

# AI-POWERED EDR: STREAMLINING BLACKBERRY CYBERSECURITY WITH DATABRICKS



Justin Lai – Distinguish Data Architect  
Robert Lombardi – Director of Product Management  
Digan Parikh – Sr. Solution Architect (Databricks)



# Challenges in Cybersecurity

## 4 common challenges in Cybersecurity operations



Cost



Scale



ML & AI



Centralization

# Databricks Vision for Cybersecurity

Databricks for Long-Term Storage + Analytics integrating with other tools like SIEMs & SOARs



Operations

SIEM

SOAR



Engineering

Intel



Risk & Compliance

Fraud, AML,  
Insider Threat

Fusion  
Analytics

Databricks Data Intelligence Platform



Data Sources

OS

(Windows, Linux)

Security

(XDR, Antivirus)

Agent

(Antivirus, DLP)

Network

(IPS, Sandbox)

PaaS/SaaS

(CSP, SSO, AD)

# ROBERT LOMBARDI

## Director of Product Management



- Started as an Engineer @ BB in 2009
  - Platform & Product Design
  - Advanced Technology & Research
- Transitioned to Product Management in 2017
  - Consumer Security Applications for Mobile
  - Launch of Protect Mobile (MTD)
  - Cylance Console Platform
  - CylanceOPTICS
  - CylanceENDPOINT

# JUSTIN LAI

## Distinguished Data Architect



- Started at BlackBerry 2010
- Worked in the security field for the past 12 years
- Data Platform Team for over 4 years
- Second time presenting at DAIS

# BLACKBERRY CYLANCE

## Cybersecurity Portfolio Overview



### CylancePROTECT (EPP)

- Best-in-class Antimalware AI
- Attack Surface Reduction
- Exploit Prevention



### CylanceOPTICS (EDR)

- MITRE ATT&CK
- Telemetry Capture & Context
- Incident Response



### CylanceGATEWAY (ZTNA)

- Secure Network Communications
- Network Detection & Response
- Content Filtering & Firewalling



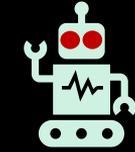
### CylanceMDR

- Managed Detection & Response
- Managed Threat Hunting
- Environment Tuning
- Secure Critical Communications
- Incident Response
- Digital Forensics
- XDR Enabled

# OPPORTUNITIES



Alert fatigue



Fear of AI



Not enough resources



Security complexity



Not the right resources



Evolving threat landscape

# DESIRED OUTCOMES

Reduce the burden and need to perform monotonous high friction tasks so that customers can take remediation steps confidently and efficiently

Support & enable customers to leverage AI where needed and gradually grow confidence in the system with transparency

Enable upskilling security operations centers of all sizes by providing clear context & guidance throughout the response workflow

Provide focus and clarity to end users so that they can spend their very limited time on high value tasks

# CYLANCE AI

Innovation in *Predictive & Generative AI*

Threat Prevention

SOC Assistant

Kill-chain  
Summarization

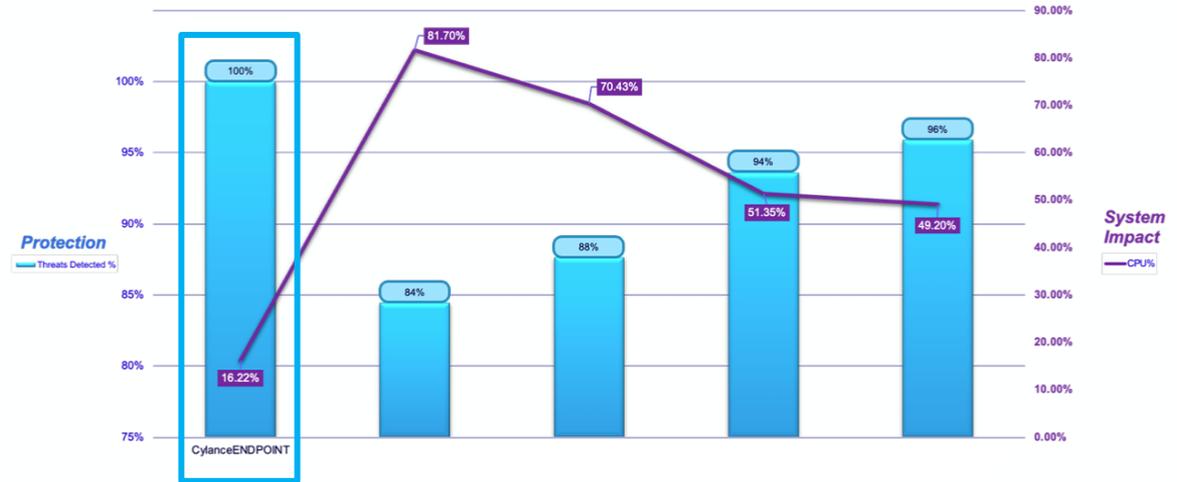
AI-Assisted FP  
Handling

Automated Tuning

Adaptive Policy

Incident Generation

**Windows 10 Endpoint Protection Efficacy & CPU Utilization**  
Scanning A Collection of 1,000 Recent Virus Samples - Composite of Offline & Online Scans  
(Detection % determined by number of files remaining in folder after scan)



Note: Scan is triggered by system decompressing a password-protected "zip" file containing 1,000 malware samples sourced from a major public source. Same sample set used for each solution. Higher detection and lower CPU utilization are the better results. CPU utilization was averaged across the duration of the scan.

