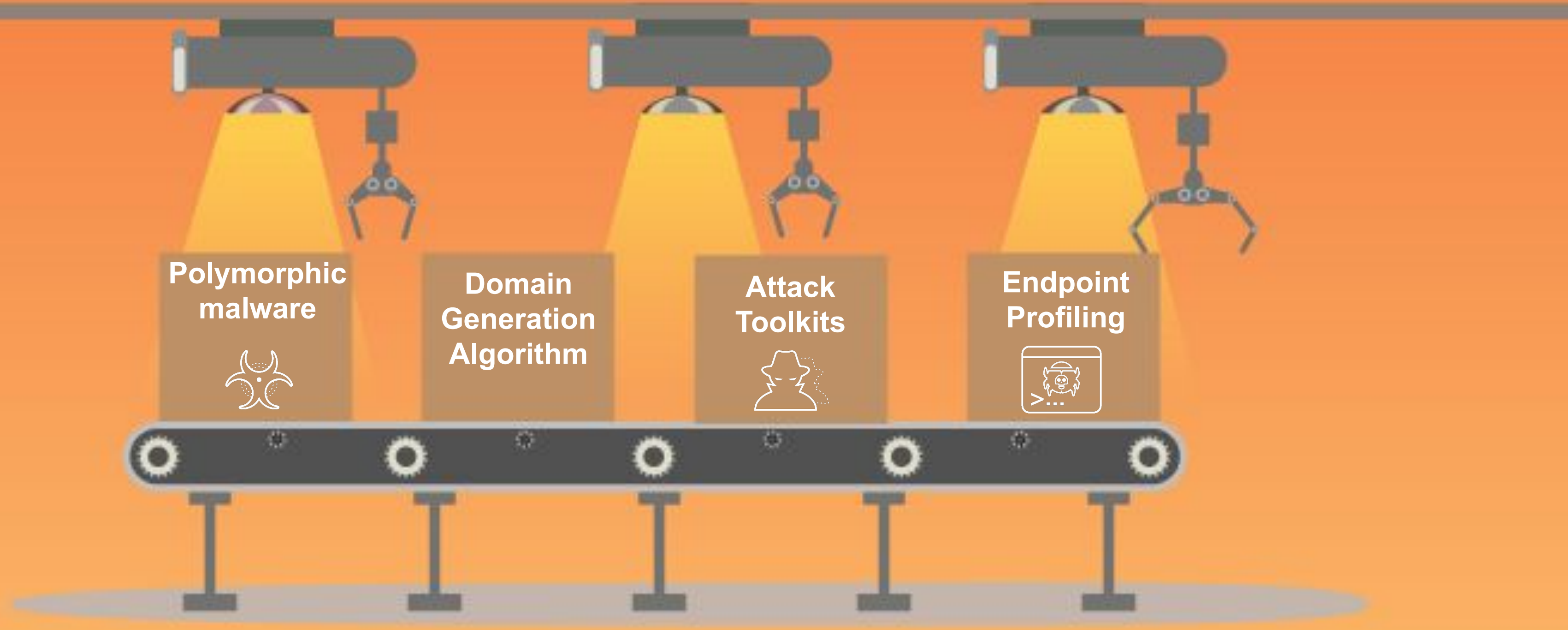
Využití automatizace a ML algoritmů pro zastavení pokročilých hrozeb

Jakub Jiříček, Systems Engineer Cortex
Palo Alto Networks

říjen 2020

THREAT ACTORS USE AUTOMATION FOR ATTACKS & EVASION



CHALLENGES OF A DYNAMIC THREAT LANDSCAPE

No Known Bad

Once attackers have infiltrated the organization, they use benign tools

Attackers Aim to Bypass Security

With polymorphism, DGA, 2FA bypass

Static Rules Generate Many False Positives

As they are not automatically derived from the data, static rules are error prone

