BLUEHEXAGON

Cyber AI You Can Trust

Microsoft

Accelerate your Threat Hunting + IR with Next-Gen NDR + EDR

Speakers:
Balaji Prasad, Blue Hexagon
Heike Ritter, Microsoft
Arun Raman, Blue Hexagon

July 17th, 3 pm ET

BLUEHEXAGON

COMPANY

Founders and team members with expertise in Deep Learning, Threat Research, Security, High Performance Compute

- Qualcomm machine learning expertise (500+ patents)
- FireEye, Symantec, Palo Alto Networks, Juniper security expertise
- PHDs - MIT, Georgia Tech, Purdue, Princeton

CUSTOMERS

- Healthcare
- Insurance
- Financial Services
- Retail

PACIFIC DENTAL SERVICES

DELTA DENTAL

HEFFERNAN INSURANCE BROKERS

Greenhill

PARTNER INTEGRATIONS

Member of Microsoft Intelligent Security Association

aws partner network Advanced Technology Partner

Microsoft

aws

CROWDSTRIKE

CARBON BLACK

splunk>

ixia

DEMISTO A PALO ALTO NETWORKS COMPANY

Gigamon

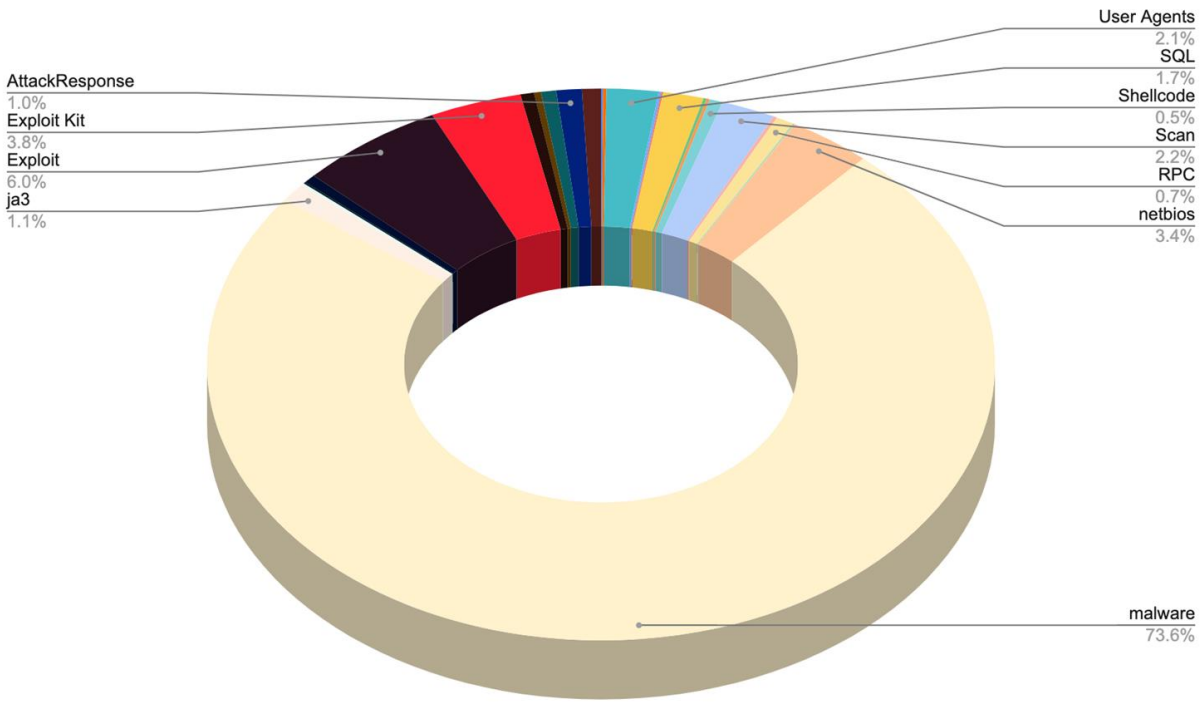
Breaking News: Blue Hexagon recognized by leading industry analysts

- ➔ *2020 Gartner Market Guide for Network Detection and Response*
- ➔ *2020 Forbes AI 50: America's Most Promising Artificial Intelligence Companies*
- ➔ *Forbes Report: Gartner's Top 25 Enterprise Software Startups To Watch In 2020*

