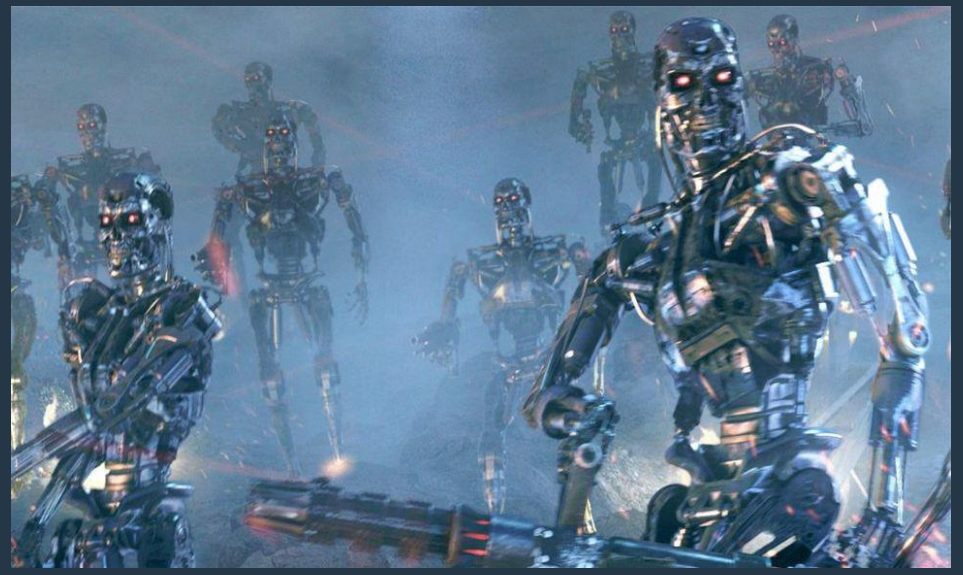
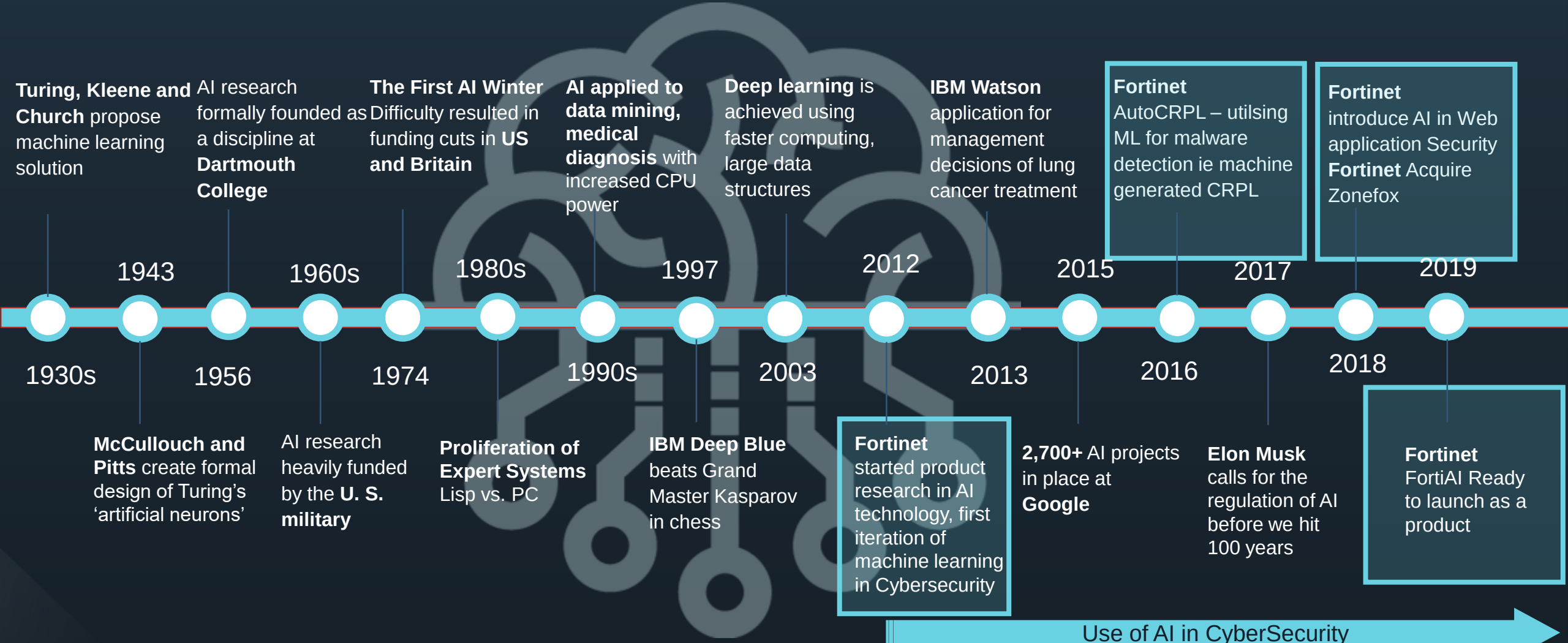
Demystifying AI