Source: Tolly, January 2024

Figure 1

# CYLANCE AI

## Innovation in Predictive & Generative AI

Threat Prevention

SOC Assistant

Kill-chain  
Summarization

AI-Assisted FP  
Handling

Automated Tuning

Adaptive Policy

Incident Generation

← Alerts > GUARD: UAC Bypass via Fodhelper.exe Registry Exploit

Overview

**ALERT SUMMARY**

Priority: **HIGH**

Description: GUARD: UAC Bypass via Fodhelper.exe Registry Exploit

Classification: TA0004 Privilege Escalation, TA0005 Defense Evasion

Sub-classification: T1548 Abuse Elevation Control Mechanism, T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control

Product: CylanceOPTICS

ID	STATUS	Source
5f7b21df-0c15-4ba6-9...	NEW	TTLSE-ST-6G15
c8295e26-921b-4e37-...	NEW	TTLSE-ST-6G15

Cylance AI

Summary analysis:  
**GUARD: UAC Bypass via Fodhelper.exe Registry Exploit**

Here is a summary of the alert "GUARD: UAC Bypass via Fodhelper.exe Registry Exploit" detected by CylanceOPTICS:

Fodhelper.exe is a legitimate Windows file that is used to manage font files. However, it has been exploited by threat actors to bypass User Account Control (UAC) on Windows systems. UAC is a security mechanism introduced in Windows Vista and later to help prevent unauthorized changes to the operating system. It requires users to provide explicit consent before an administrator can make potentially harmful changes.

This exploit takes advantage of a weakness in how Fodhelper.exe interacts with the registry. By default, it runs with elevated privileges even when called from a limited context user. Threat actors can craft a malicious .fon font file that contains executable code and registry modifications. When opened by Fodhelper.exe, this code would silently make changes to elevation settings in the registry without triggering the UAC consent prompt.

This effectively bypasses UAC and allows the actor's code to run with full administrative privileges, even if the current user account does not have them. From here, the compromise can escalate further through installation of malware, credential theft, lateral movement and more.

Some recommended mitigations include hardening UAC settings to always prompt for consent, applying the latest patches to Fodhelper.exe to fix the exploited vulnerability, and monitoring for unusual modifications to registry keys related to process elevation. Endpoint detection and response tools like CylanceOPTICS can also help identify suspicious activity indicative of this exploit technique. Early detection is important as it can prevent adversaries from fully compromising systems and establishing persistence.

In summary, this alert warns of a UAC bypass method using a legitimate Windows binary and registry modifications to silently elevate privileges without consent. Strong access controls, patching, and monitoring are prudent precautions against this and similar privilege escalation attacks.

# CYLANCE AI

## Innovation in Predictive & Generative AI

Threat Prevention

SOC Assistant

Kill-chain  
Summarization

AI-Assisted FP  
Handling

Automated Tuning

Adaptive Policy

Incident Generation

The screenshot displays the Cylance AI security dashboard for a suspected APT41 intrusion. The main incident summary is highlighted with a blue box and contains the following text:

**Incident summary**

Our analysts have detected a series of suspicious events that appear to be related to an intrusion by APT41, a Chinese state-sponsored threat group known for cyber espionage. The alerts indicate the threat actor gained an initial foothold via a spearphishing email containing a malicious attachment. They then used base64-encoded PowerShell to download additional payloads, including a remote access trojan (RAT) that establishes reverse TCP connections for command and control. The RAT allows the actor to execute arbitrary commands and scripts on the infected system, including through PowerShell. Their goal is likely long-term access for network reconnaissance and data exfiltration.

Key indicators observed in the alerts align with APT41's typical tactics, such as abusing legitimate administration tools like Powershell for lateral movement and privilege escalation (T1047, T1068, T1086). The RAT and use of reverse TCP connections also correlate to APT41's custom malware arsenal and preference for C2 over encrypted channels (T1219).

