Managed Security Services in The Age Of Artificial Intelligence

February 2020

Nikitas Kladakis
Information Security Director

A new Era in Threat Landscape

netbull

A New Era in Threat Landscape – AI

Changes in the landscape of threats - AI

- Expansion of existing threats
- Introduction of new threats
- Change to the typical character of threats

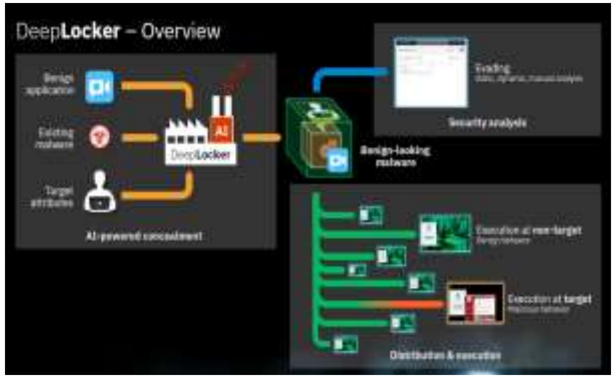
AI Data Breach Scenarios

AI Malware

AI Malware

- Hackers have even started using AI to accelerate polymorphic malware, causing code to constantly change and make it undetectable

- Advanced tactics allow hackers to work around security to bypass facial security and spam filters, promote, fake voice commands and bypass anomaly detection engines



AI Social Engineering

Social Engineering

- Victims' online information is used to automatically generate custom malicious websites/emails/links they would be likely to click on, sent from addresses that impersonate their real contacts, using a writing style that mimics those contacts.

- As AI develops further, convincing chatbots may elicit human trust by engaging people in longer dialogues, and perhaps eventually masquerade visually as another person in a video chat.

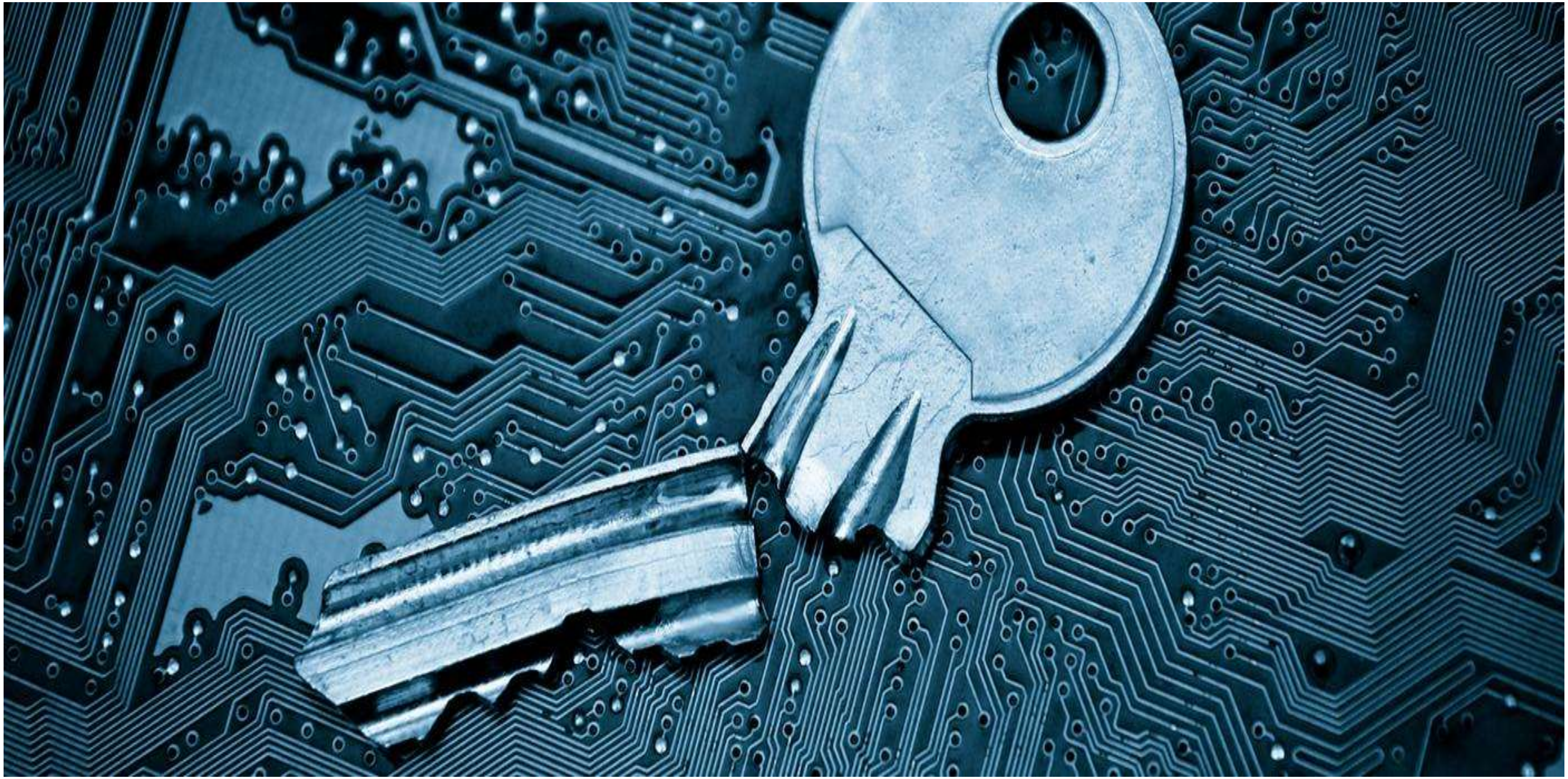
APT: Automation of hacking

Automation of Hacking

- AI is used (autonomously or in concert with humans) to improve target selection and prioritization, evade detection, and creatively respond to changes in the target’s behavior