Jamie Graves
Vice President Security Analytics



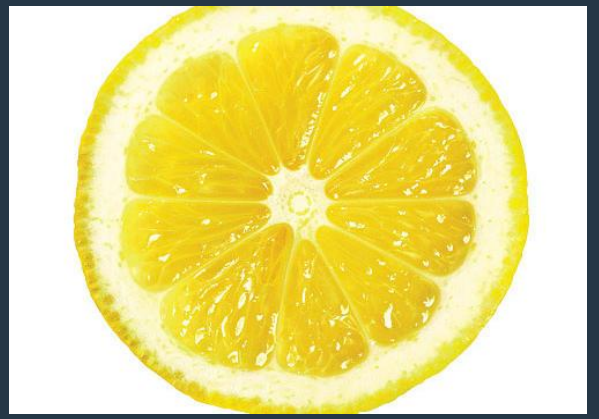
Artificial Intelligence – a Century of Hype…?

History of AI



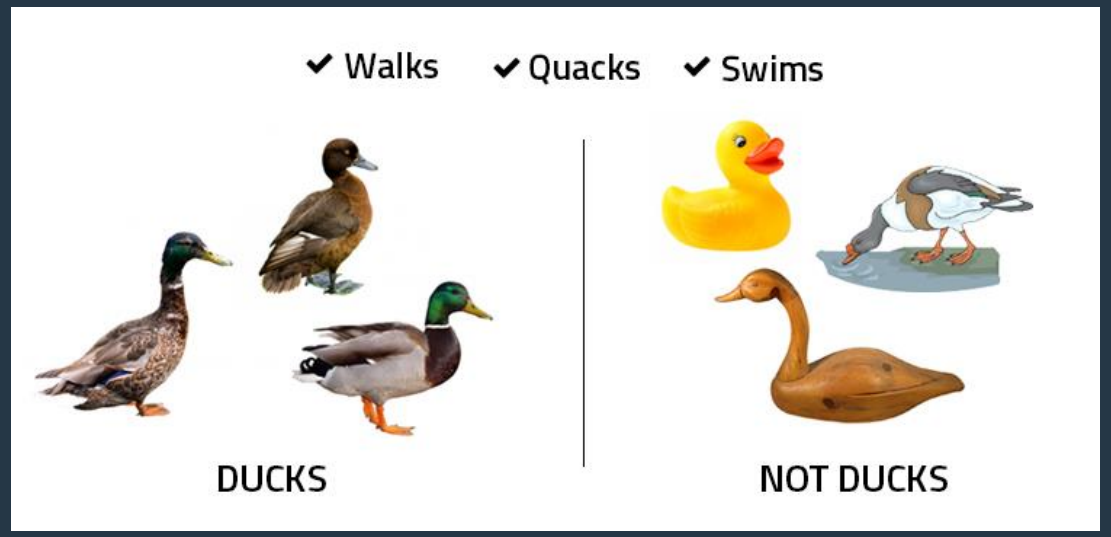




How do we use AI in Cyber Security?