**Alerts**

DEVICES	C...	P...	CLASSIFICATION	SUB-CLASSIFICA...	DESCRIPTION
SE-STATIC-4G-39	7	1	Execution TA0002	Command and S...	Suspicious Base64 Encoded Powersh
DEVICE_02	4	1	Command and c...	Ingress tool tran...	Powershell Download Command Exe
		1	Threat	Malware-Trojan	Remote Access Trojan Malware
		2	Command and c...	Ingress tool tran...	Powershell Download Command Exe
		3	Execution	Command and S...	Powershell Command Execution wif
		2	Network		Reverse TCP Connection Established
		2	Network	Signature detect...	Reverse TCP Connection Established

**Actions to resolve**

1 of 3 actions completed

- ✓ Lock device  
SE-STATIC-4G-39  
DEVICE\_02  
Completed by FirstLastname on 2023-09-01
- ⚠ Block any or all IP/Domains in the payload URL  
185.199.110.133  
20.05.110.133  
PENDING ACTION BY GUARD
- Quarantine file  
...Local/Temp/pwnd.exe  
...Local/Temp/fohelper.exe  
UNABLE TO RESOLVE

**Kill-chain diagram:** A flowchart showing the progression of the attack. It starts with a 'Spearphishing' node leading to 'Initial Foothold' (PowerShell), which then branches into 'Command and Control' (RAT), 'Malware Execution' (Trojan), and 'Reverse TCP Connection'. The RAT node further leads to 'Remote Access Trojan Malware' and 'PowerShell Command Execution'. The diagram is also highlighted with a blue box.

# CYLANCE AI

Innovation in *Predictive & Generative AI*

Threat Prevention

SOC Assistant

Kill-chain  
Summarization

AI-Assisted FP  
Handling

Automated Tuning

Adaptive Policy

Incident Generation



## Alerts

+ ADD EXCEPTION

PRIORITY STATUS

PRIORITY	STATUS
HIGH	New
HIGH	New
HIGH	New
MEDIUM	New
HIGH	New
HIGH	New

### Add exception

Settings Applied To

Alert description  
Browser Credential Theft

Name \*  
Exception for browser credential theft

Description

#### CONDITIONS

AND	Instigating Process	Name	browser.exe
AND	Instigating Process	Path	c:\program files\browser\browser.exe
AND	Instigating Process	SHA256	f1f98021dc799357a4466583180a

### Add exception

Settings Applied To

Specify the applied scope of the exception.

- Apply to \*
- Tenant
- Affected zones only
- Affected devices only
- Custom

Win Service Execution Mitre T1569

Win Impair Defence Services Mitre T1562

Win Powershell DownloadFile T1059

2.65k

46

2.62k

44

2.62k

44

# CYLANCE AI

Innovation in *Predictive & Generative AI*

Threat Prevention

SOC Assistant

Kill-chain  
Summarization

AI-Assisted FP  
Handling

Automated Tuning

**Adaptive Policy**

Incident Generation

Scope A



Scope B



Scope C



Scope D



Scope E



Scope F



# CYLANCE AI

## Innovation in *Predictive & Generative AI*

Threat Prevention

SOC Assistant

Kill-chain  
Summarization

AI-Assisted FP  
Handling

Automated Tuning

Adaptive Policy

Incident Generation

The screenshot displays a security dashboard for a suspected APT41 intrusion. The main title is "Suspected APT41 intrusion utilizing PowerShell for command and control". The incident is categorized as "HIGH" and "IN PROGRESS". The incident summary describes a series of suspicious events related to an intrusion by APT41, a Chinese state-sponsored threat group. The summary mentions that the threat actor gained an initial foothold via a spearphishing email containing a malicious attachment, which then used base64-encoded PowerShell to download additional payloads, including a remote access trojan (RAT) that establishes reverse TCP connections for command and control. The RAT allows the actor to execute arbitrary commands and scripts on the infected system, including through PowerShell. The goal is likely long-term access for network reconnaissance and data exfiltration. Key indicators observed in the alerts align with APT41's typical tactics, such as abusing legitimate administration tools like PowerShell for lateral movement and privilege escalation (T1047, T1068, T1086). The RAT and use of reverse TCP connections also correlate to APT41's custom malware arsenal and preference for C2 over encrypted channels (T1219).

The "Alerts" section shows a table of alerts with the following columns: C..., P..., CLASSIFICATION, SUB-CLASSIFICA..., and DESCRIPTION. The table is highlighted with a blue border.

C...	P...	CLASSIFICATION	SUB-CLASSIFICA...	DESCRIPTION
1	▲	Execution TA0002	Command and S...	Suspicious Base64 Encoded Powersh
1	●	Command and c...	Ingress tool tran...	Powershell Download Command Exe
1	◆	Threat	Malware-Trojan	Remote Access Trojan Malware
2	●	Command and c...	Ingress tool tran...	Powershell Download Command Exe
3	●	Execution	Command and S...	PowerShell Command Execution wif
2	◆	Network		Reverse TCP Connection Established
2	◆	Network	Signature detect...	Reverse TCP Connection Established

The "Actions to resolve" section shows 1 of 3 actions completed. The actions are:

- Lock device (SE-STATIC-4G-39, DEVICE\_02) - Completed by FirstLastname on 2023-09-01
- Block any or all IP/Domains in the payload URL (185.199.110.133, 20.05.110.133) - PENDING ACTION BY GUARD
- Quarantine file (...Local\Temp\pwnd.exe, ...Local\Temp\fdhelper.exe) - UNABLE TO RESOLVE

