VARONIS DBTRONIX

Threat Detection ana Response with Data Analytics and Machine Learning

April 2020

How do we do it?

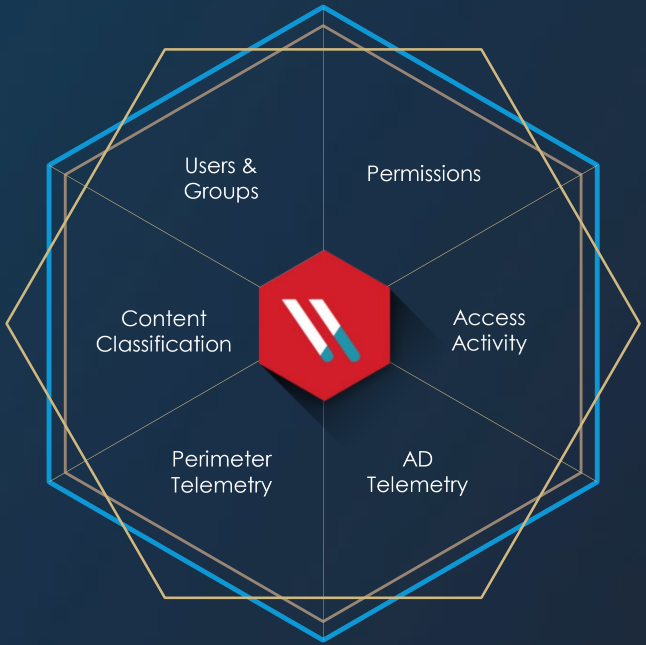
DBTRONIX VARONIS

Varonis Data Security Platform

ENTERPRISE DATA STORES AND INFRASTRUCTURE

- Windows
- Office 365
- Exchange
- Unix/Linux
- SharePoint
- NAS
- Box
- Directory Services
- Edge Services

DATA ANALYTICS & AUTOMATION



Users & Groups

Permissions

Content Classification

Access Activity

Perimeter Telemetry

AD Telemetry

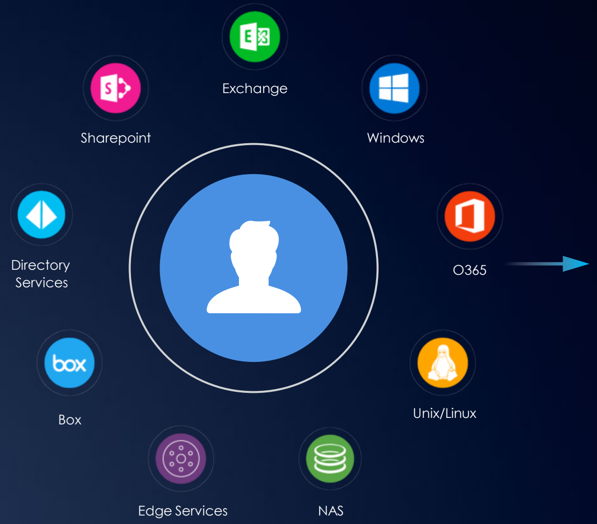
USE CASES

- DATA PROTECTION
- COMPLIANCE
- THREAT DETECTION & RESPONSE

DBTRONIX VARONIS

Collect Enrich Learn Alert

Varonis **collects billions of events** from the right data sources, unobtrusively, and without endpoint agents



