Using Data Science To Secure Cloud Workloads

Mikkel Hansen
Sales Engineer Manager
mhansen@cylance.com

Securing Your Cloud
Different Lenses

Aaron Bryson
Technical Director, Red Team Services
abryson@cylance.com

Using Data Science To Secure Cloud Workloads

Mikkel Hansen
Sales Engineer Manager
mhansen@cylance.com

Safe Harbor

The information in this presentation is confidential and proprietary to Cylance® and may not be disclosed without the permission of Cylance. This presentation is not subject to your license agreement or any other service or subscription agreement with Cylance. Cylance has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein.

This document, or any related presentation and Cylance's strategy and possible future development, product, and/or platform direction and functionality are all subject to change and may be changed by Cylance at any time for any reason without notice. The information on this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. This document is for informational purposes and may not be incorporated into a contract. Cylance assumes no responsibility for errors or omissions in this document.

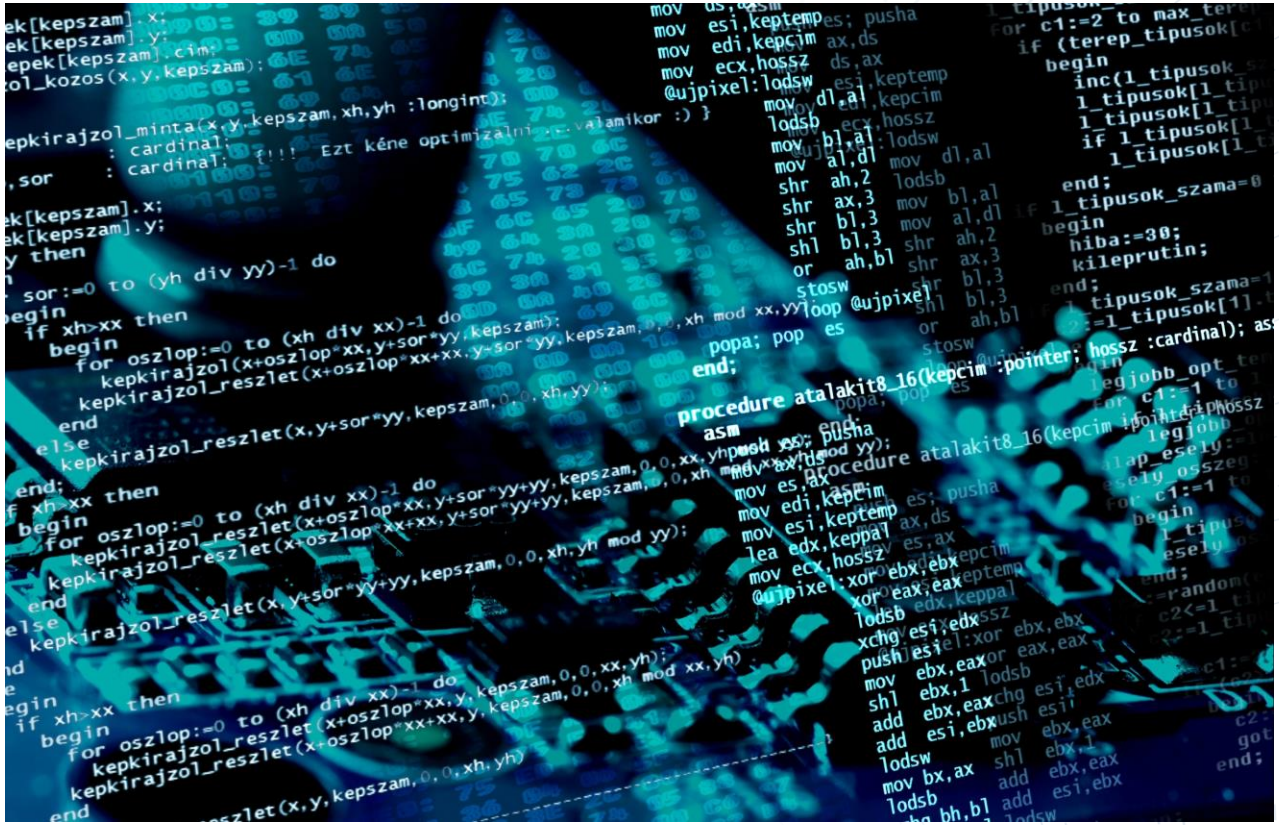
Agenda

- What is Data Science?
- Data Science Subcomponents
- Why Data Science for Security
- Traditional Security Layers
- Benefits of Applying Data Science To Security
- Cylance Protect Supported Operating Systems
- Securing Your Cloud: Different Lenses with Aaron Bryson

CYLANCE

Introduction

You may not have realized that most security products are using data science more than ever before. The entire security industry has moved towards using data science in existing products and new offerings.



CYLANCE

What Is Data Science?