- Classification



- Anomaly Detection

"Is this normal?"

SPAM

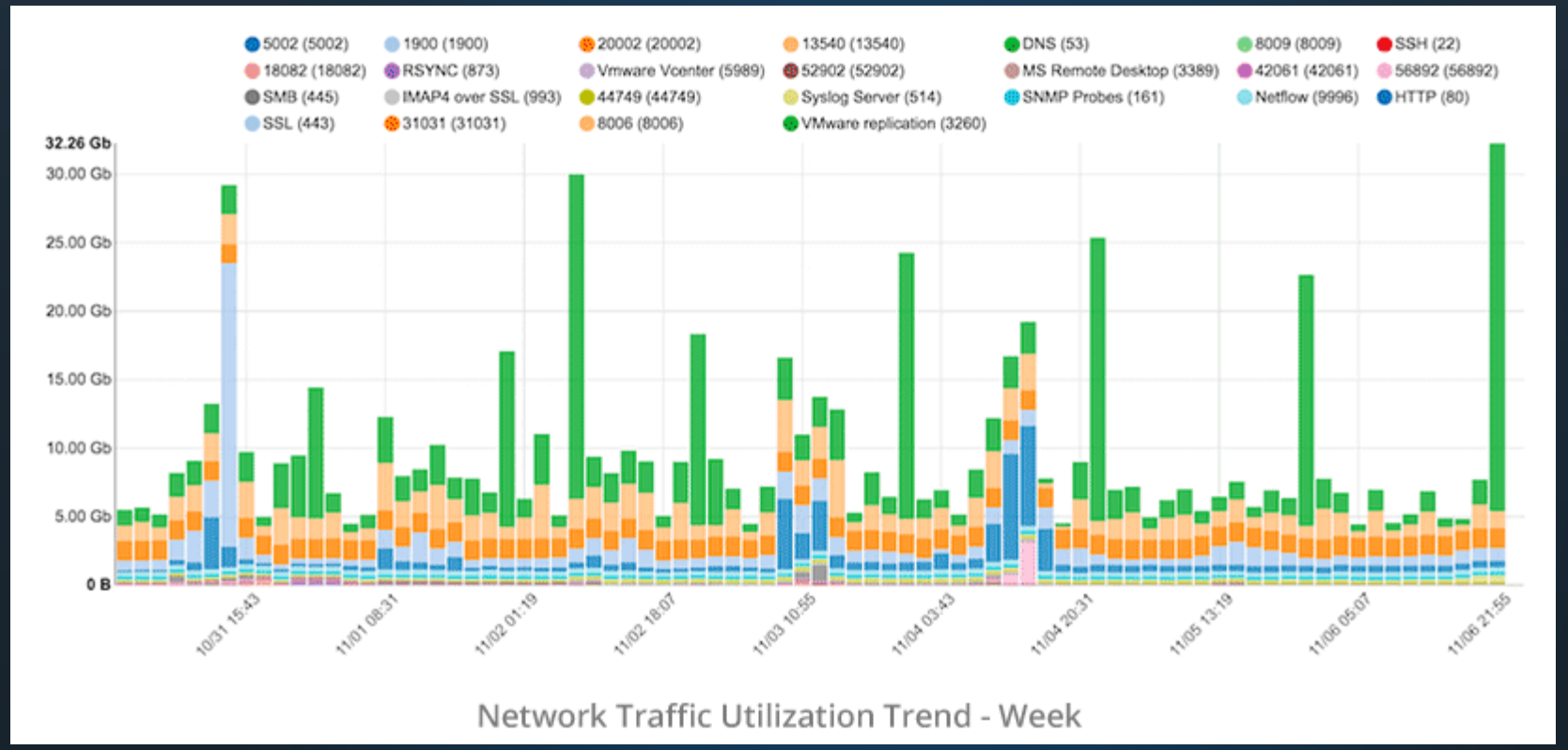
Classification

- Old
  - Known patterns/rules
  - Blacklists
- New
  - Bayesian techniques
  - ANNs