BLUEHEXAGON

Network Threats : Malware, Exploits and C&C → Higher Variety

Dynamic Evolving Threats vs Static Threats



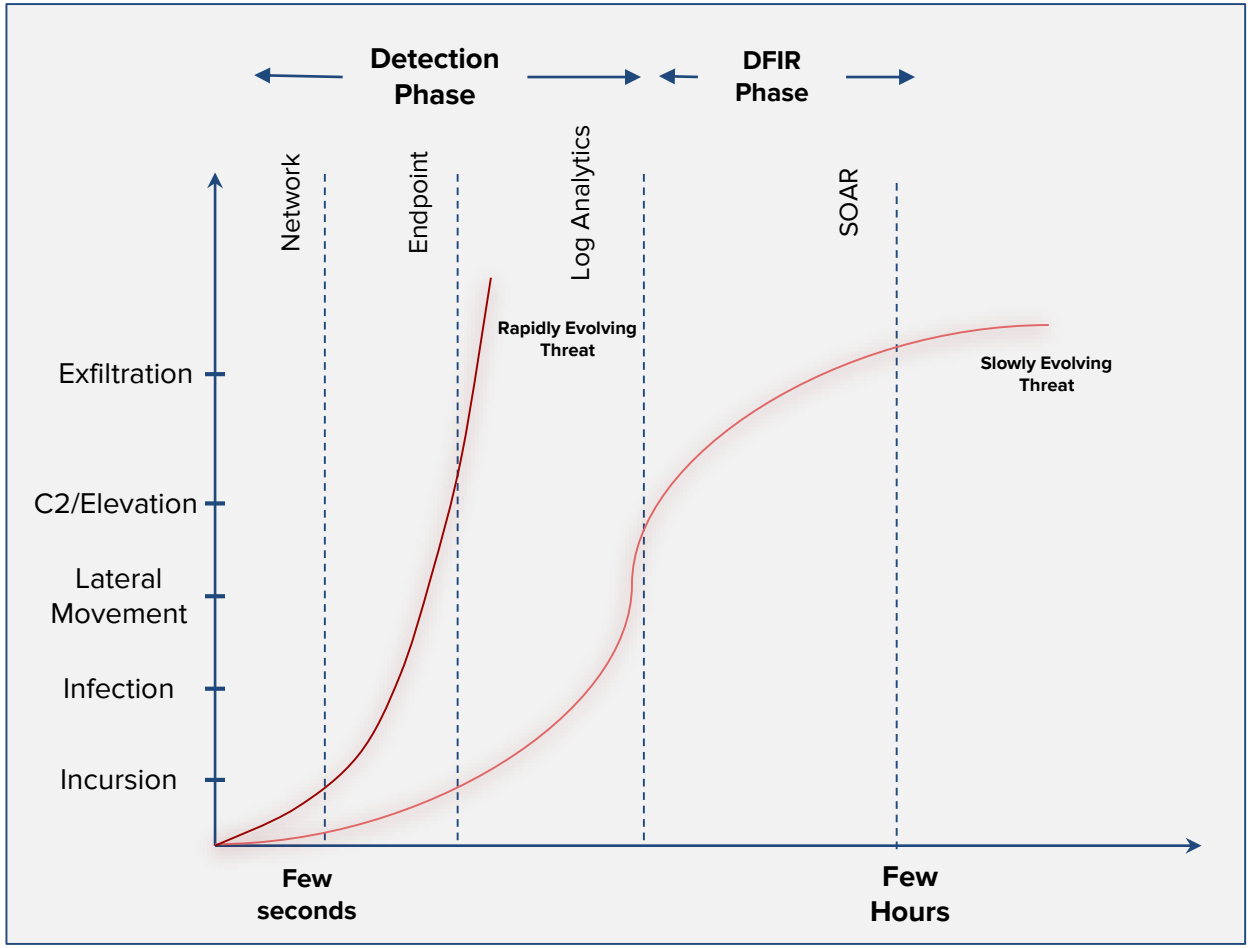
Malware, Exploits and C&C

- Hard to keep up with fast evolving content and techniques
- Rules do not scale
- Needs fundamental innovation
- Real Time Deep Learning scales

Protocol attacks, DOS, Network Scans

- Evolve slowly and are very specific
- Behavior based or static rule based detection
- Reducing the sigs and rules helps improve performance

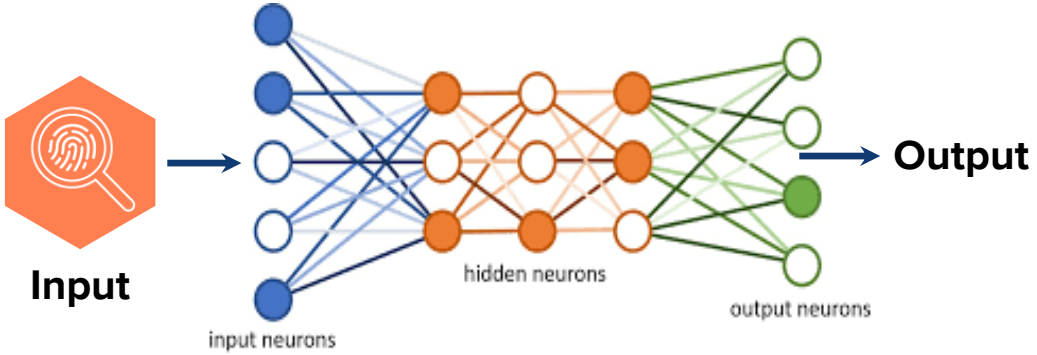
Can more technology improve DFIR?