Data science is a set of algorithmic tools that allow us to understand and make automated decisions about data using statistics, mathematics, and statistical data visualizations.

Data Science Subcomponents

- **Machine Learning —** Machine learning is a field of artificial intelligence that uses statistical techniques to give computer systems the ability to "learn" from data, without being explicitly programmed. The name machine learning was coined in 1959 by Arthur Samuel

- **Data Mining —** Data mining is the process of discovering patterns in large data sets involving methods at the intersection of machine learning, statistics, and database systems.

- **Data Visualization —** Data visualization is viewed by many disciplines as a modern equivalent of visual communication. It involves the creation and study of the visual representation of data. To communicate information clearly and efficiently, data visualization uses statistical graphics, plots, information graphics, and other tools.

Why Data Science for Security?

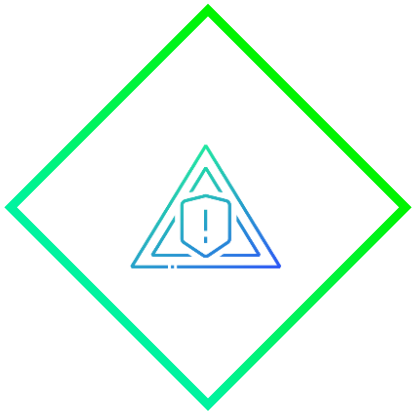
- Security is all about the data
- Too much manual work to keep up with the threat landscape
- Over 700 Million unique malicious executables

CYLANCE

Traditional Security Layers

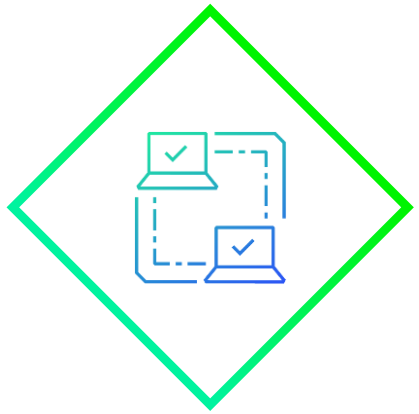
Antivirus

Using data science algorithms deployed on endpoints to detect malware



Firewall

Using data science algorithms to identify anomalous network events and user behavior



SIEM

Uses data science to identify suspicious trends and events based on data it’s collected from your infrastructure, workstations, and servers

Benefits of Applying Data Science To Next-Gen AV?

Threat Predictive Advantage

Emotet

Goldeneye

Wannacry

List of Supported Operating Systems

Linux:

- Red Hat Enterprise Linux 6.6-6.9
- Red Hat Enterprise Linux 7.0-7.5
- CentOS 6.5-6.9
- CentOS 7.0-7.5
- Ubuntu 14.04 and 16.04
- Amazon Linux 2017.09 and 2018.03

Windows:

- Windows Server 2003 R2
- Windows Server 2008 and 2008 R2
- Windows Server 2012 and 2012 R2
- Windows Server 2016

Applying Data Science To Next-Gen AV Products Allows You To Become Predictive Instead of Reactive!

Thank You

Mikkel Hansen
mhansen@cylance.com

Next up…Aaron Bryson

Securing Your Cloud
Different Lenses

Aaron Bryson
Technical Director, Red Team Services
abryson@cylance.com

Cloud Security: Different Lenses

Assurance

- **Architecture** (data design, services, integrity, anonymity, network segmentation, microservices, serverless, etc.)
- **Threat modeling** (network, apps, data)
- **Configuration review**
- **Penetration testing** (network and apps)