Static Rules Are Labor Intensive

Static rules require constant adapting and maintenance

DEFENDERS NEED MACHINE LEARNING TO OUTPACE ATTACKERS

Stop Attacks Faster

Automatically analyze unknown files and domains to block threats

Detect Stealthy Threats

Uncover threats that would be virtually impossible to find manually

Reduce Manual Errors

Avoid overlooking risks and alert fatigue with consistent analysis

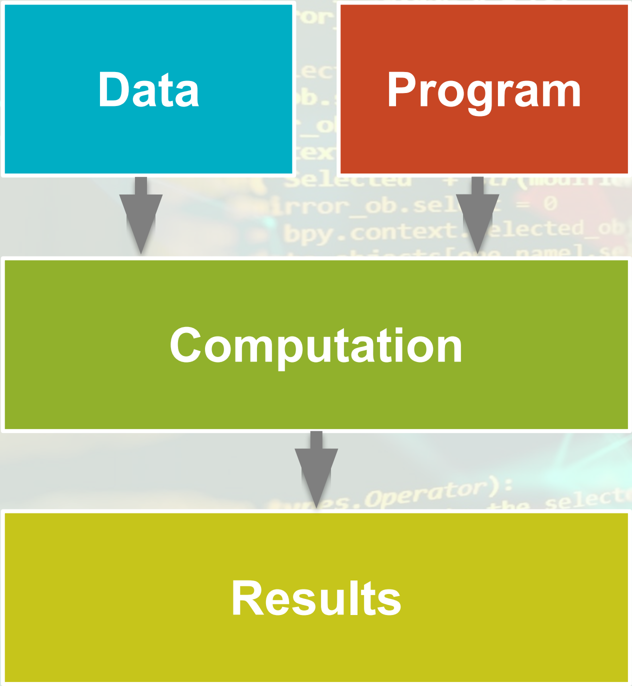
Simplify Operations

Eliminate repetitive tasks and make your life easier

What is machine learning?