Network Intrusion Detection

Anomaly Detection

- Old
  - Hueristics –encode expertise and observations into rule-sets or at best ‘fuzzy’ rules
- New
  - Anomaly detection with ML
  - Create baseline, understand deviances, alert



Fortinet at the Bleeding Edge of Cyber AI

Cutting Edge Products and Services

FortiInsight

FortiSandbox

FortiGuard

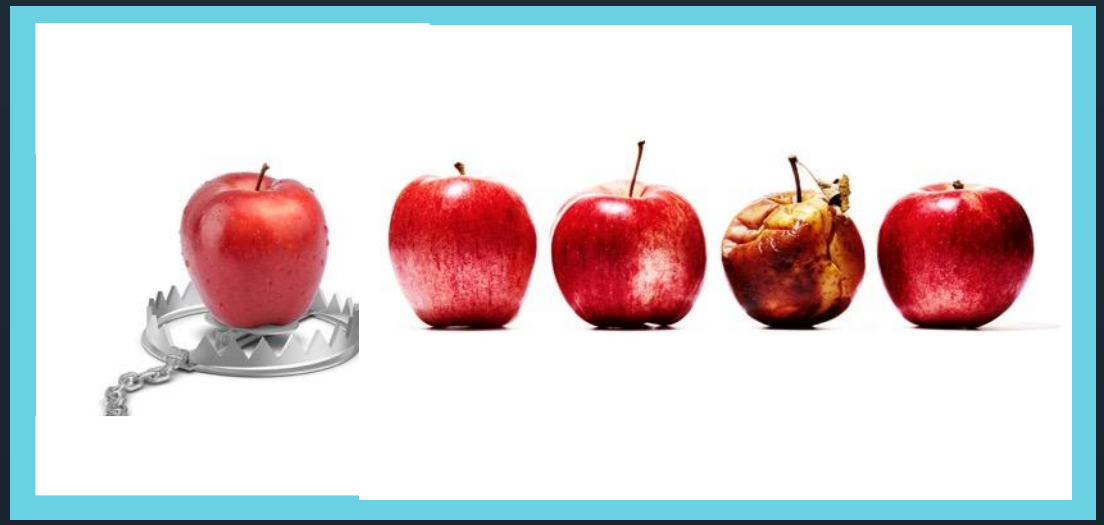
FortiClient

FortiAI

FortiWeb

AI Use Cases

Fortinet AI Products



AV Engine
inspect core of apple…..um it’s bad

AutoCPRL
let me describe it, rotten, smells...um it’s bad

FortiSandbox
let me take a bite……um it’s bad

FortiInsight
who’s the bad apple in the barrel?

FortiDeceptor
let me drop some apples…with traps

FortiAI
where do rotten apples come from?

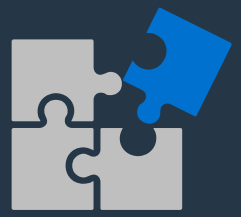
UEBA Machine Learning

For Anomalous Behavior Detection with FortiInsight

Machine Learning

- The FortiInsight Machine Learning capability allows users to detect ‘unknown unknowns’
  - For example: Leavers – Bob is about to leave his job, and his behavior has changed. This is hard to detect with rules alone

Profile Building



- Builds profiles of normal behavior so that it can detect abnormal behavior

Easy Setup

- Easy to set up and starts learning user behavior without configuration

User Tracking

- Uses UBA to track users and detect threats, by looking at patterns of human behavior

