AI Virtuálny Bezpečnostný Analytik pre SecOps

Peter Kocik
Systems Engineer CEE

One –Two Punch

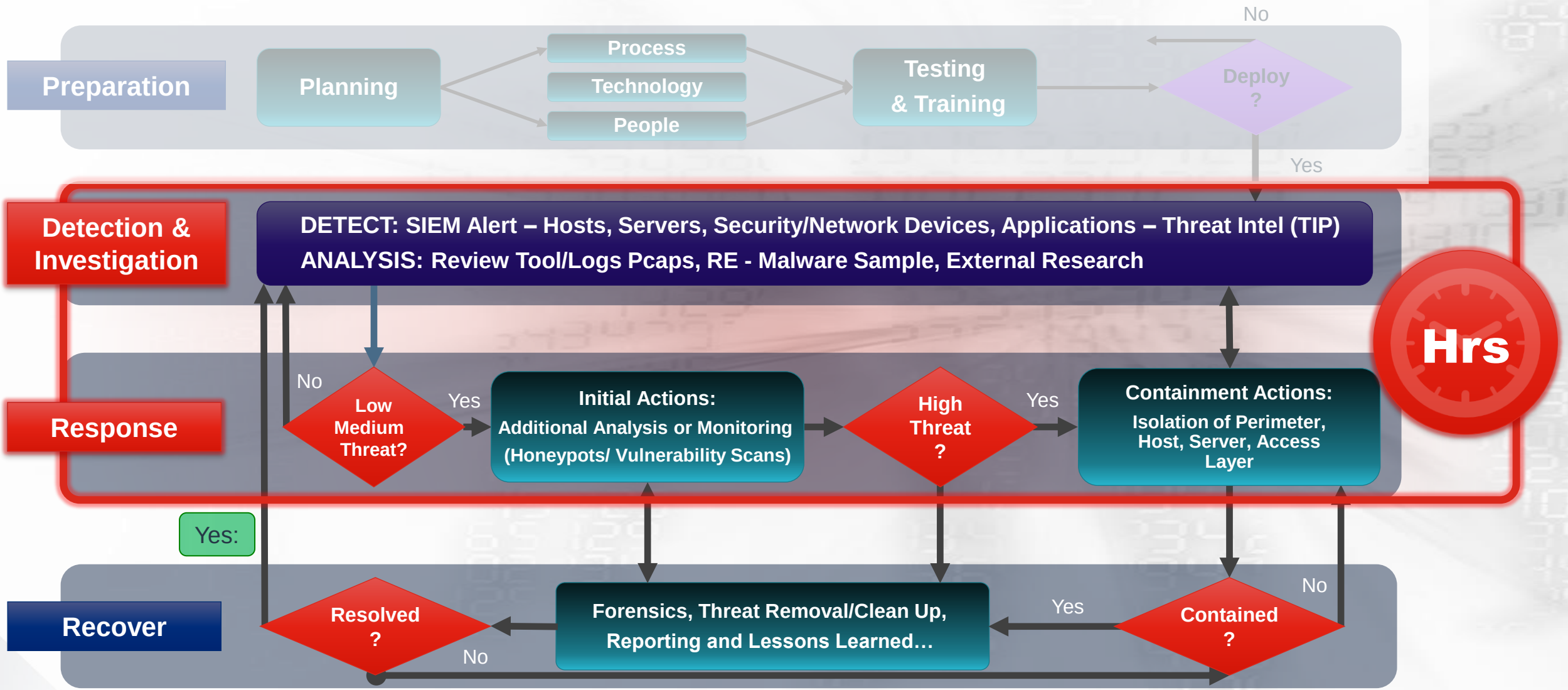
Targeted Ransomware Attacks

Data Exfiltration

Drop Destructive Payload

FORTINET

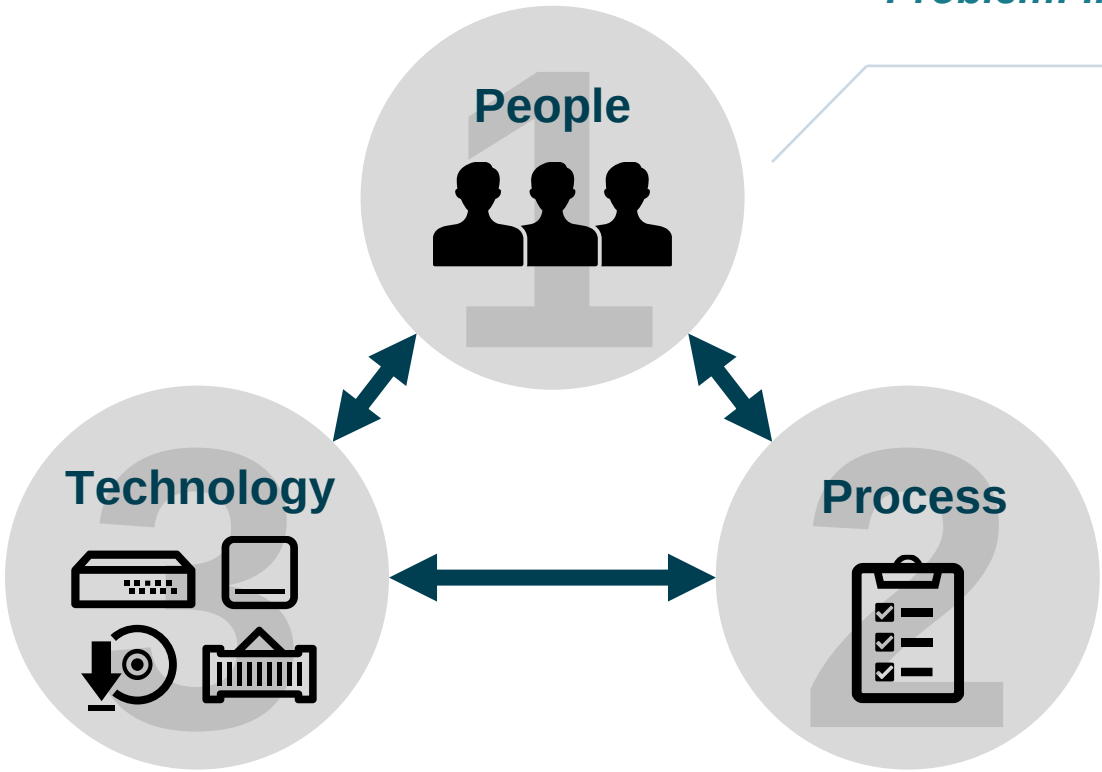
Incident Response Process



Traditional SecOps Approach

Human element that consist of SecOps analyst(s) that manage security technologies and drive threat resolution within a well defined process