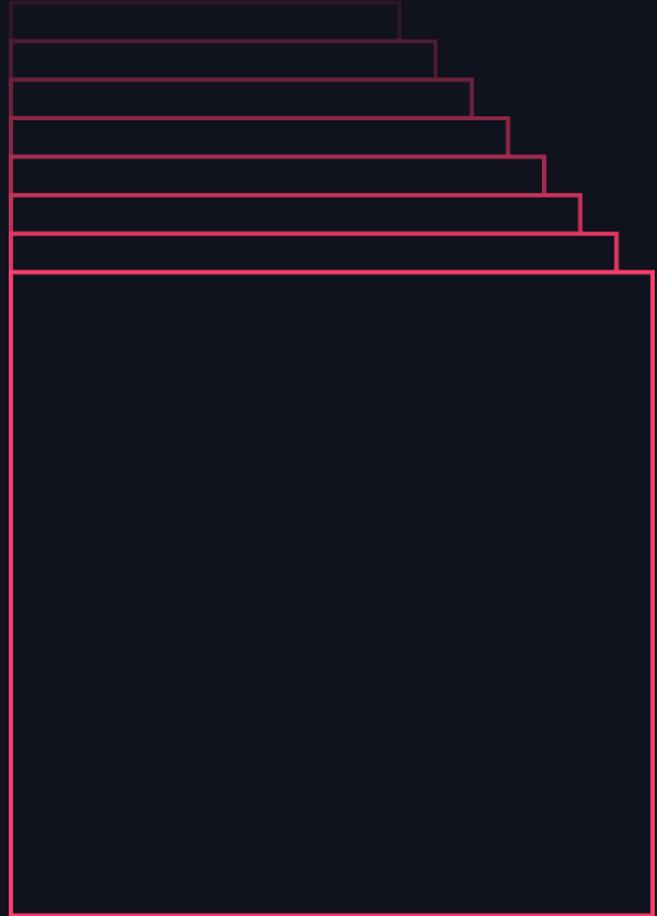
# AGENDA

- High Level Overview
- Leveraging AI in our day to day
- Machine Learning Use Cases
- The Future

# HIGH LEVEL OVERVIEW

---

Data Lake to Lake House to Intelligence Platform



# HIGH LEVEL OVERVIEW

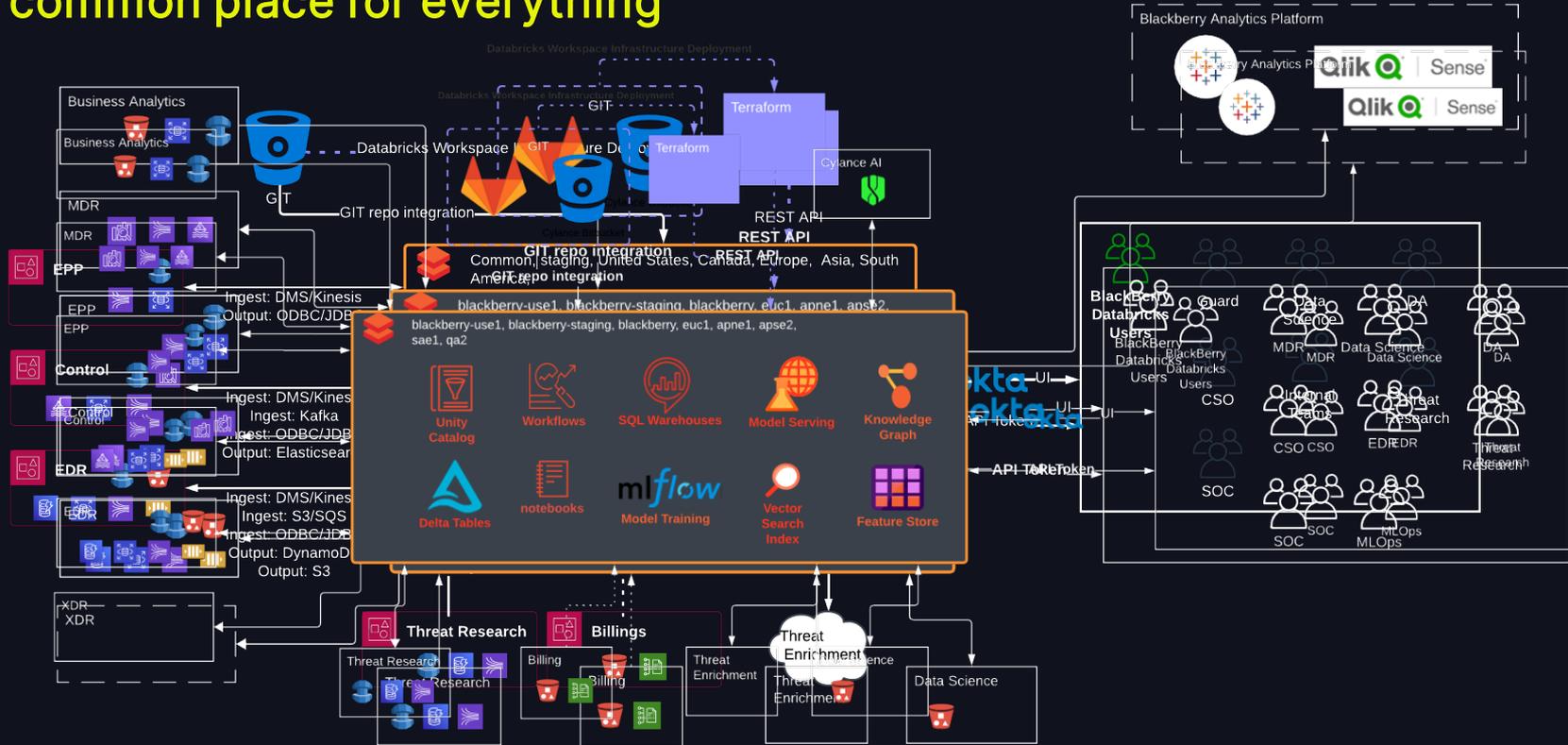
## Data lake to lakehouse to intelligence platform