MACHINE LEARNING BACKGROUND

Conventional Software



Data

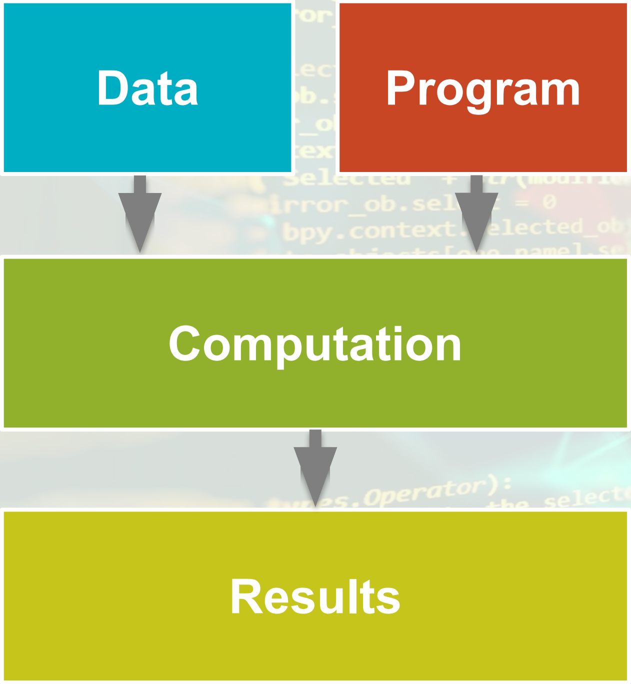
Program

Computation

Results

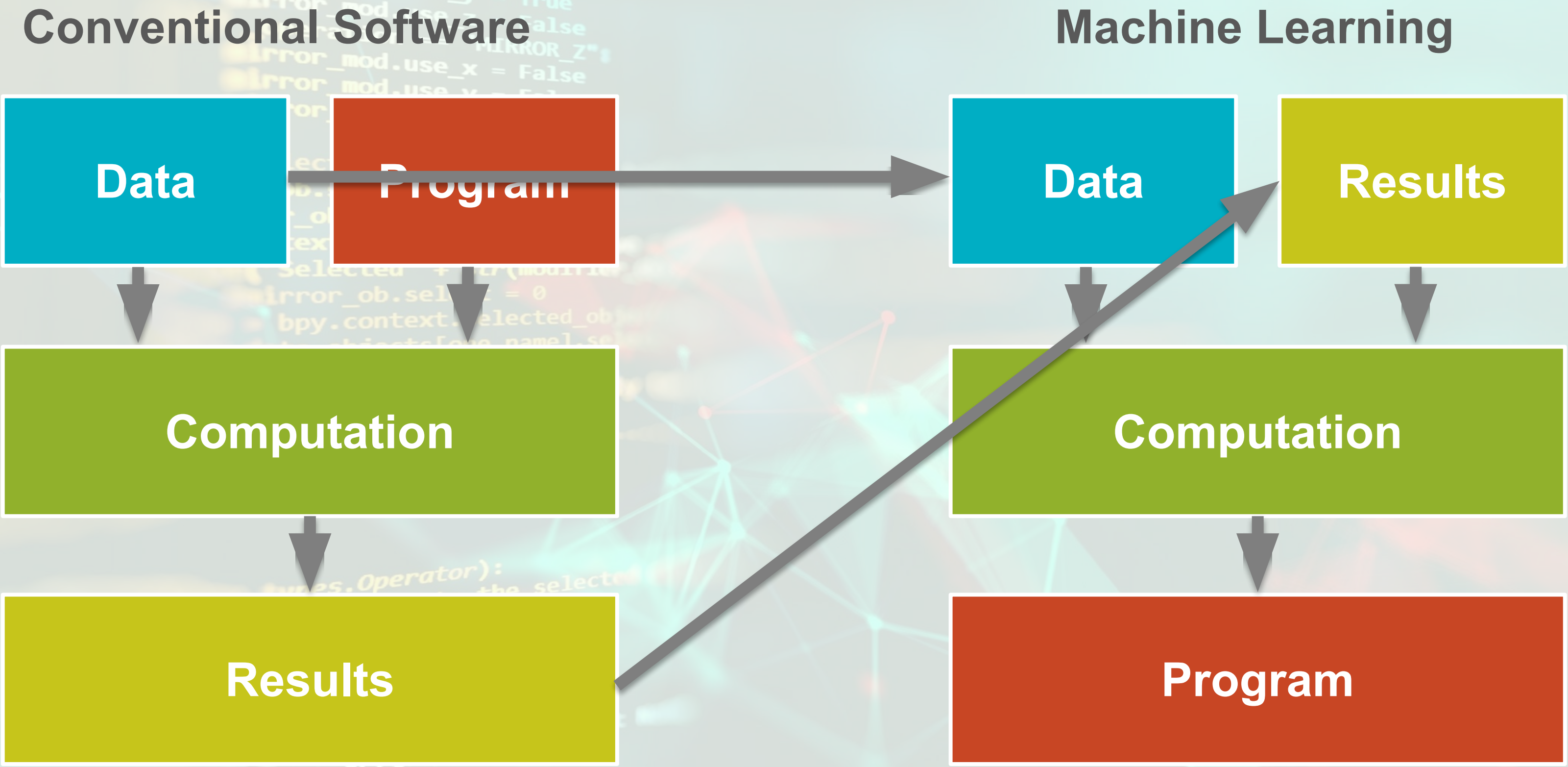
MACHINE LEARNING BACKGROUND

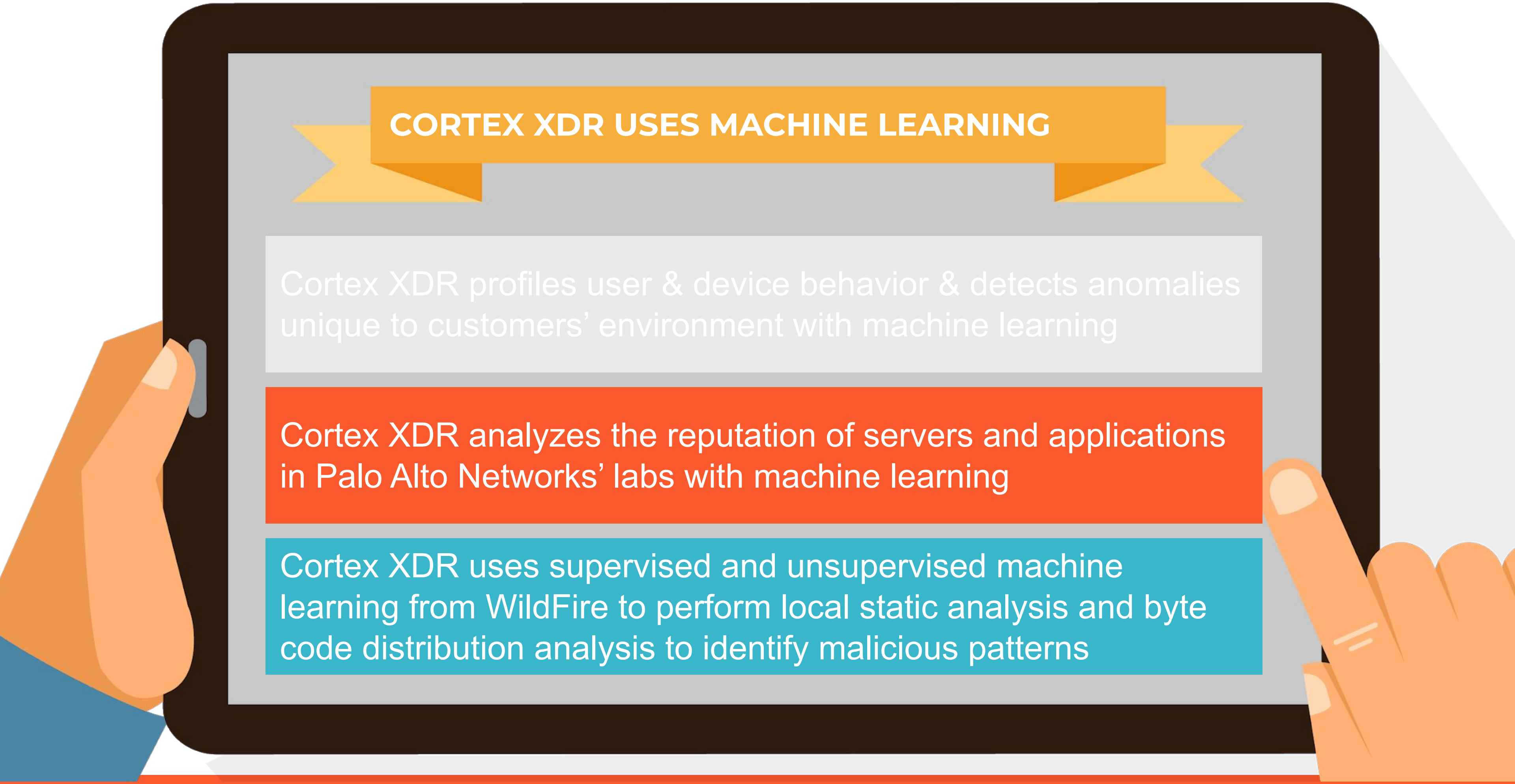
Conventional Software