Problem: InfoSec Shortage



Products that provides threat visibility and response actions

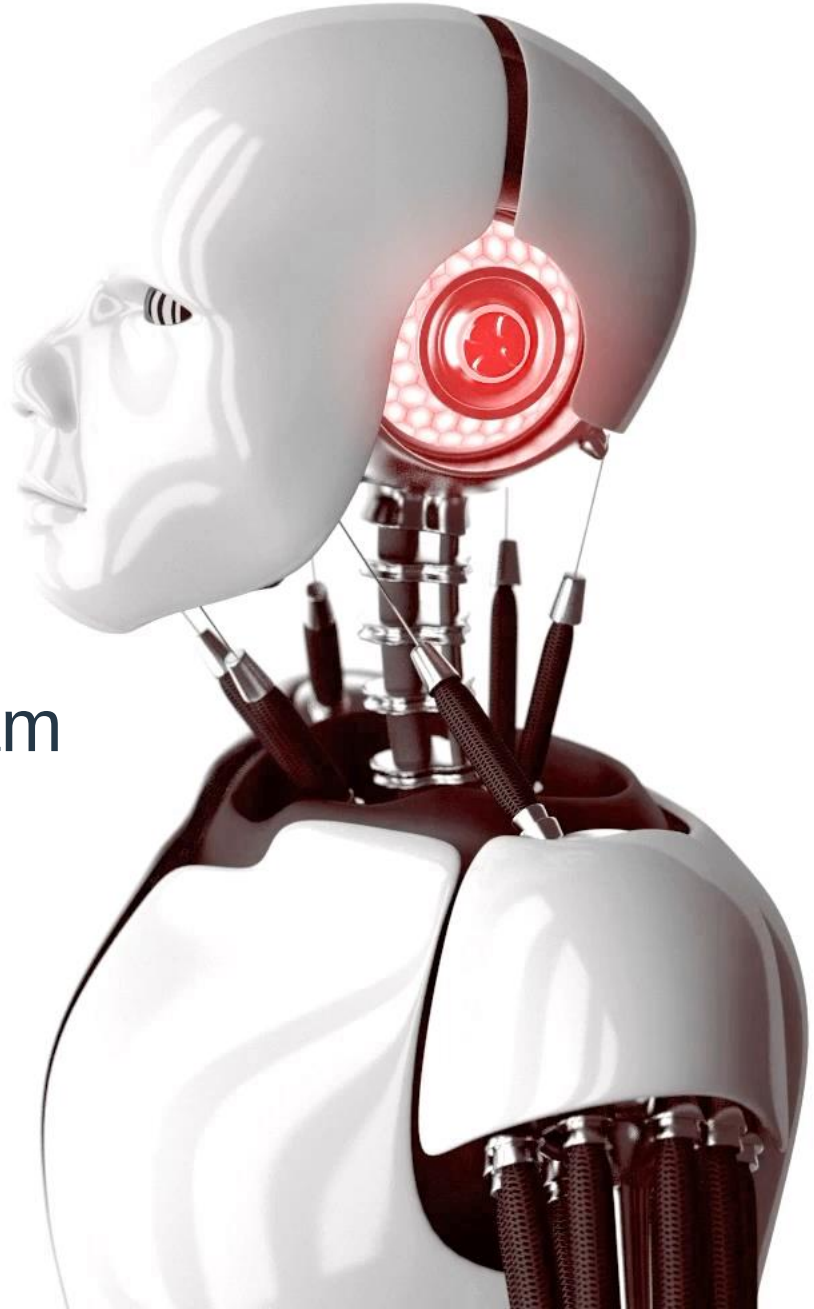
Problem: Traditional Detection

A systematic approach to detect, investigate and respond to threats

Problem: Manual Processes

FortiAI

Virtual FortiGuard Analyst on your team



FORTINET

Virtual Security Analyst™ powered by Deep Neural Networks that **identifies**, classifies, and investigates sophisticated threats in sub-second, and proactively blocks them.