- SOC Triad - NDR, EDR & SIEM
- Different timescales & data lakes ⇒ RCA & correlation hard
- More suited for slowly evolving threats that registers activity on various security controls
- Rapidly evolving threat will circumvent the control triad.

- **Solution: Stop threats at point of incursion using tightly correlated NDR & EDR**

A new Approach
Harnessing Deep Learning for Real-Time Detection



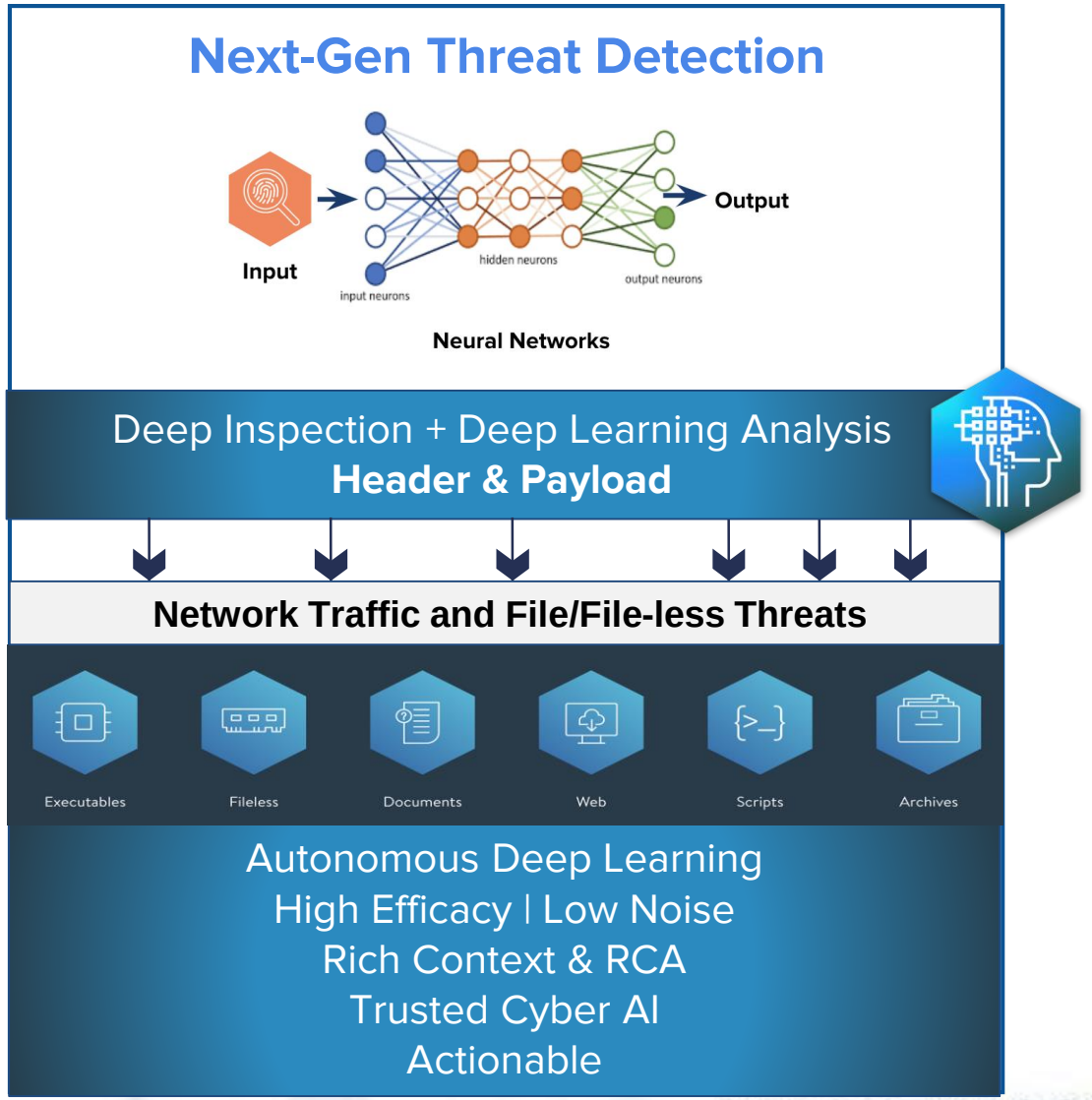
Neural Networks

Similar to deep learning bounding box around photos, apply deep learning to network traffic