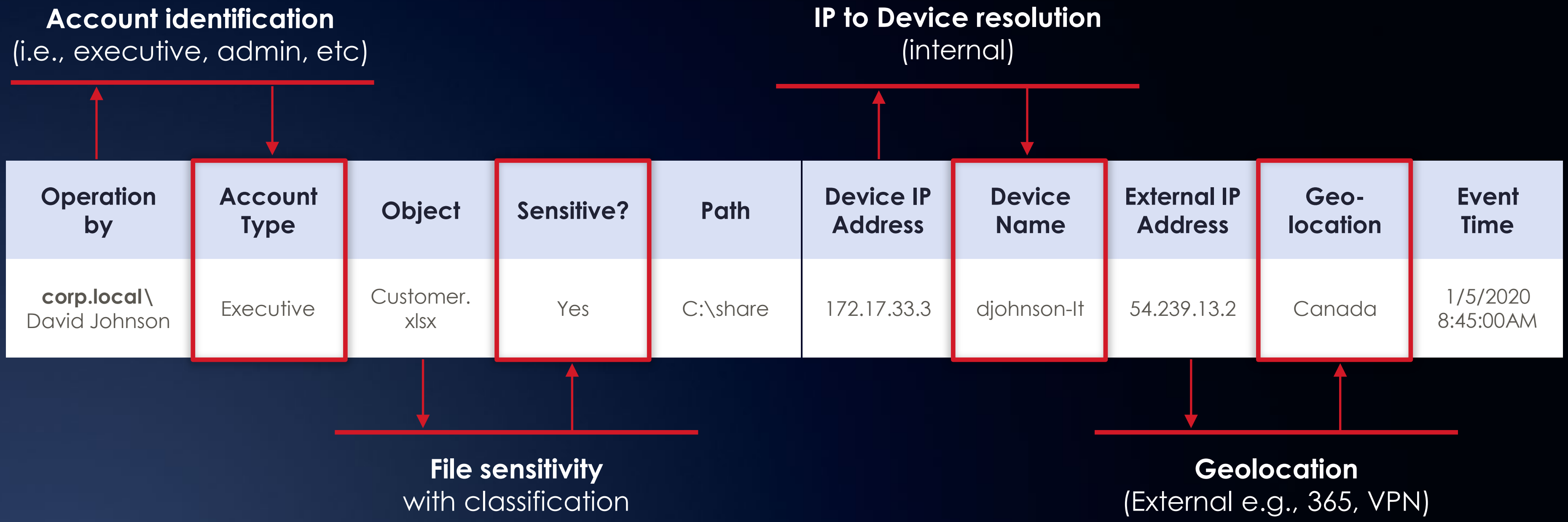
- Data access events
- VPN/Cloud connections
- Authentication events, DNS, and web connections

But they're clean events

Operation by	Object	Path	Device IP Address	External IP Address	Event Time
corp.local\ David Johnson	Customer.xlsx	C:\share	172.17.33.3	54.239.13.2	1/5/2020 8:45:00AM

Collect **Enrich** Learn Alert

Then, we **combine** and **enrich** them



Account identification
(i.e., executive, admin, etc)

IP to Device resolution
(internal)

Operation by	Account Type	Object	Sensitive?	Path	Device IP Address	Device Name	External IP Address	Geo-location	Event Time
corp.local\ David Johnson	Executive	Customer.xlsx	Yes	C:\share	172.17.33.3	djohnson-lt	54.239.13.2	Canada	1/5/2020 8:45:00AM

File sensitivity
with classification

Geolocation
(External e.g., 365, VPN)

DBTRONIX

Collect | Enrich | **Learn** | Alert

And use AI to **learn** behavioral baselines and profiles

David Johnson

- ✓ This person is an **executive**
- ✓ Usually works from **“David’s device”**
- ✓ Usually logs in from an IP address **based in the US**
- ✓ David’s peers
- ✓ **Doesn’t usually access customer data** (but has access)
- ✓ David’s active and idle data

Collect | Enrich | Learn | **Alert**

Our Threat Models **alert** on **meaningful** deviations

✓

David Johnson

- ✓ This person is an **executive**
- ✓ Usually works from **“David’s device”**
- ✓ Usually logs in from an IP address **based in the US**
- ✓ David’s peers
- ✓ David’s active and idle data
- ✓ Typical working hours 8am-6pm EST