- Partnered with Databricks to support our EDR Infrastructure
- Built a data lake to support our EDR product
- Built a cybersecurity data lakehouse
- Building a data intelligence platform



# HOW DOES IT LOOK?

## A common place for everything



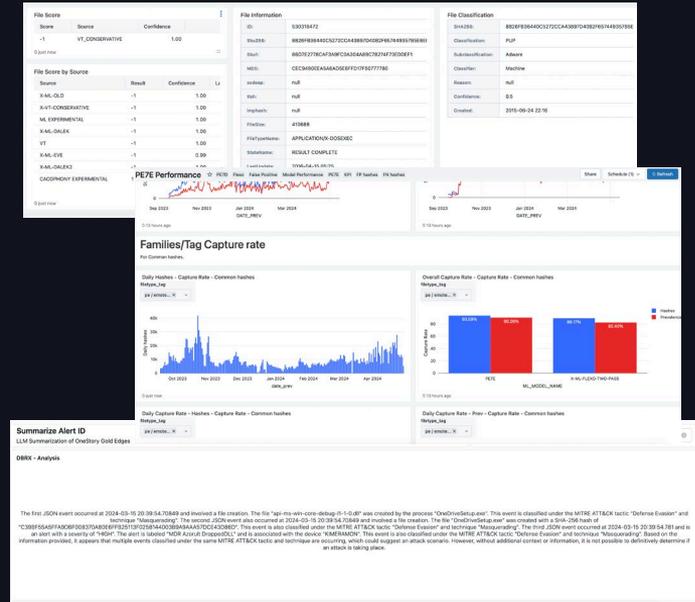
# USE CASES

Data Lake to Lake House to Intelligence Platform

# DASHBOARDING

## USE CASES

- Visualize how our models are performing globally
- Enables collaboration between engineers from different area of speciality
- Low code way to concept up visual elements powered by AI



# AI IS PART OF OUR DAY TO DAY

## Use Case: Inferring Pipeline Status

- Generate Table Aggregates
- Leverage SQL to prep data for LLM to process
- Visualize LLM output in an easy to use format
- Leverage Dashboard inputs to enable interaction with LLM

The screenshot displays a dashboard titled "Pipeline Status Current Date Summary" with a subtitle "Provide live insights into all Guard Detections ingestion Pipelines". A summary text states: "Based on the data, none of the pipelines are overall delayed. The majority of detections in each pipeline have no ingestion delay, with vw\_guarddetectionl\_apse2 at 91.95% and vw\_guarddetectionl\_sae1 at 97.68%".

Below this is the "Ask Data Platform" section, which includes a query input field containing a SQL query to summarize guard pipeline status. The query is:

```
select
concat(
  "For the pipeline ",
  a.view_name,
  ", there are ",
  a.detection,
  " detections with ",
  classification,
  " and represents ",
  string(((a.detection / sum(a.detection) OVER()) * 100),
  "% of total detections."),
CASE
  WHEN classification = "no ingestion delay"
  AND ((a.detection / sum(a.detection) OVER()) * 100 >= 90 THEN "Pipeline is not suffering any delay."
  WHEN classification = "no ingestion delay"
  AND ((a.detection / sum(a.detection) OVER()) * 100 <= 90 THEN "Pipeline is delayed."
  WHEN classification = "ingestion delay"
  AND ((a.detection / sum(a.detection) OVER()) * 100 >= 100 - 90 THEN "Pipeline is delayed."
  WHEN classification = "ingestion delay"
  AND ((a.detection / sum(a.detection) OVER()) * 100 <= 100 - 90 THEN "Pipeline is not delayed."
END
) as summary
```

The dashboard also shows a "Response" section with a text output: "The pipeline 'vw\_guarddetections\_apse2' is not significantly delayed, with 92.03% of detections having no ingestion delay and only 7.97% experiencing delay. The delay-to-no-delay ratio is approximately 1/15." The interface includes input fields for the view name (vw\_guarddetections\_apse2) and the date (May 10, 2024).