- ✓ Massive threat data exists
- ✓ GPUs now available for processing
- ✓ Enhancements in deep learning models

Evolving to Next-Gen AI - Real Time Deep Learning

- Deep Learning for Malware, Exploits and C&C detection
  - Train using labeled samples
  - Classify unseen sample based on learned characteristics
  - High generalization capacity ➔ deals with daily new variants
  - Low FP ➔ blocking possible
- Behavior Analytics for Exfiltration, Recon and Post-Infection detection
- Rules only needed for small set of static attacks ➔ better scaling with Gbps



BLUEHEXAGON

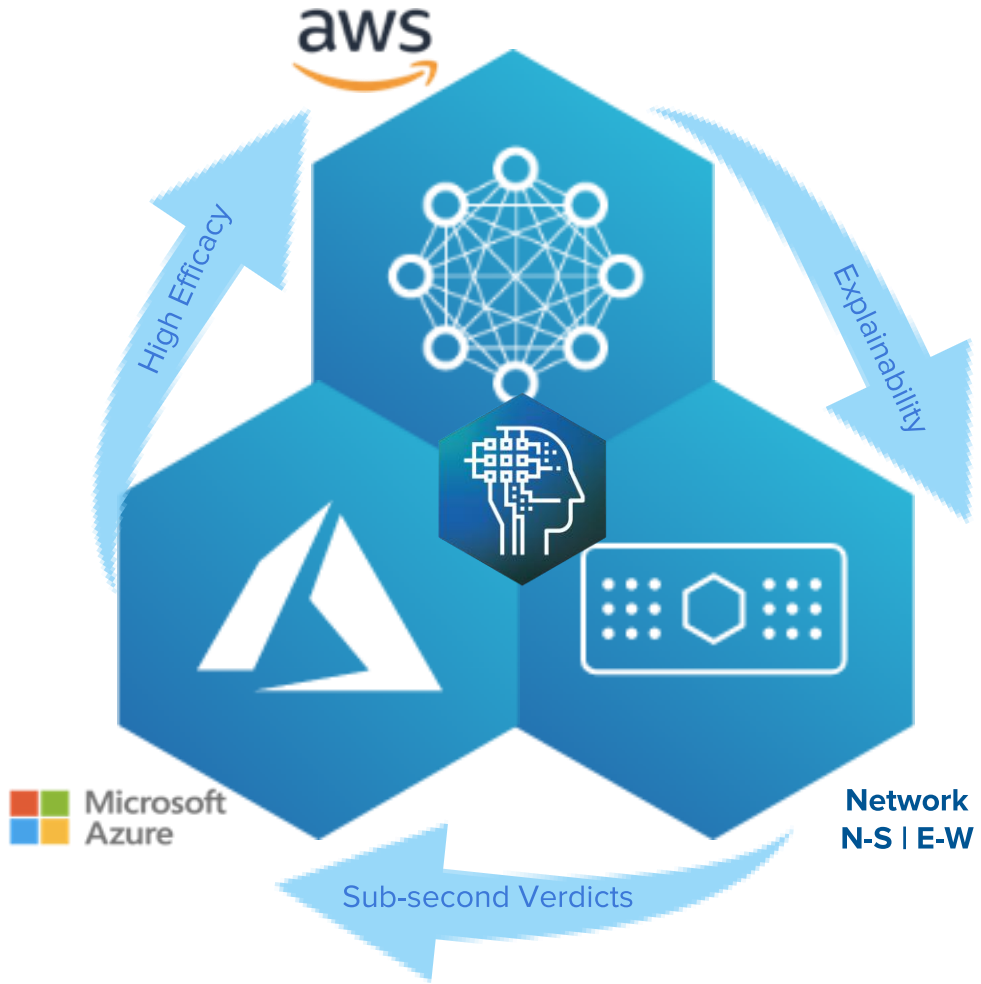
BLUEHEXAGON

Cyber AI You Can Trust

Real Time Deep Learning

- **~100%** efficacy and **sub-second** detection
- Detect and Prevent known & **0-day malware and threats**
- Predictive **AI Explainability** for advanced detection and hunting