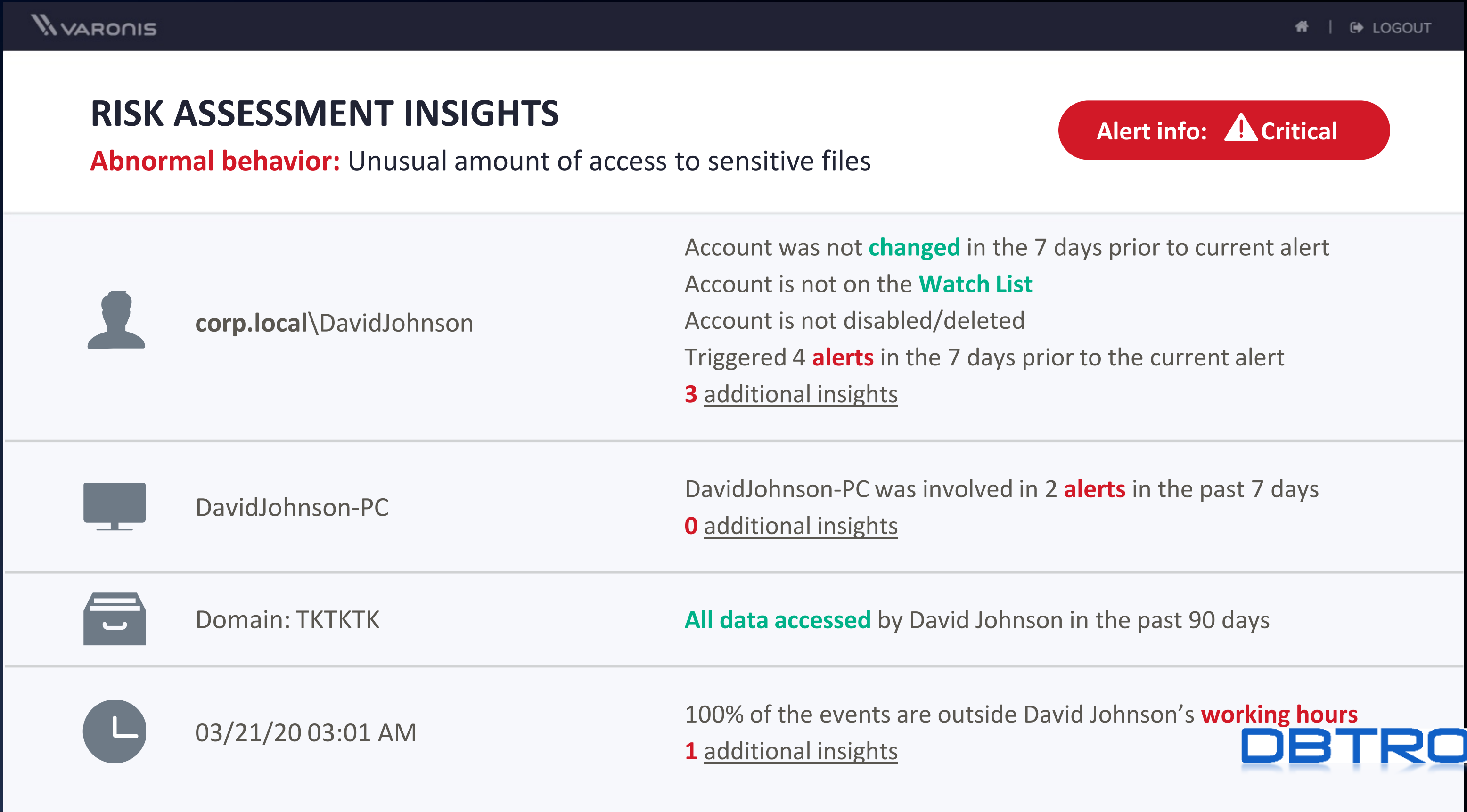
✗

Person logging in as David Johnson

- ✓ This person is an **executive**
- ✗ From a **device associated with another user**
- ✗ From an **atypical geolocation**
- ✗ Behaving **unlike his peers**
- ✗ Accessing data that **he doesn’t typically access**
- ✓ During working hours