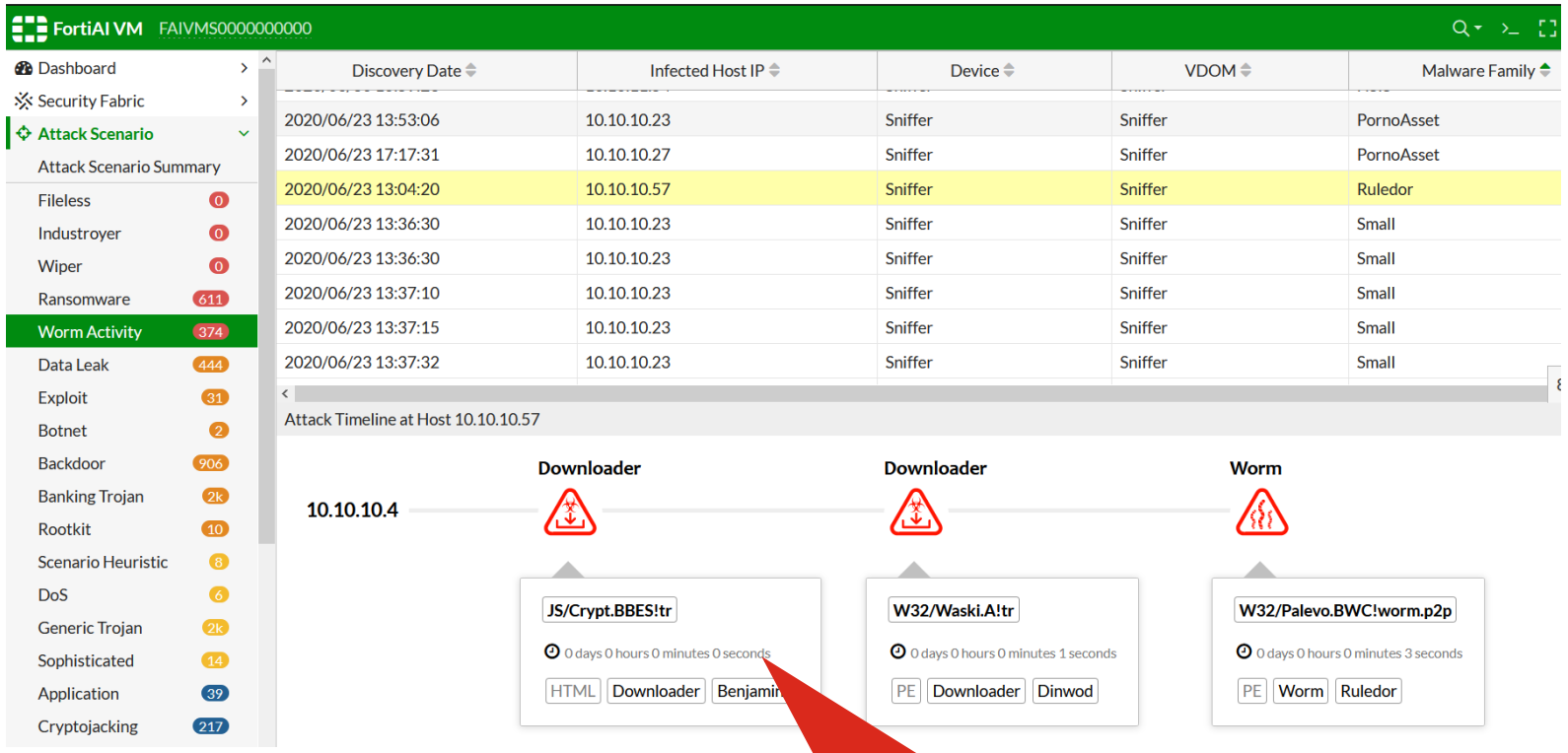
1

Identify

Disrupt threats with sub-second detection and adapts to new threats instantaneously.

Solves

SecOps are facing increased volume, velocity and sophistication of threats



Virtual Security Analyst™ powered by Deep Neural Networks that identifies, **classifies**, and investigates sophisticated threats in sub-second, and proactively blocks them.