Machine Learning

MACHINE LEARNING BACKGROUND





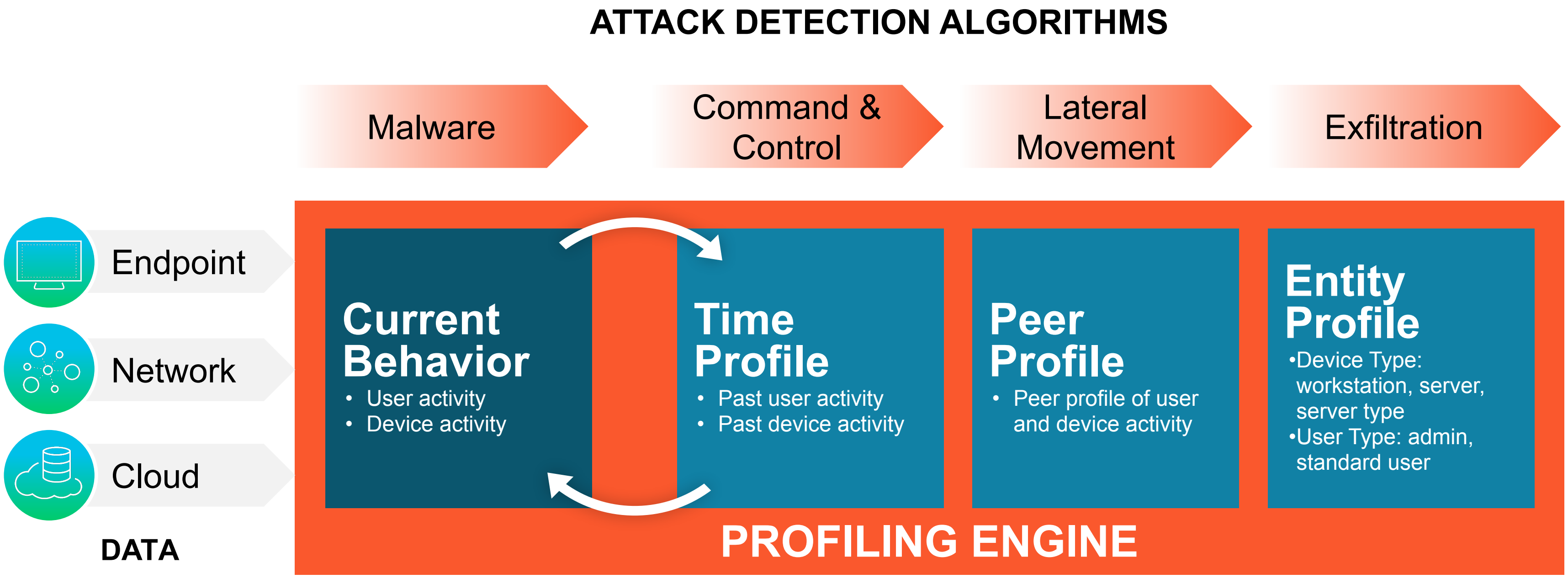
CORTEX XDR USES MACHINE LEARNING

Cortex XDR profiles user & device behavior & detects anomalies unique to customers' environment with machine learning