Get Full Visibility



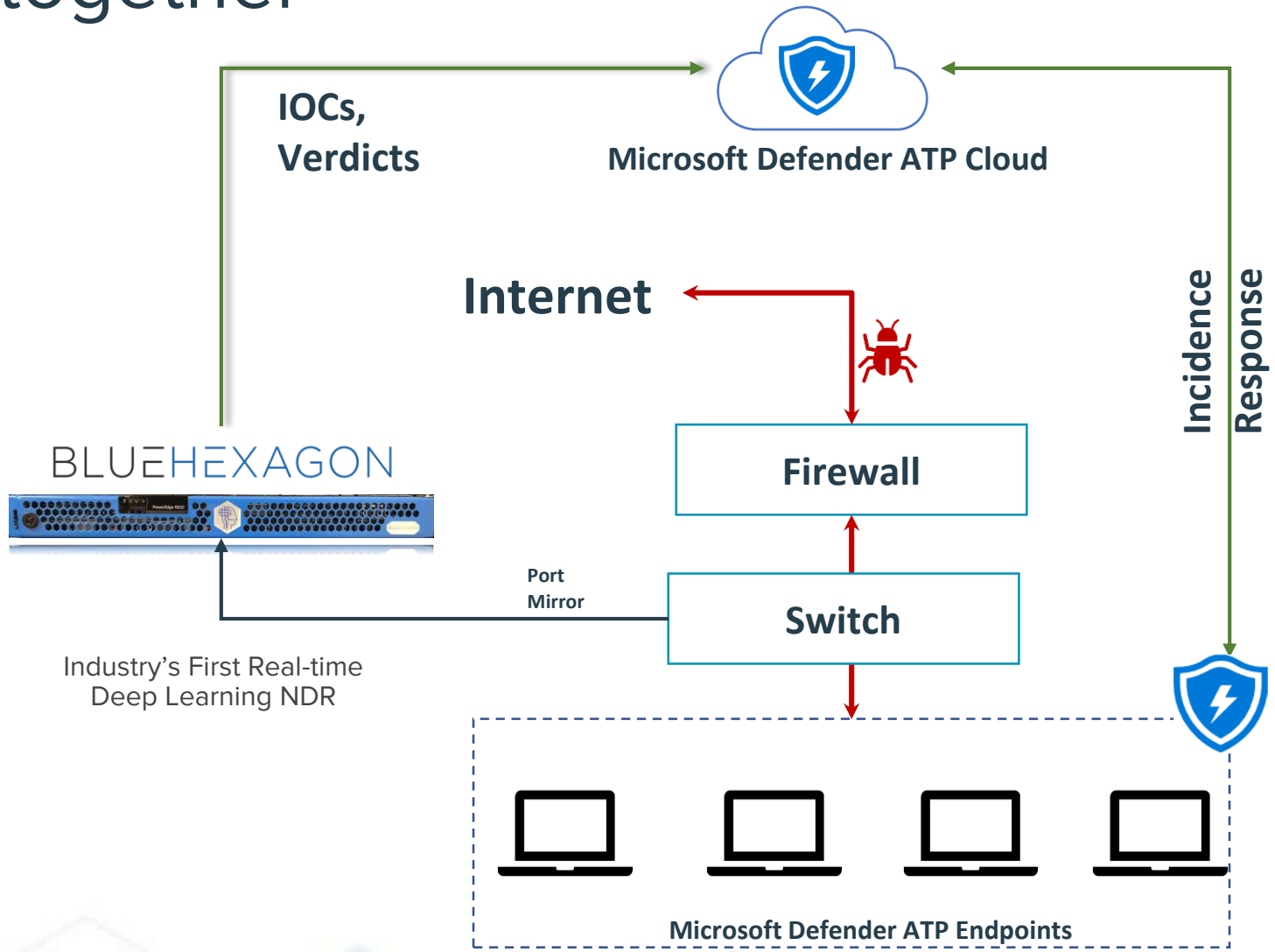
Easy to Deploy & Manage

- **Autonomous Analysis** - no baselining or learning delays
- **No rules, signatures or sandbox** required
- **Cloud-managed** on-prem and cloud deployment