2

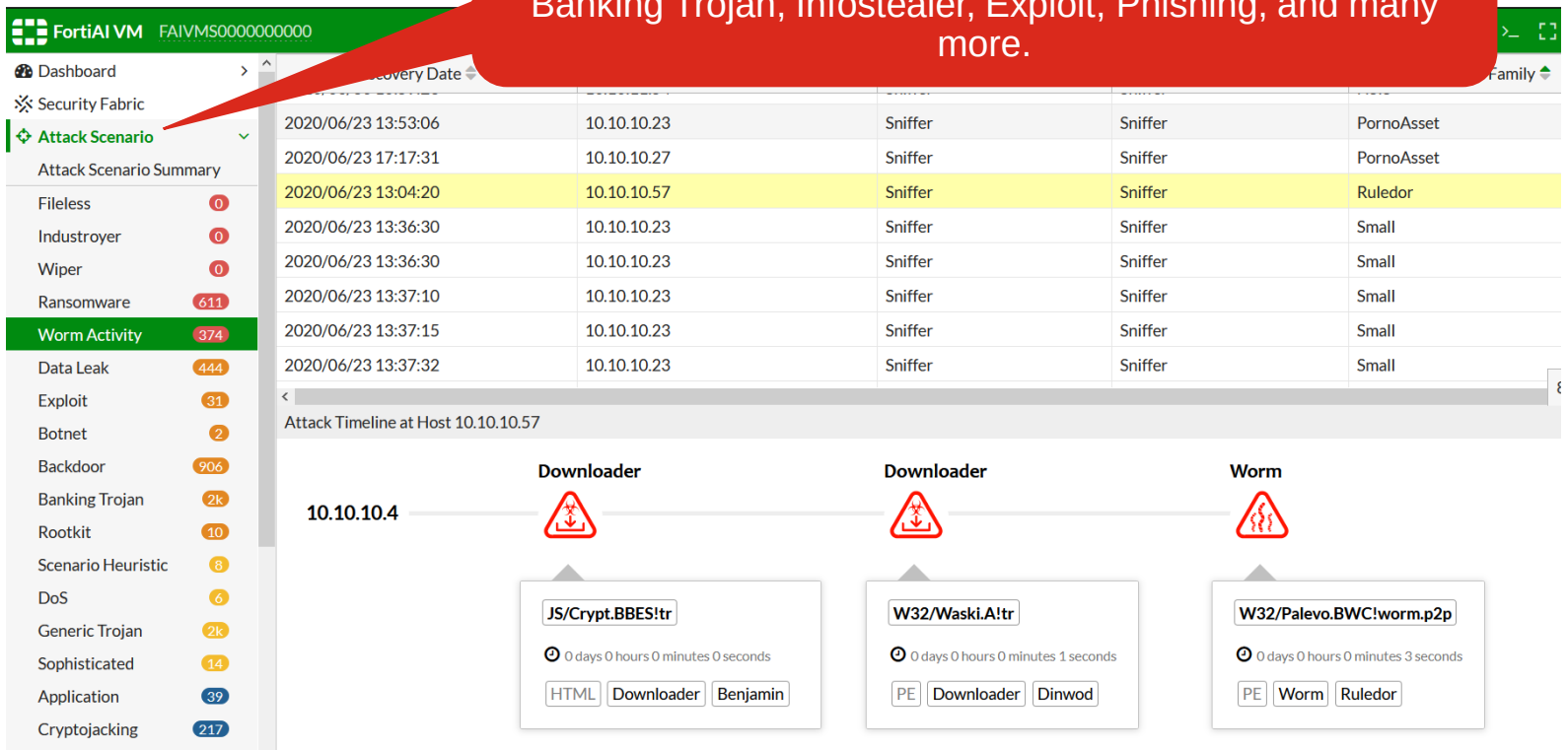
Classify

Scientifically analyze IT and OT malware to accurately determine the type of threat and reduces false positives.

Solves

Masquerading malware evades security controls and prolongs mitigation effort.

Classify IT and OT threats: Industroyer, Wiper, Fileless, Ransomware, Worm, Downloader, Dropper, Rootkit, Banking Trojan, Infostealer, Exploit, Phishing, and many more.



Virtual Security Analyst™ powered by Deep Neural Networks that identifies and classifies, and **investigates** sophisticated threats in sub-second, and proactively blocks them.