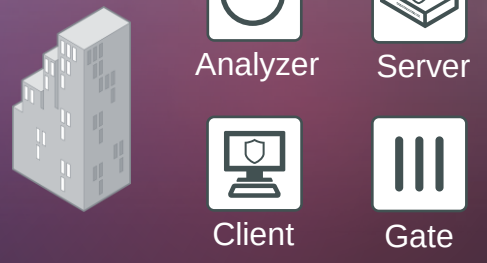
UEBA as a Service

Cloud-based AI Insights Service

Benefit from pooled insights across customer base

Frequent model updates

Telemetry

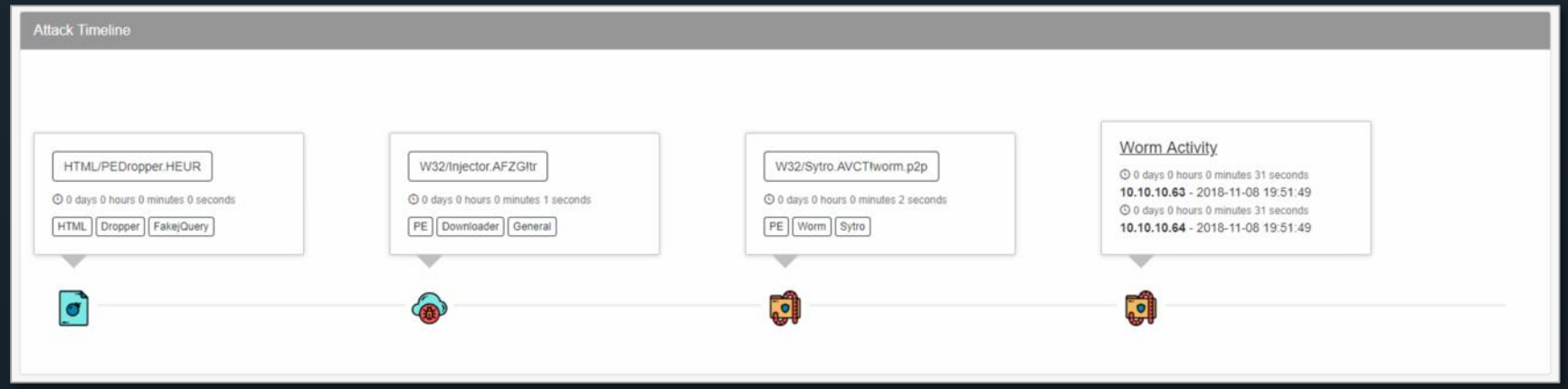


Fabric Response

FortiAI - Virtual Analyst

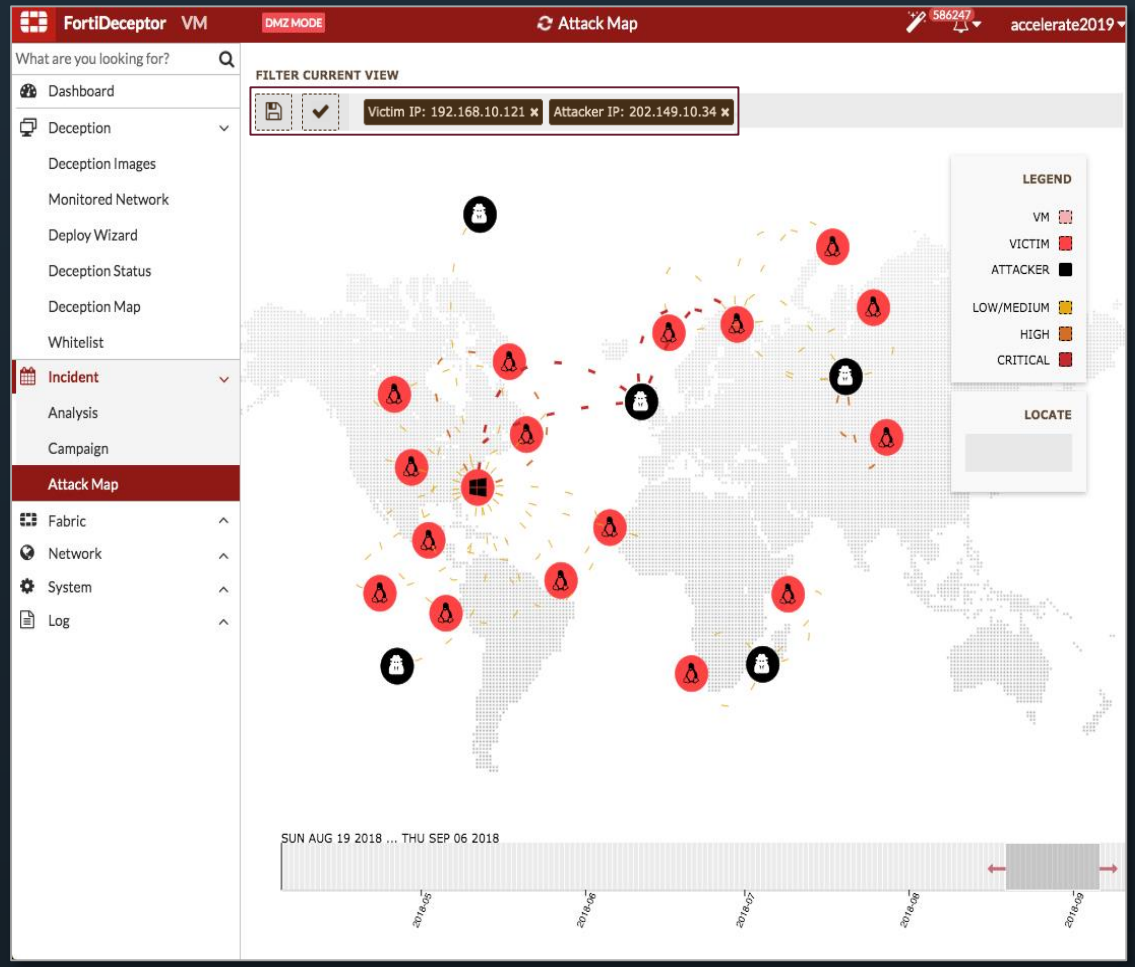
Attack Scenario & Story Mode

- Find the **Original Source of attack**
  - E.g. Attack scenarios learnt = malware-1 download malware-2
  - Find out How it was spread through the network
    - Sample-1 = {worm} on host1 has ability to spread via SMB
    - Sample-2 = {worm} on host**2**, src host1, port 445
    - Attack scenario learnt = sample-1 spreading within network via SMB (e.g. WannaCry)