# STREAMING EDR MODEL INFERENCE



# STREAMING EDR MODEL INFERENCE

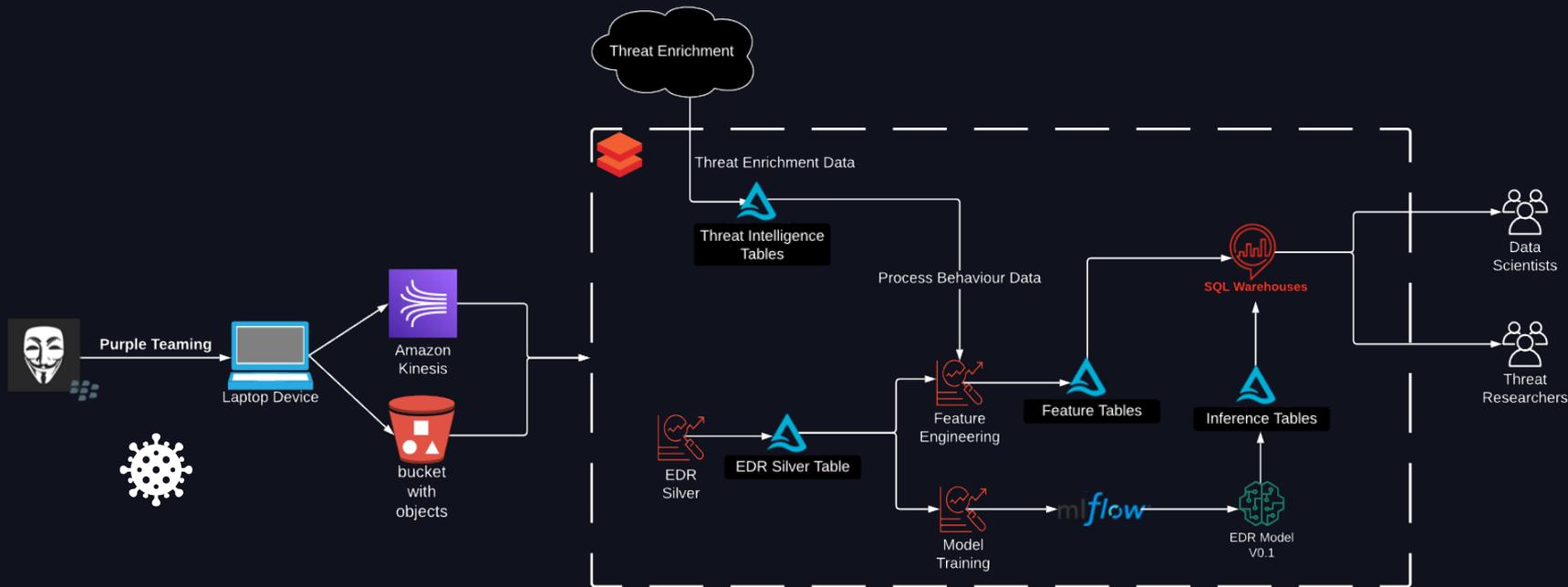
## Putting Telemetry to work

- EDR Telemetry data is noisy
- Over 5 million events a day per tenant
- Model Training with Apache Spark and MLFlow
- Collaborated with Threat Research