Cortex XDR analyzes the reputation of servers and applications in Palo Alto Networks' labs with machine learning

Cortex XDR uses supervised and unsupervised machine learning from WildFire to perform local static analysis and byte code distribution analysis to identify malicious patterns

PINPOINT ATTACKS UNIQUE TO YOUR ENVIRONMENT WITH AI



Current Behavior

- User activity
- Device activity

Time Profile

- Past user activity
- Past device activity

Peer Profile

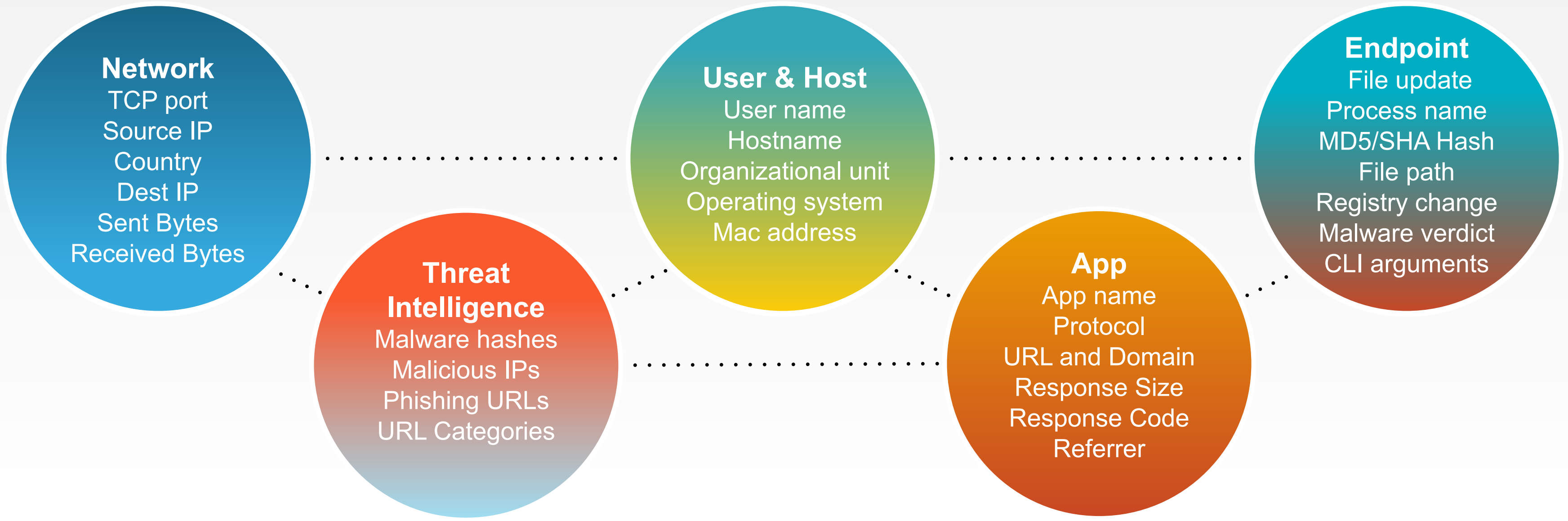
- Peer profile of user and device activity

Entity Profile

- Device Type: workstation, server, server type
- User Type: admin, standard user

