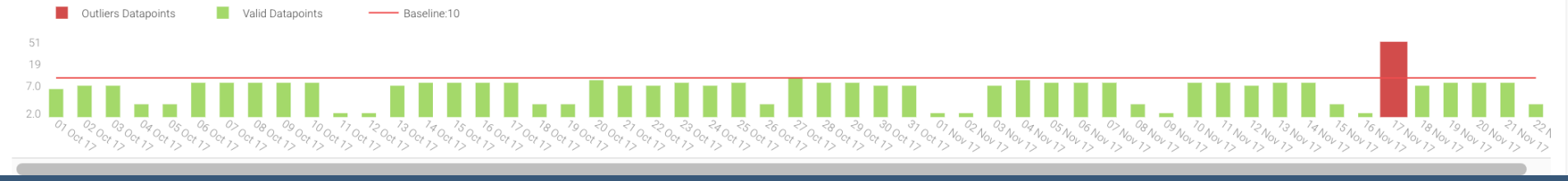
Outlier Frequency

52

Day Event was violated : Fri, 17 Nov 2017 @ 01:00:00

Behavior Profile Details - Emails sent to Personal Email Address

The below graph represents current behavior details. The count of a datapoint(Bar in graph) may be different than count of the outlier. This happens when we have New incoming data for the datapoint after the behavior outlier has been flagged.



Showing behavior profile for EmailtoSelfBaseline

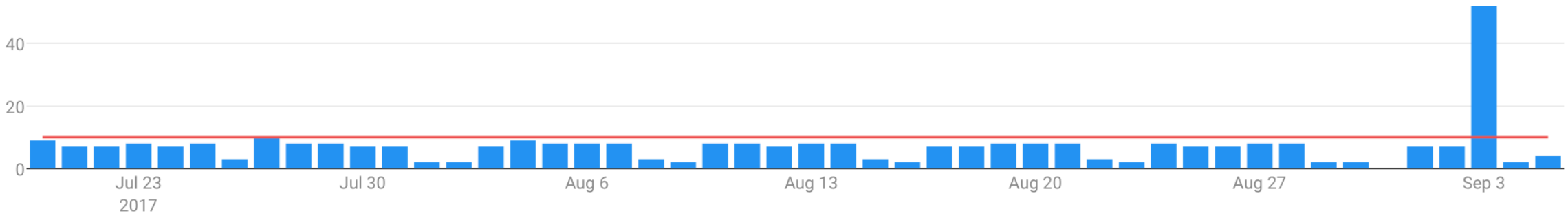
Type Account Names | Resources Ironport Data | Accounts OGWA.HARRY

View Behaviour For :

DAILY | WEEKLY | MONTHLY | DAY OF WEEK | TIME OF DAY

Transaction - All Attributes

BASELINE	DATA POINT	TOTAL FREQ	AVG FREQ	ABSOLUTE FREQ
10	47	339	7.21	2 min 52 max



Enlaces de interés:


Securonix Security Operations & Analytics Platform

Cloud-native Analytics-driven SIEM with Efficient Collection, Detection, and Response

https://www.securonix.com/resources/esg-technical-and-economic-validation/


Critical Capabilities for Security Information and Event Management

https://www.securonix.com/resources/gartner-critical-capabilities-for-security-information-and-event-management-2020/

https://www.securonix.com/resources/2020-gartner-magic-quadrant-for-siem/