# STREAMING EDR MODEL INFERENCE

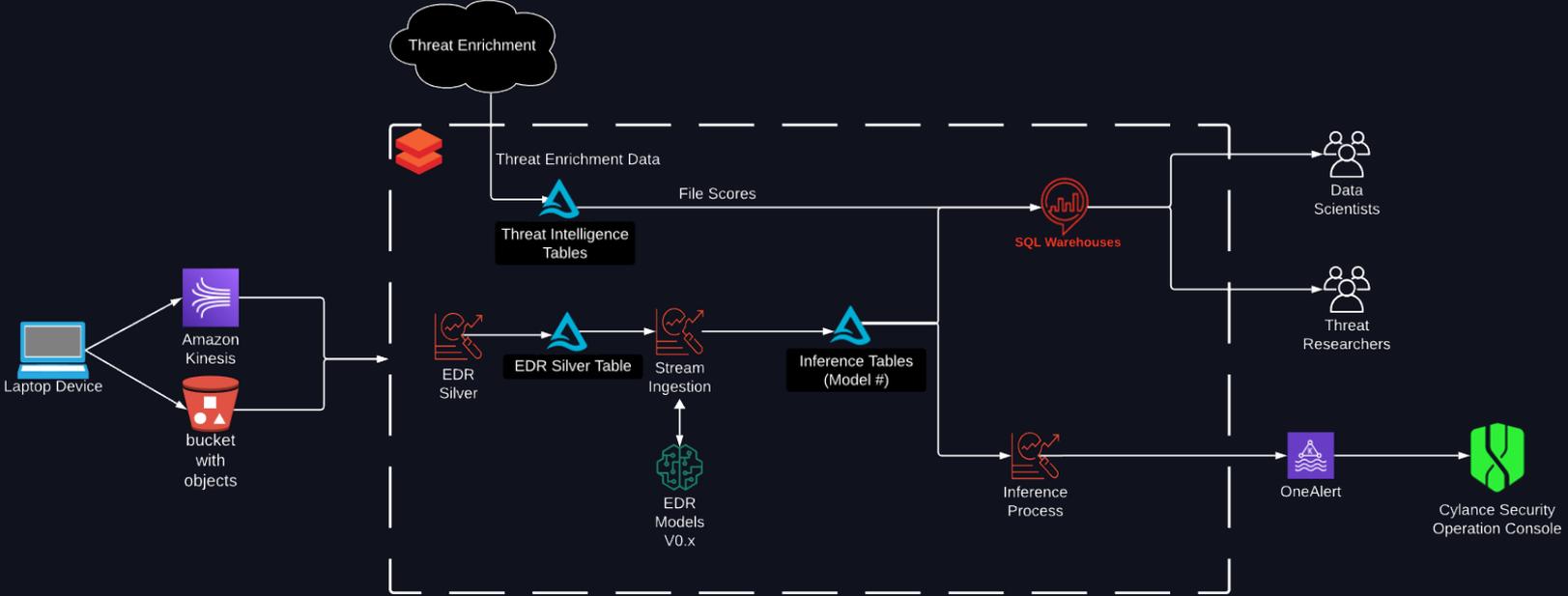
## Model Training





# STREAMING EDR MODEL INFERENCE

## Streaming Model Pipeline



# STREAMING EDR MODEL INFERENCE

## Conclusion

- Dynamic Threat Modeling
- Global Threat Intelligence
- Behavioral Analysis
- Handling Large Volumes of Data

# ALERT PRIORITIZATION



# ALERT PRIORITIZATION

## Problem

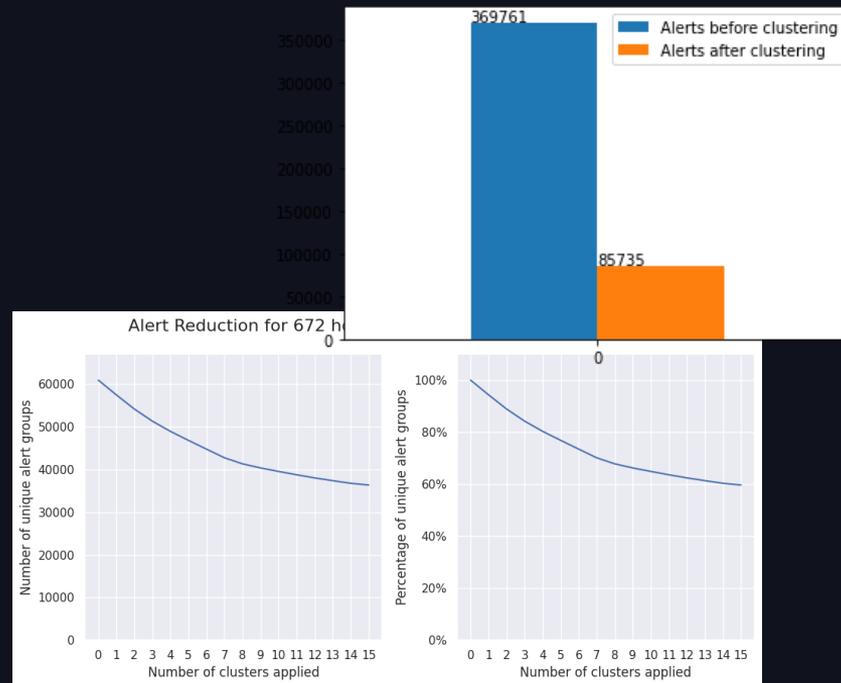
- OneAlert uses *key indicators* (KIs) to determine if an alert is unique, or if it is another occurrence of a previous alert.
- If the KIs are similar, they are counted as unique alerts

Filepath	Command
c: \\windows\\microsoft.net\\framework64\\v4.0.30319\\csc.exe	"C: \\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\csc.exe" /noconfig /fullpaths @"C: \\Windows\\TEMP\\3ecp1ys3\\3ecp1ys3.cmdline"
c: \\windows\\microsoft.net\\framework64\\v4.0.30319\\csc.exe	"C: \\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\csc.exe" /noconfig /fullpaths @"C: \\Windows\\TEMP\\mnnh5vg3\\mnnh5vg3.cmdline"