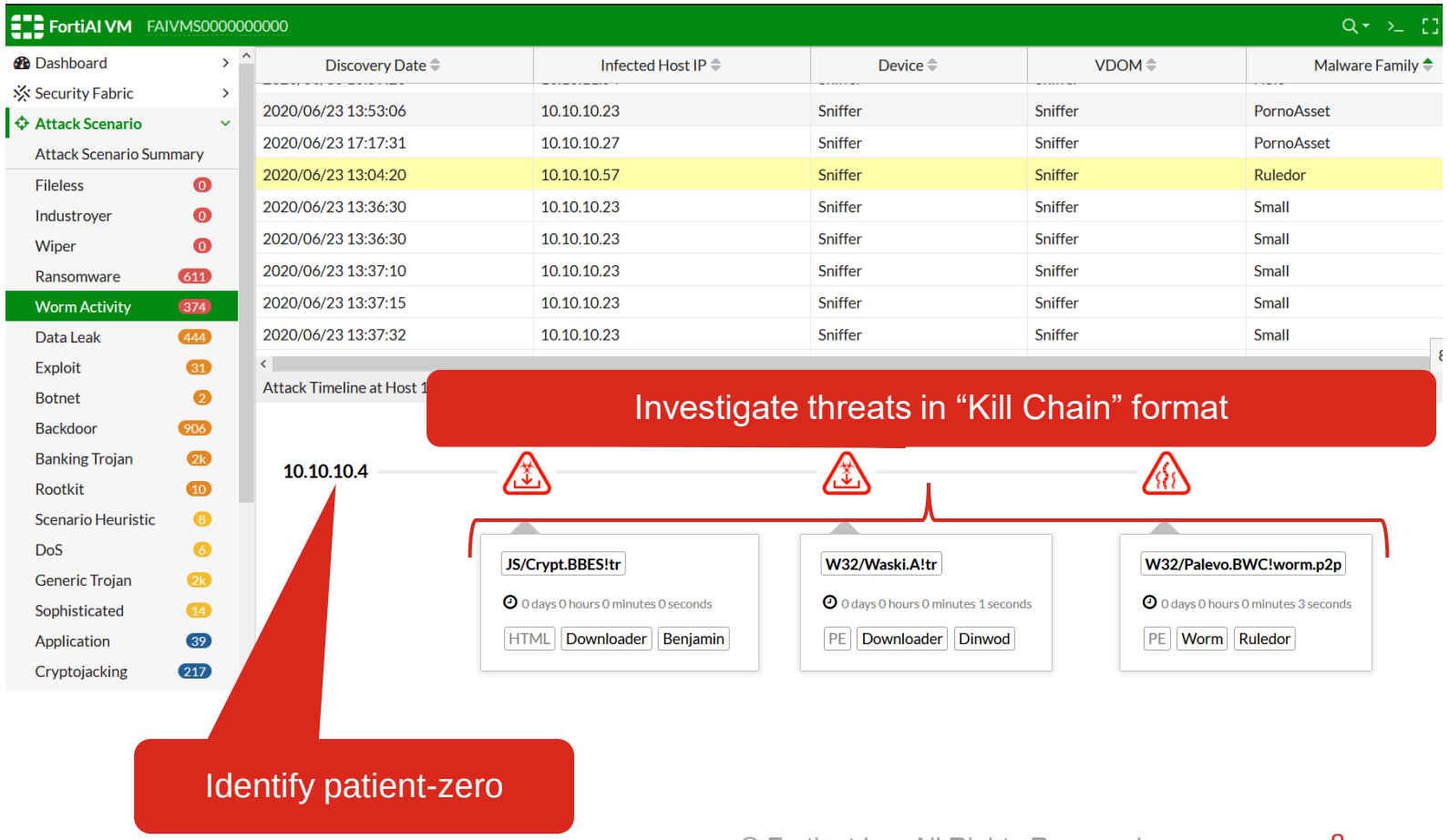
3

3 Investigate

Speeds investigation by analyzing the entire threat movement and identifies patient zero and subsequent victims in real-time.

Solves

Manual investigation of a malware outbreak/lateral spread



Virtual Security Analyst™ powered by Deep Neural