DBTRONIX

Investigations are **quick** and **conclusive**

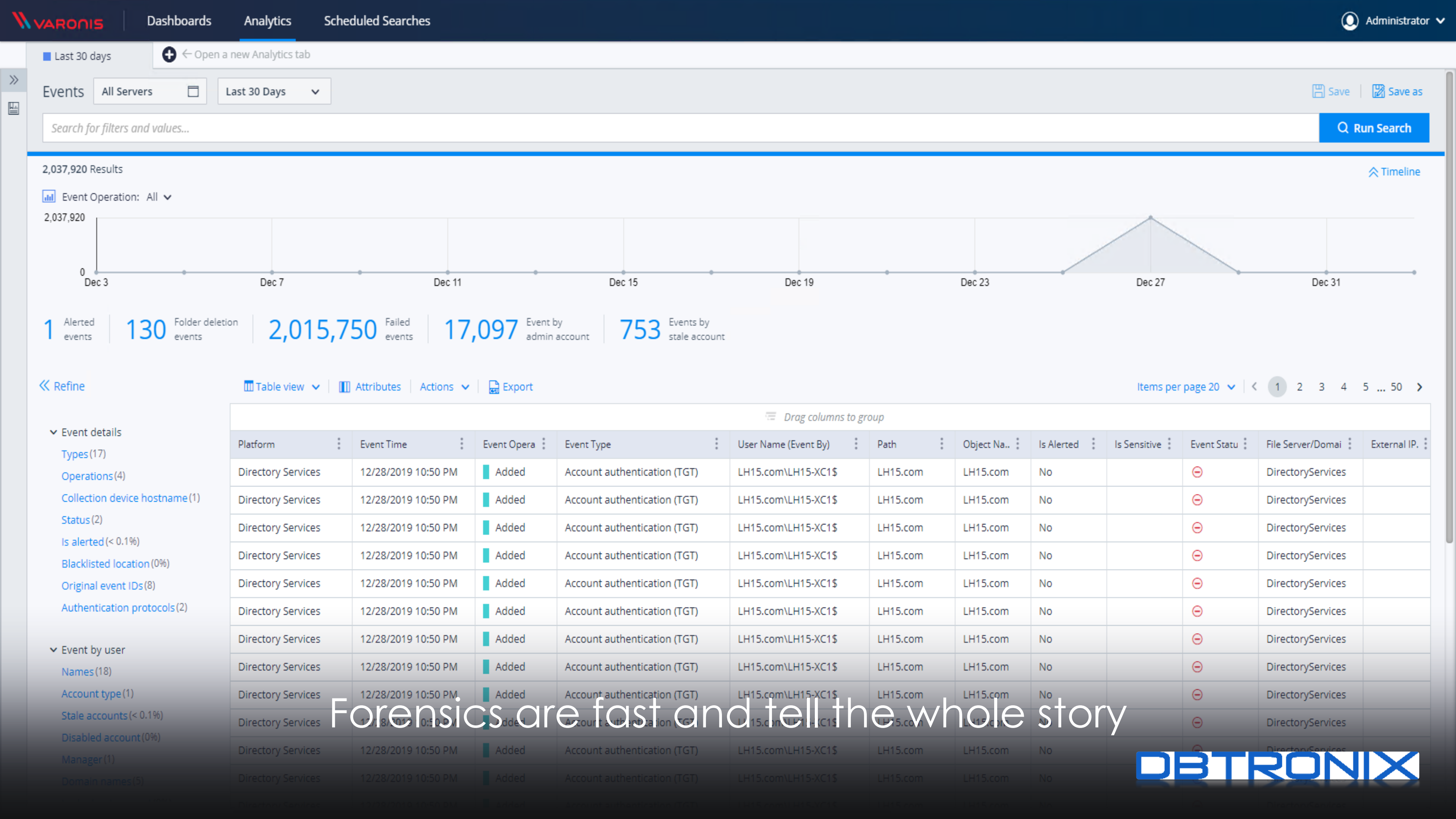


RISK ASSESSMENT INSIGHTS

Abnormal behavior: Unusual amount of access to sensitive files

Alert info: ⚠ Critical

corp.local\DavidJohnson	Account was not **changed** in the 7 days prior to current alert Account is not on the **Watch List** Account is not disabled/deleted Triggered 4 **alerts** in the 7 days prior to the current alert **3** additional insights
DavidJohnson-PC	DavidJohnson-PC was involved in 2 **alerts** in the past 7 days **0** additional insights
Domain: TKTKTK	**All data accessed** by David Johnson in the past 90 days
03/21/20 03:01 AM	100% of the events are outside David Johnson’s **working hours** **1** additional insights



2,037,920 Results

1 Alerted events | 130 Folder deletion events | 2,015,750 Failed events | 17,097 Event by admin account | 753 Events by stale account

- Event details
  - Types (17)
  - Operations (4)
  - Collection device hostname (1)
  - Status (2)
  - Is alerted (< 0.1%)
  - Blacklisted location (0%)
  - Original event IDs (8)
  - Authentication protocols (2)
- Event by user
  - Names (18)
  - Account type (1)
  - Stale accounts (< 0.1%)
  - Disabled account (0%)
  - Manager (1)
  - Domain names (5)

Platform	Event Time	Event Opera	Event Type	User Name (Event By)	Path	Object Na..	Is Alerted	Is Sensitive	Event Statu	File Server/Domai	External IP.
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	
Directory Services	12/28/2019 10:50 PM	Added	Account authentication (TGT)	LH15.com\LH15-XC1$	LH15.com	LH15.com	No		⊖	DirectoryServices	

Forensics are fast and tell the whole story

DBTRONIX

Thank You

Arthur Yeung
SE Manager, APAC
info@dbtronix.com.hk or 21558000

DBTRONIX

VARONIS