Cloud Native or Hybrid

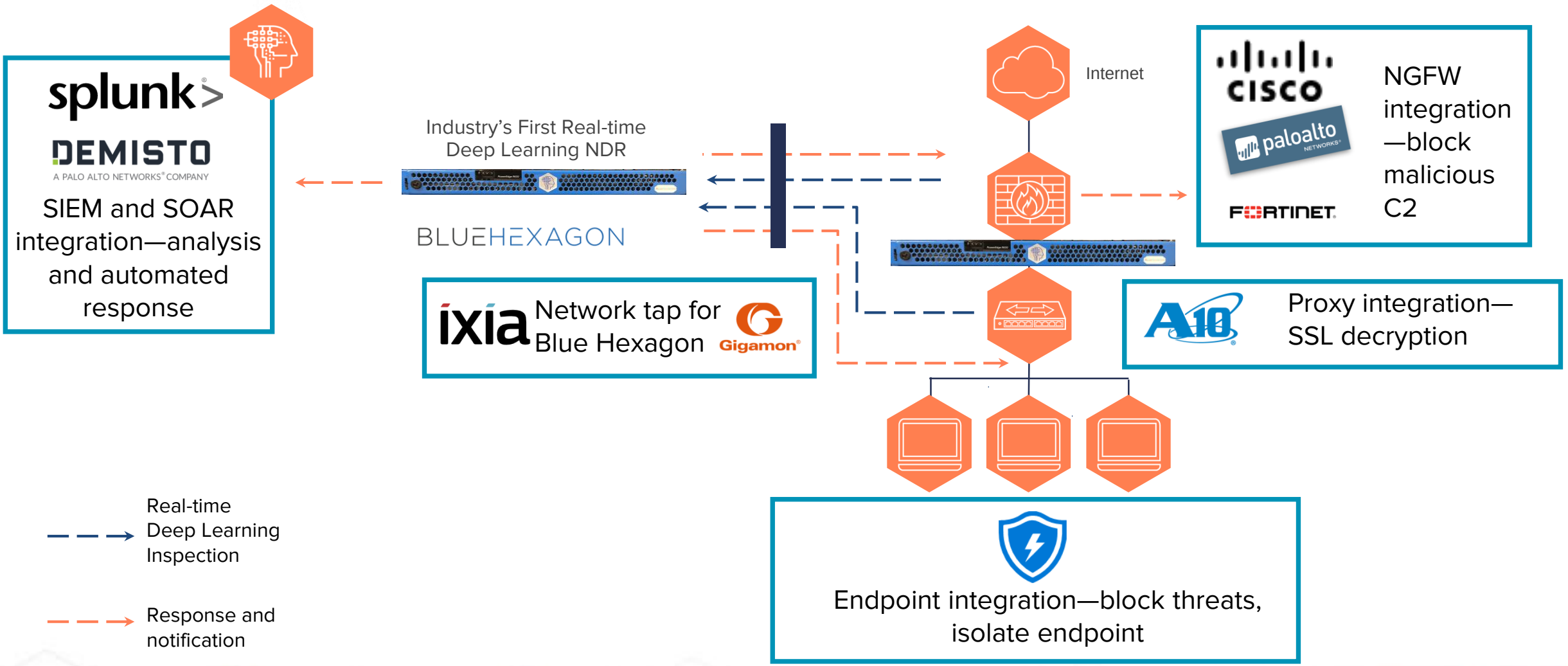
Next-Generation
Network Detection and Response

Blue Hexagon and Microsoft Defender ATP - Better together



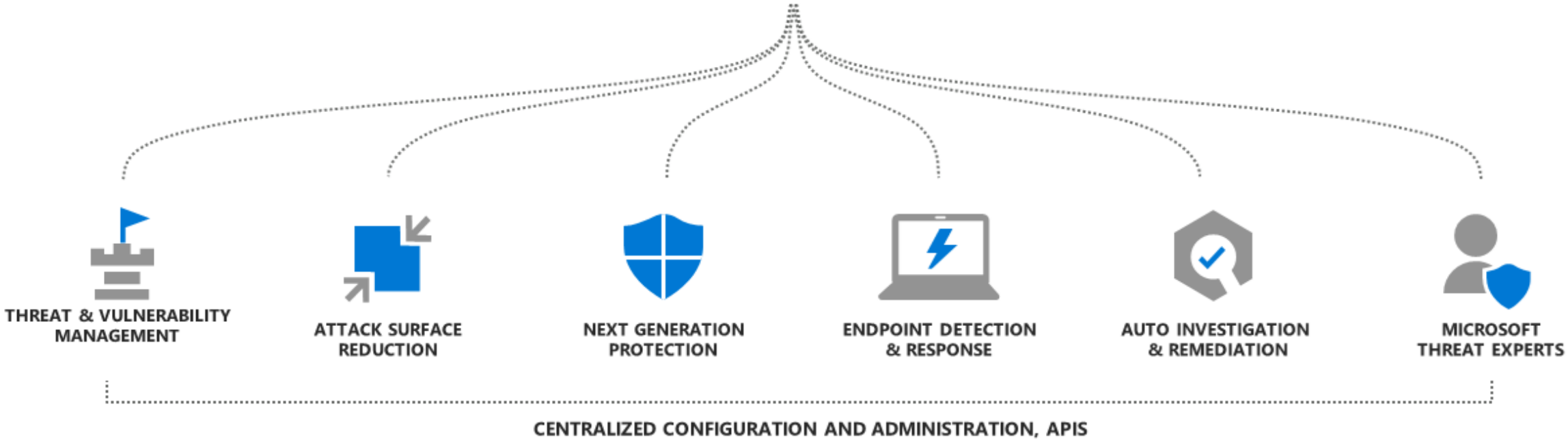
- Currently, the ONLY network security partner to integrate with Microsoft Defender ATP
- BH detects threats early in the network and notifies Microsoft Defender ATP for incident response
- File blacklisting, endpoint quarantine & Forensics Collection supported
- One click integration using Microsoft Graph API

Enterprise Ecosystem



Microsoft Defender
Advanced Threat Protection

Built-in. Cloud-powered.