Profile behavior & detect anomalies indicative of an attack

COMPREHENSIVE, CORRELATED DATA POWERS MACHINE LEARNING



Network
TCP port
Source IP
Country
Dest IP
Sent Bytes
Received Bytes

Threat Intelligence
Malware hashes
Malicious IPs
Phishing URLs
URL Categories

User & Host
User name
Hostname
Organizational unit
Operating system
Mac address

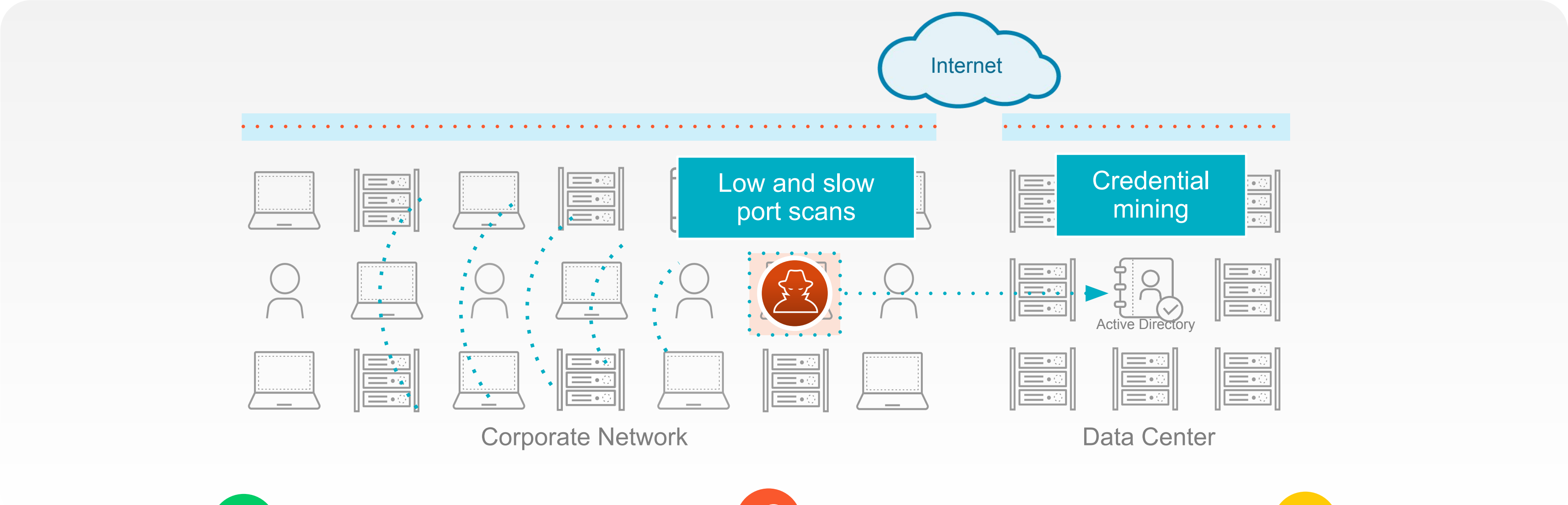
App
App name
Protocol
URL and Domain
Response Size
Response Code
Referrer

Endpoint
File update
Process name
MD5/SHA Hash
File path
Registry change
Malware verdict
CLI arguments

Collect rich data for behavioral analytics & AI

Automatically correlate data to gain context for investigations

CORTEX XDR USES MACHINE LEARNING TO DETECT RECON



1

Monitor access to key servers like Active Directory

2

Classify devices and profile user & peer behavior

3

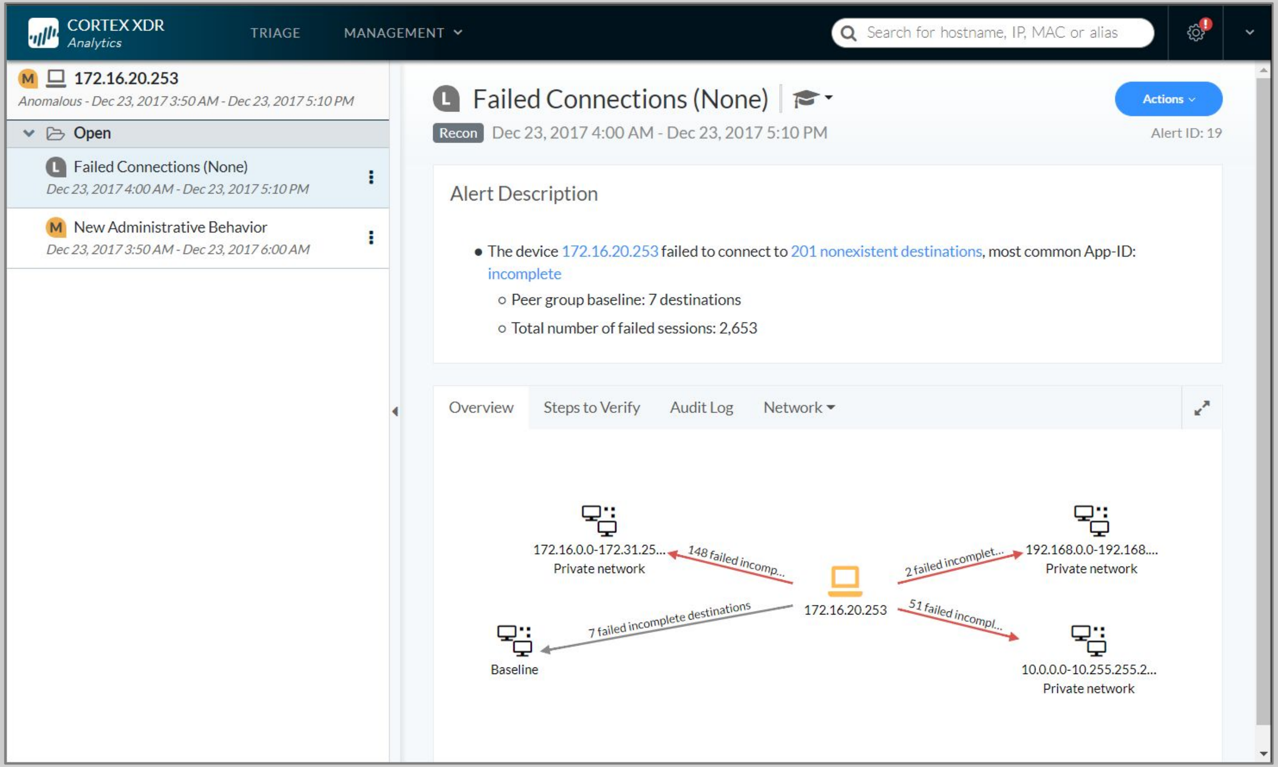
Uncover attacks by detecting anomalies indicative of reconnaissance