Networks that identifies and classifies, and investigates sophisticated threats in sub-second, and proactively **blocks** them.

4

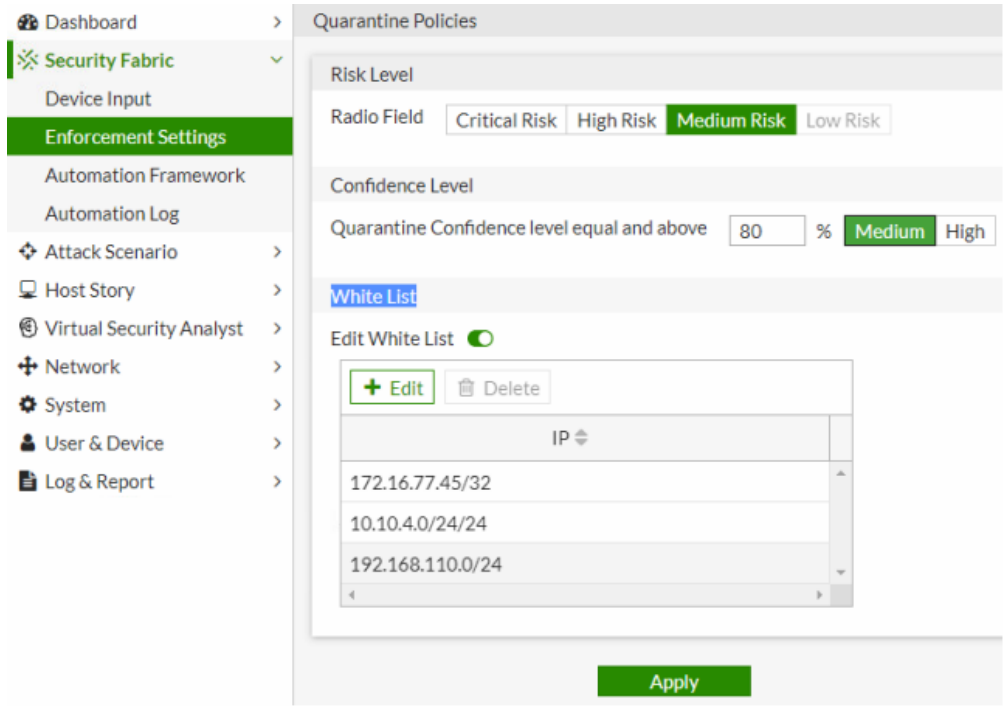
4

Automated Response

Quarantines these threats in real-time found in the network through the seamless integration with FortiGate.