Deception technology

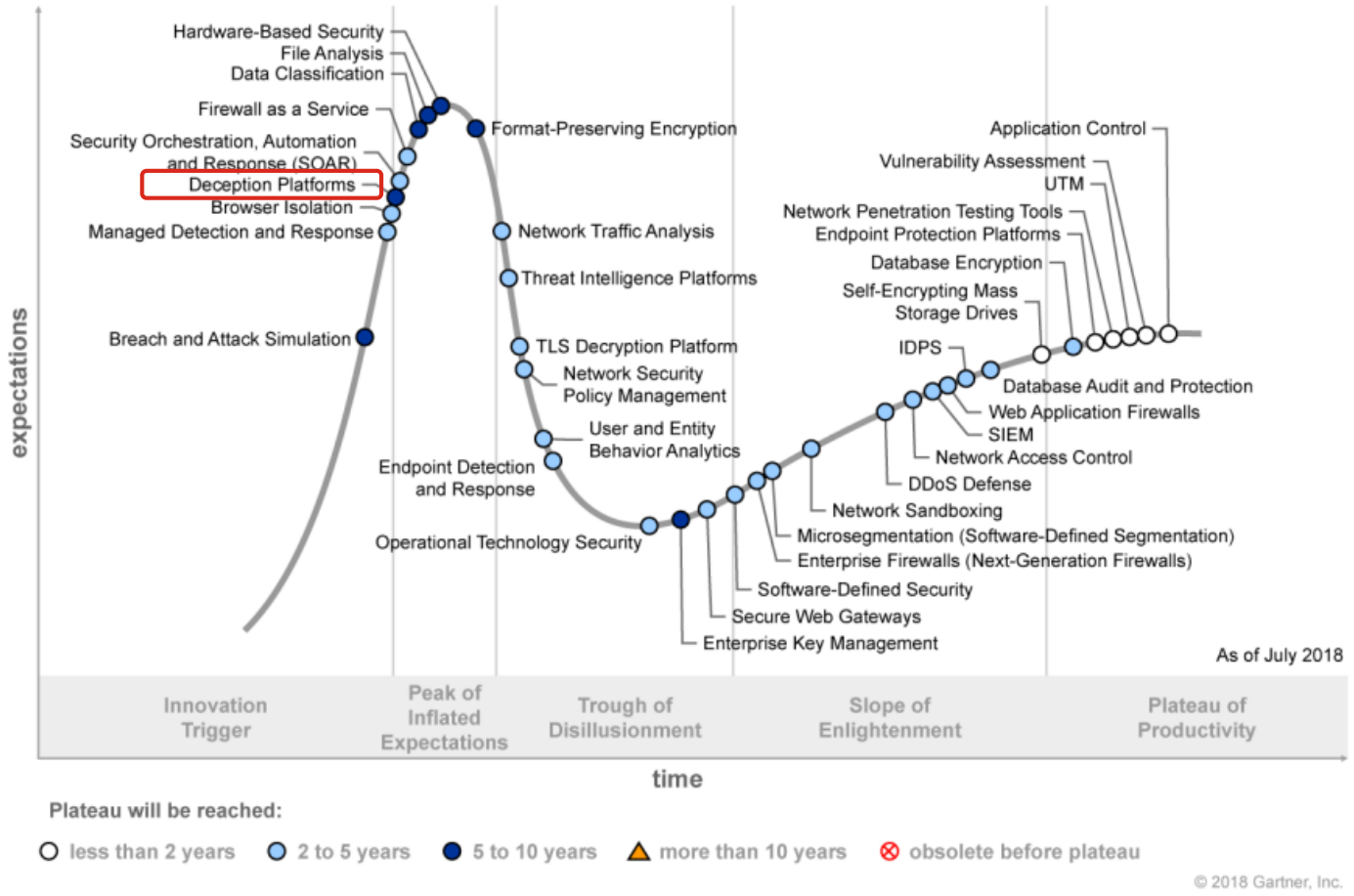
- Protects **critical assets**
- **Deception** technology will help to:
  - Divert attention from critical assets
  - Understand attackers profile
  - Gather more local intelligence



Gartner - Deception Technology Cycle

Innovation starts here

Figure 1. Hype Cycle for Threat-Facing Technologies, 2018



Source: Gartner (July 2018)

Deception Market – Target customers

- Gartner
  - Type A Enterprise aka ‘Lean forward Organization’
  - Revenue: $1B or more
  - Employee: 1,000 or more
- Business Unit
  - **More Mature** Security Operations
- Technology deployed
  - Sandbox, EDR, NGFW, SIEM, UEBA, NTA, SOAR, TIP *
- Top segments
  - Financial services, healthcare, government

Next Generation Fire Wall (NGFW), Endpoint Detection and Response (EDR), Security Information & Event Management (SIEM),
User & Entity Behavior Analytics (UEBA), Network Traffic Analysis (NTA), Security Orchestration, Automation & Response (SOAR), Threat Intelligence Platform (TIP)

Operational Cyber M.L.

Operational Cyber M.L.

Conclusion

- AI is everywhere and is often cited as the solution to all of our problems
- AI is a very useful tool, but currently it's only good at things it's been designed to do
- In cybersecurity AI can be used for classification or anomaly detection
- Fortinet have leading AI products to help you solve a number of critical cyber security issues


FORTINET