# ALERT PRIORITIZATION

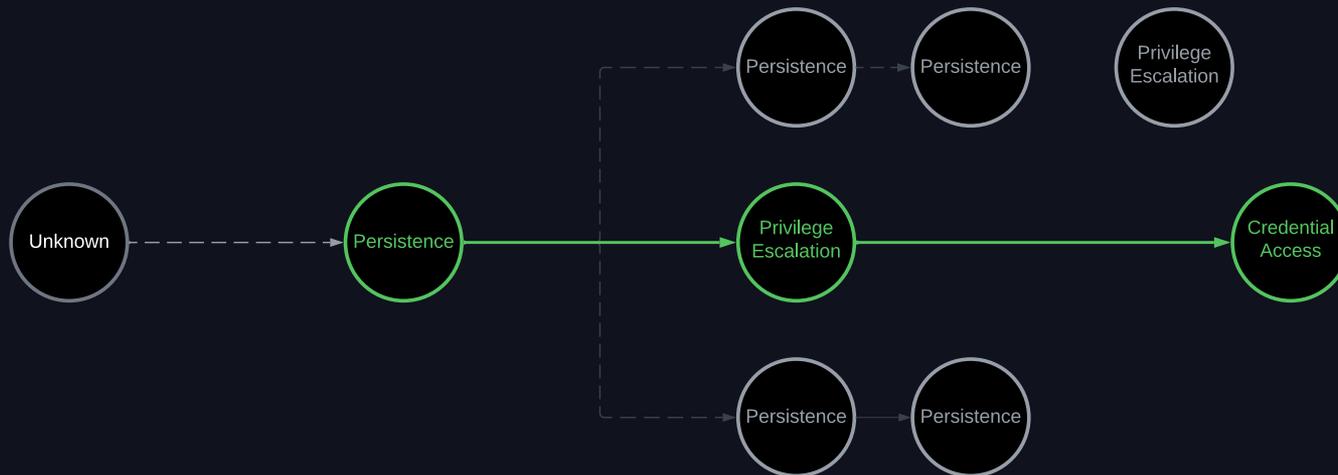
## Solution

- Group similar Alerts together
- Individually Customized
- Leverage DBSCAN
- Tag Clusters by score
- Generate grouping



# ALERT PRIORITIZATION

## Future



- Explore other methods for prioritize and group Alerts
- Enhance Integration of ML Pipeline with Production Infrastructure
- Continue global roll out of Alert Prioritization

# THE FUTURE

Data Lake to Lake House to Intelligence Platform



# CYLANCE AI FOR BLACKBERRY

## Supporting all Products and ecosystems

- Leverage Vector Search Index capabilities with Databricks to serve up data for LLM RAG workflows
- Data is ingested, transformed, and loaded within Databricks
- Existing Data is customized to be optimally served by Vector Search Index to ensure products such as Cylance AI has the most accurate and up to date information

# THE FUTURE

Where we are going? Are we there yet?

*“Create a BlackBerry Cybersecurity Data Intelligence platform to protect our customers from Cybersecurity threats”*

- Expand Machine Learning and AI uses with BlackBerry Cybersecurity data
- Continue to incorporate AI into everything we do

Special thanks to Databricks team  
Digan Parikh, Tal Flatt, and Amisha Singh



Special thanks to BlackBerry's team  
Laura Greaves, Rejish Cheruvatta, and  
Helbert Diaz



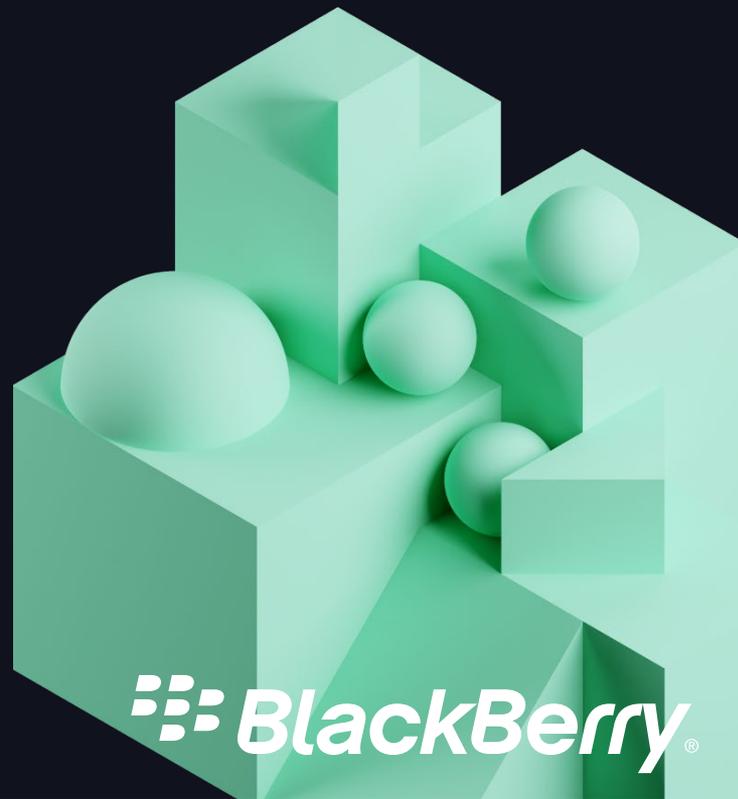
# DATA+AI SUMMIT

BY  databricks

# THANK YOU!



Find out more about Cylance AI!



 **BlackBerry**<sup>®</sup>