Solves

Manual mitigation efforts to an on-going attack or an outbreak scenario



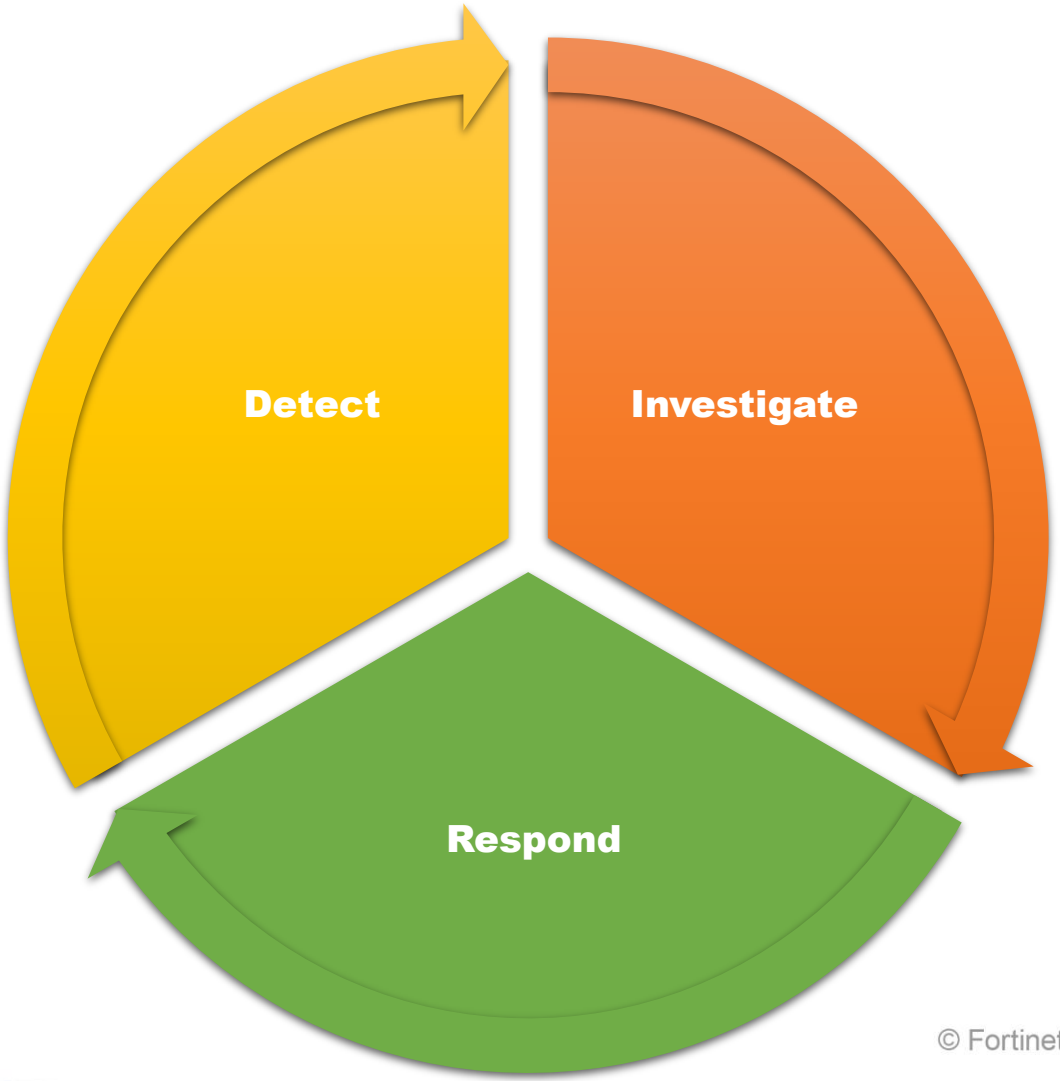
FortiGate quarantine based on FortiAI risk & confidence levels

Example: WannaCry Response Life Cycle

The traditional approach with SecOps analysts only

Detect (1+ hrs)

- Assume out of 100's – 1000's threats alerts on a SOC dashboard, threat selected happen to be ransomware or,
- Alerted directly by an affected user



Investigate (4+ hrs)

- Log into security product(s)
- Review logs/alerts
- Use built-in and external tools to validate ransomware
- Perform external research
- Log into security product(s) to search for WannaCry's lateral movement
- Create mitigation plan

Respond (2+ hrs)