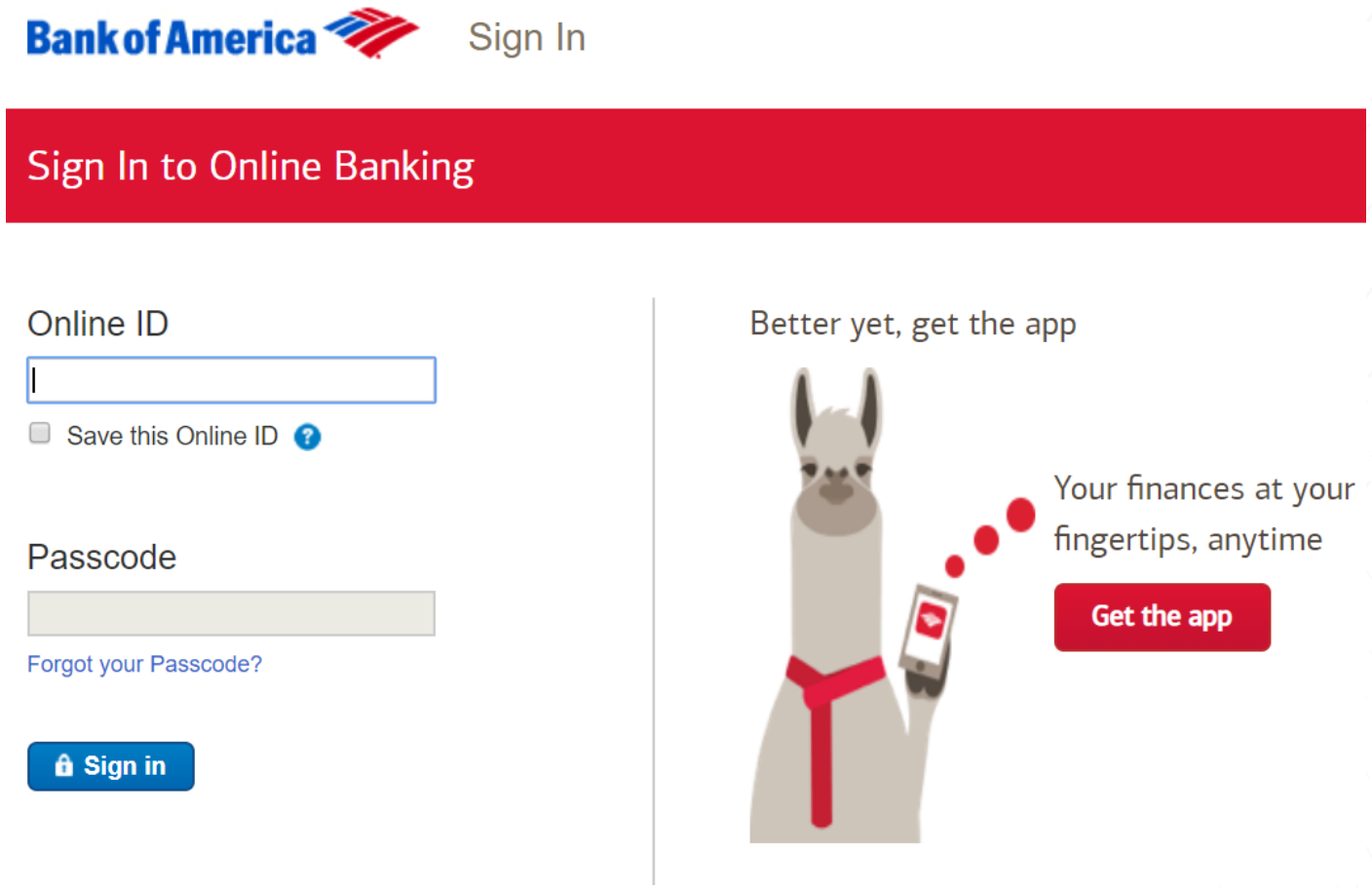
Configuration Review

- **Identity and Access Management** (multifactor, password policies, account pollution, access key rotation, etc.)
- **Logging** (Enabling CloudTrail, AWS Config for all regions, rotating CMKs)
- **Monitoring** (Log metrics & alarms for Network Access Control Lists, Configuration changes, S3 bucket policy changes, route table changes, network gateway changes, unauthorized API calls)
- **Networking** (security groups, ingress, egress, VPC flow logs)

Configuration Review

- **EC2** (TCP/UDP ports, default security groups, unused security groups, non-empty rulesets, data tagging)
- **S3** (access logging enabled, world-listable, MFA delete enabled, versioning enabled, object and bucket ACLs parity, server-side encryption, data tagging, etc.)
- **RedShift** (cluster database encryption, TLS required, user activity logging enabled, data tagging, etc.)

Penetration Testing Applications



Penetration Testing Services / APIs

post `/cashpro/payments/v1/payment-initiations`

Payment Initiations allows for the origination of single payment instruction through CashPro Global Payments. Upon delivery, payment will enter Global Payments workflow allowing for approvals, repair, and release.


```
{
  "paymentIdentification": {
    "instructionIdentification": "instrId123",
    "endToEndIdentification": "e2eId123"
  },
  "paymentMethod": "TRF",
  "requestedExecutionDate": "2018-01-13",
  "amount": {
    "value": "1.00",
    "type": "CREDIT"
  },
  "debtorAccount": {
    "identification": "601011111111",
    "schemeName": "BBAN",
    "currency": "string"
  },
  "debtorAgent": {
    "institution": {
      "name": "string",
      "identifiers": [
        {
          "identification": "BOFAFRPP",
          "schemeName": "BIC"
        }
```


CYLANCE

Penetration Testing Cloud Network

- ec2-52-XXX-122-132.compute-1.amazonaws.com (domain)
- 52.XXX.122.132 (public IP)
- debitcards.s3.amazonaws.com

Incident Response

- Pre-requisite Knowledge and Information
  - Do you know when the house is burning down?
- Legal Counsel
- Incident Response Plan
- Cyber Liability Insurance

Thank You

Aaron Bryson

abryson@cylance.com

www.cylance.com/webinars