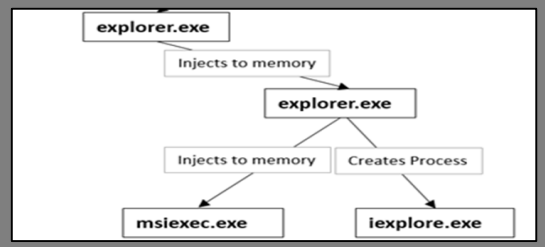


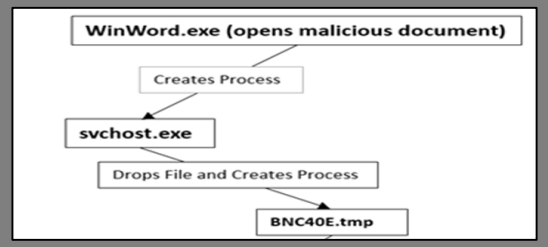
Microsoft

EDR “Process Trees” Detection Layers at a Glance

Input

Process Trees





Layer 1

“Expert” Models

- Network Classifier
- Registry Classifier
- Memory Classifier
- PowerShell Classifier
- LsHash Classifier
- PE attributes Classifier
- Command Line Classifier
- AMSI VB Classifier
- AMSI JS Classifier
- PowerShell Deep Learning Classifier(s)
- …

Layer 2

Ensemble Decision Models

- Decision Models (Word, Excel, PowerShell,…)

Alert

Microsoft

Triage & Investigation

Understand what was alerted

Alert investigation experience provides detailed description, rich context, full process execution tree

Investigate device activity

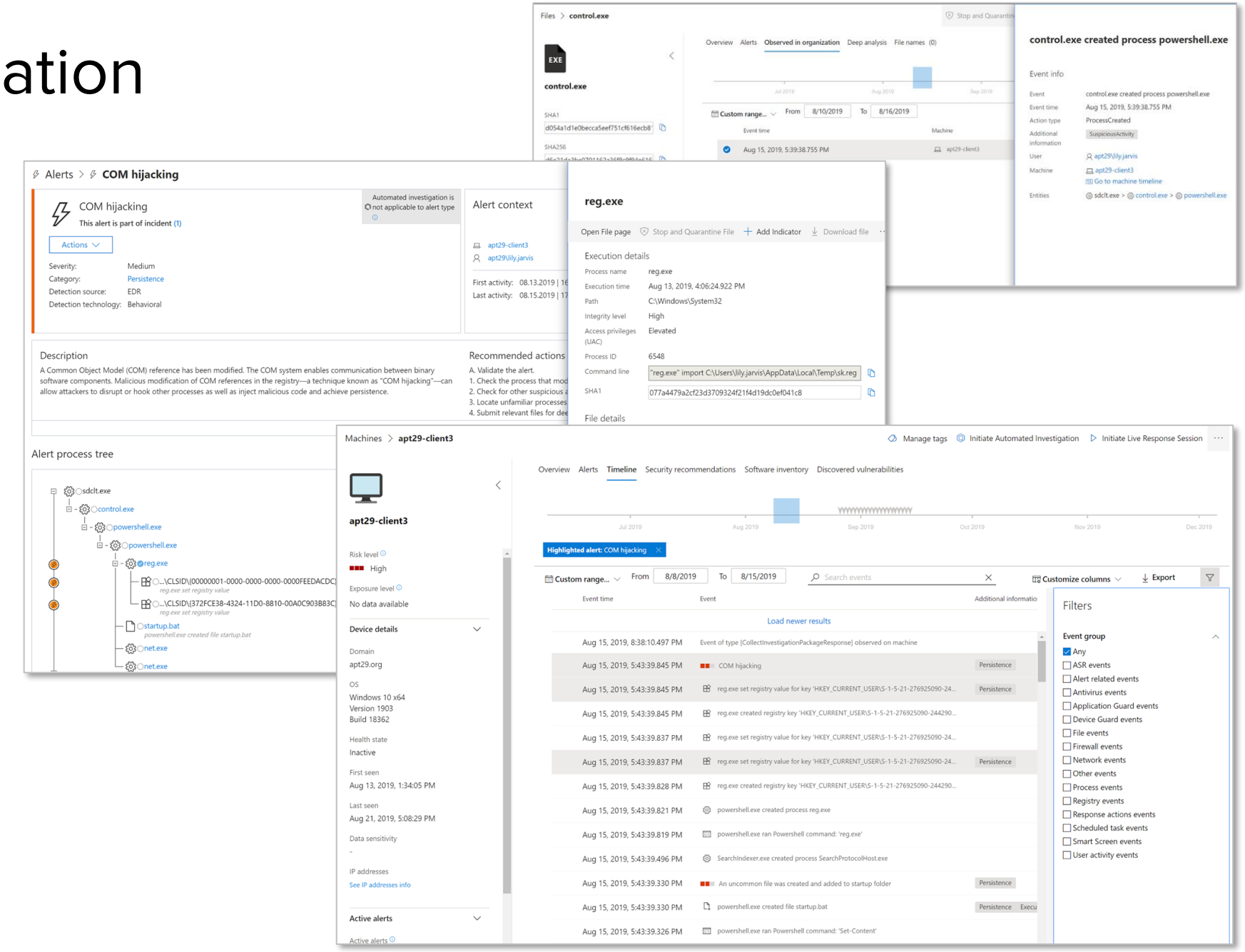
Full machine timeline to drill into activities, filter and search