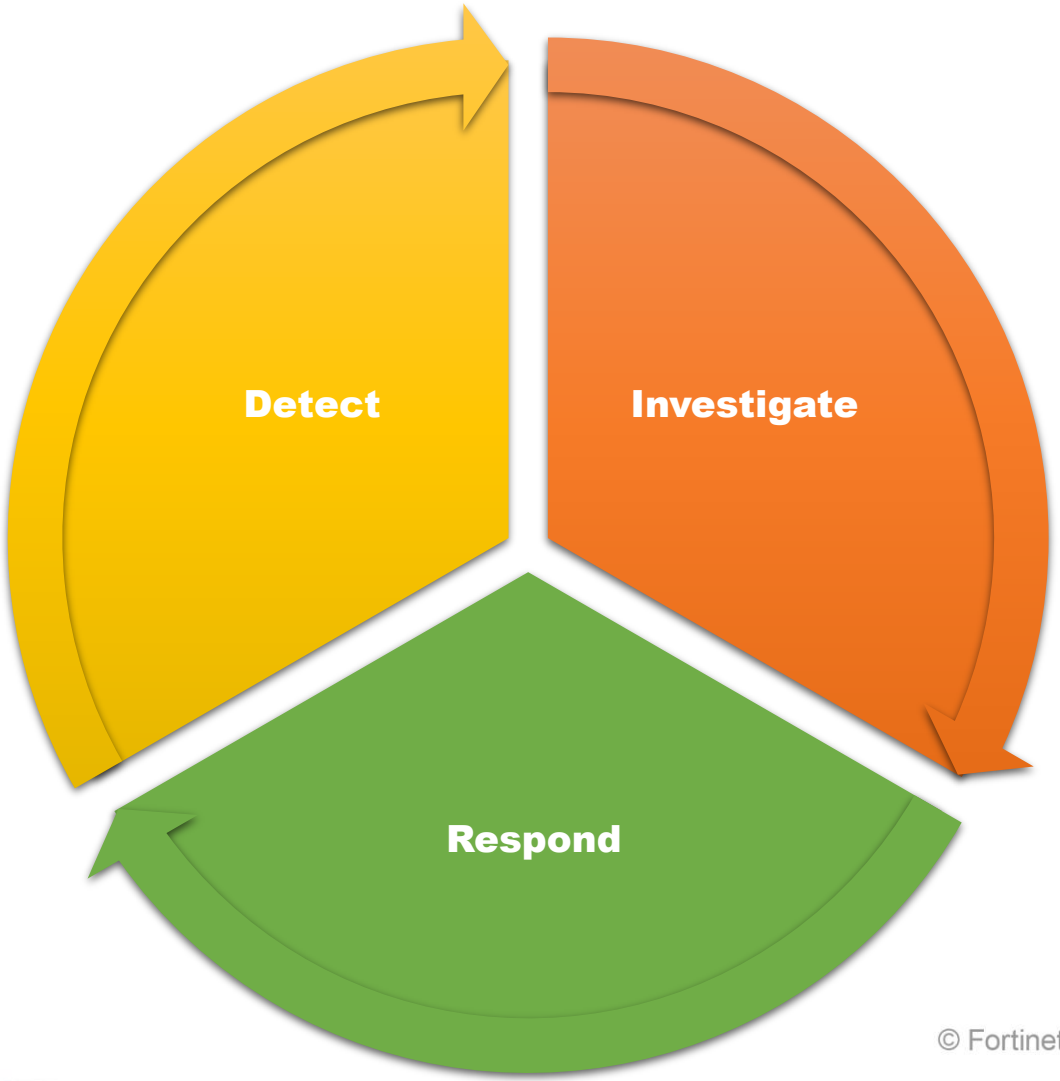
- Quarantine devices(s), network segment
- Remediate device(s)/restore back-up
- Apply patches
- **Close ticket**

Example: WannaCry Response Life Cycle

SecOps analyst augmented with Deep Neural Networks (AI)

Detect (<1 ms)

- AI: Ransomware validated in sub-second
- AI: Self-learns new ransomware features



Investigate (<5 mins)

- AI: Provides WannaCry kill-chain with contextual threat research
- AI: Identify WannaCry patient-zero & lateral movement
- SecOps: Create mitigation plan

Respond (<30 mins)

- AI integrated with Security Controls:
  - Quarantine devices(s), network segment
- SecOps follow-up:
  - Remediate device(s)/restore back-up
  - Apply patches
- Close ticket

BMW i Motorsport
Official Partner