DETECTING RECONNAISSANCE WITH MACHINE LEARNING

- **Failed Connections**
  - Cortex XDR detects attempts to connect to a large number of internal nonexistent destinations with a specific port or protocol, relative to the peer group behavior

- **Port Scan**
  - Sounds simple, but traditional, rule-based port scan detection often generates false positives
  - Cortex XDR uses machine learning to differentiate between port scans, service scans and vulnerability scans
  - Using a rule-based approach, a network of 40,000 endpoints would yield roughly 40,000 port scan alerts in 3 days!
    - Rule-based approach: 42,201 port scans; 86 sources; 19,531 destinations
    - Cortex XDR port scan alerts: 7 (with only 2 false positives)

BEHAVIORAL ANALYTICS CAN DETECT ALL STAGES OF AN ATTACK



M 172.16.20.253

Anomalous - Dec 23, 2017 3:50 AM - Dec 23, 2017 5:10 PM

Open

L Failed Connections (None)
Dec 23, 2017 4:00 AM - Dec 23, 2017 5:10 PM

M New Administrative Behavior
Dec 23, 2017 3:50 AM - Dec 23, 2017 6:00 AM

L Failed Connections (None)

Recon Dec 23, 2017 4:00 AM - Dec 23, 2017 5:10 PM

Alert ID: 19

Alert Description

- The device 172.16.20.253 failed to connect to 201 nonexistent destinations, most common App-ID: incomplete
  - Peer group baseline: 7 destinations
  - Total number of failed sessions: 2,653

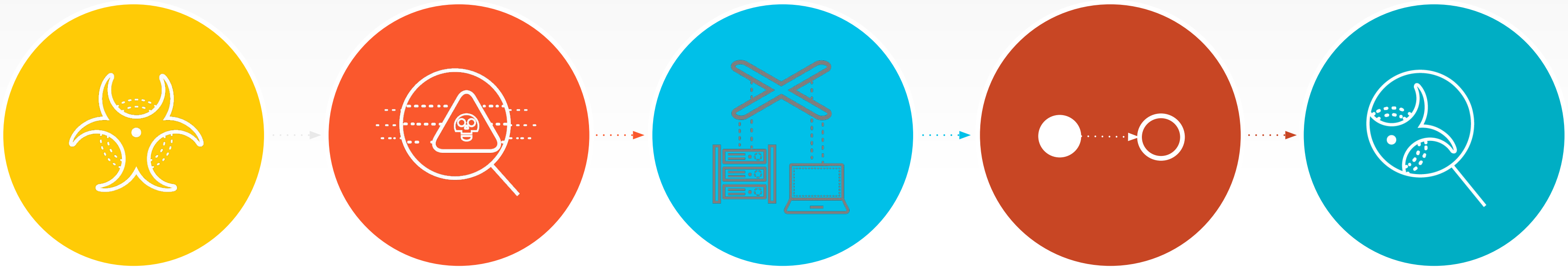
By profiling behavior, you can detect:

- Malware activity
- Command & control
- Lateral movement
- Data exfiltration

Profiling the type of device & behavior can reduce false positives

DETECT EACH STEP AFTER THE INITIAL INTRUSION

Attack Lifecycle



Vulnerability Exploit

Malware Installation

- Malware
- Riskware
- SpamBot Traffic

Command and Control

- Tunneling Process
- Failed DNS
- Random Looking DNS
- Recurring Rare Domain Access
- Recurring Rare IP Access