Rich supporting data & tools

Supporting profiles for files, IPs, URLs including org & world prevalence, deep analysis sandbox

Expand scope of breach

In-context pivoting to other affected machines/users

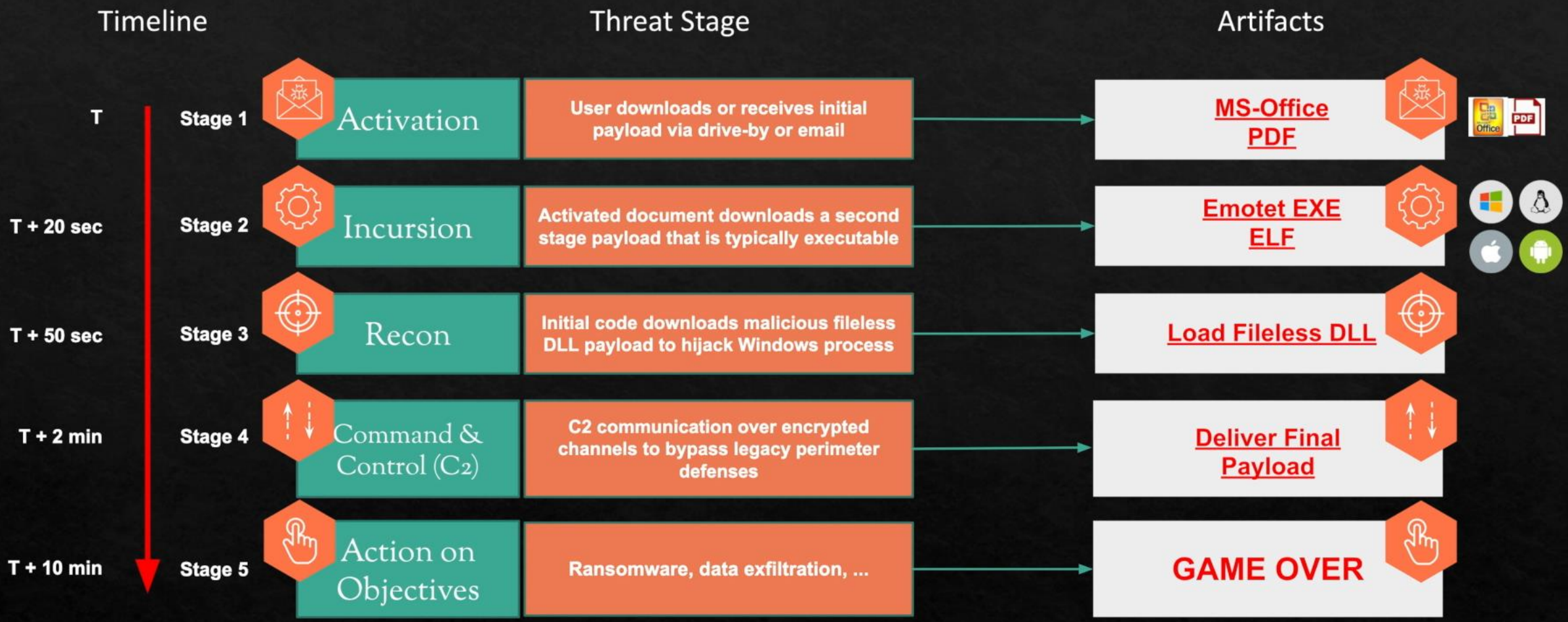


Microsoft

NDR and EDR DEMO

Dr. Arun Raman

BLUEHEXAGON



THANK YOU

Take it for a Test-Drive!

BLUEHEXAGON

Signup for a online demo and trial to get a 60-day free subscription https://bluehexagon.ai/ngndr-free-trial/

Microsoft

Signup for a online demo and trial https://aka.ms/mdatp