Lateral Movement & Recon

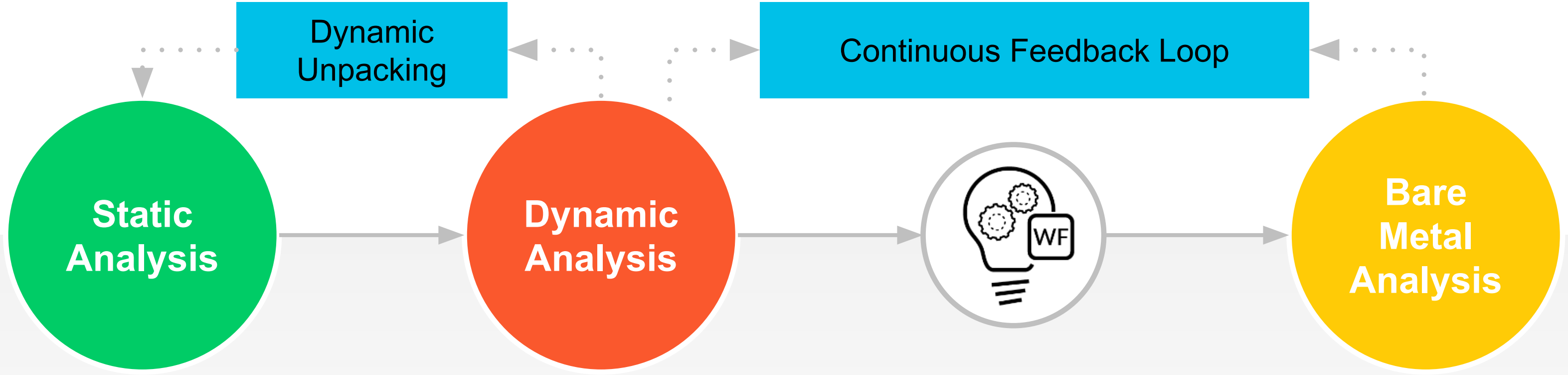
- Failed Connections
- Consecutive Connections
- High Connection Rate
- New Admin Behavior
- Port Scan
- Remote Command Execution
- Reverse Connections
- SMB/KRB Traffic from Non-Standard

Data Exfiltration

- Large Upload FTP
- Large Upload Generic
- Large Upload HTTPs
- Large Upload SMTP

CORTEX XDR USES MACHINE LEARNING TO FIND MALWARE

WildFire Malware Analysis



Dynamic Unpacking

Continuous Feedback Loop

Static Analysis

Dynamic Analysis

WF

Bare Metal Analysis

Detect known exploits, malware, and variants

- Memory analysis
- Machine learning
- File anomalies
- Malicious patterns
- Known malicious code

Find new zero-day exploits & malware through execution

- Custom hypervisor
- Behavioral scoring
- Multi-version analysis

Heuristic Engine
Steer evasive malware to bare metal

Identify VM-aware threats using hardware systems

- Full dynamic analysis
- Real desktop hardware
- No virtual environment
- No hypervisor

COMPETITIVE ADVANTAGES OF OUR MACHINE LEARNING

Behavioral Profiling

Detects anomalies unique to your environment and reduces false positives

EDR tools perform lab-based machine learning which is not tailored to each customer

Pre-Compute Architecture

Advanced ML models track 1,000+ dimensions of behavior, each detection algorithm looks at many aspects of behavior

Most SIEMs & EDRs analyze raw data with simple rules

Broader Data Set

Network, endpoint & cloud data, stitched together, removes blind spots & speeds investigations

Cortex XDR detects all stages of attacks, not just malware

Díky za pozornost

www.paloaltonetworks.com

jjiricek@paloaltonetworks.com

COMPETITIVE ADVANTAGES OF CORTEX XDR MACHINE LEARNING

Cortex XDR	Other Solutions
ML models consolidate entities **across network and endpoint**	ML models based on **partial** data (either network or endpoint)
Advanced ML models with depth (complex **entity-role** classifiers) and width (more than **1,000** profiles)	Typically, simple models that profile behavior without taking into account entity's role
ML models use **data across all customers**, that **adapt** to the customer environment they are deployed in	**Static** models built using data from lab or *some* customers, which do *not* adapt to the customer environment
ML models can pinpoint hard-to-detect **manual attacks and network attacks** as well as **malware**	ML models, especially for EDR vendors, focus on **malware only**

|