- Autonomous software has been able to exploit vulnerabilities in systems for a long time, but more sophisticated AI hacking tools may exhibit much better performance both compared to what has historically been possible and, ultimately (though perhaps not for some time), compared to humans

Vulnerability Discovery



Vulnerability Discovery

- **Generate new payloads to find out new issues:** It is entirely different from the usual approach. Attackers first have to generate unusual behavior and then use it to discover payload.
- **How attackers generate it?** Attackers put the unusual data in request fields and allow target service to create an abnormal response. This is where the Artificial Intelligence comes into existence. It analyses already revealed payloads for accessible vulnerabilities and proposes new payloads to find out new issues with improved probability

Smart Botnets

Smart Botnet

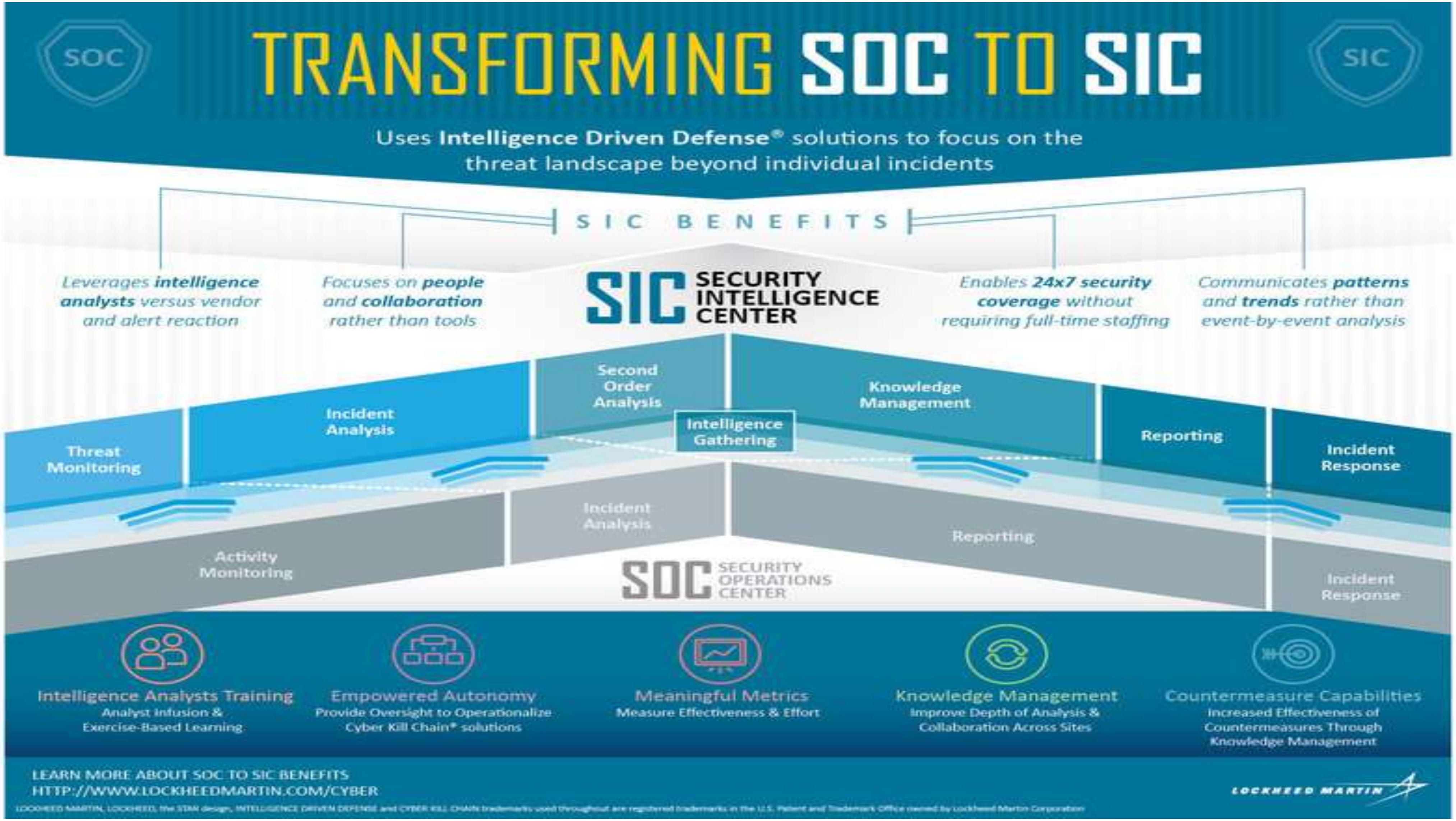
- **Simple:** the devices will able to talk to each other and make decisions based on shared local intelligence.

- **AI**, the zombies will be smarter and free from botnet herder intervention to take action on commands. As a result, there will be an exponential growth of hivenets as swarms.

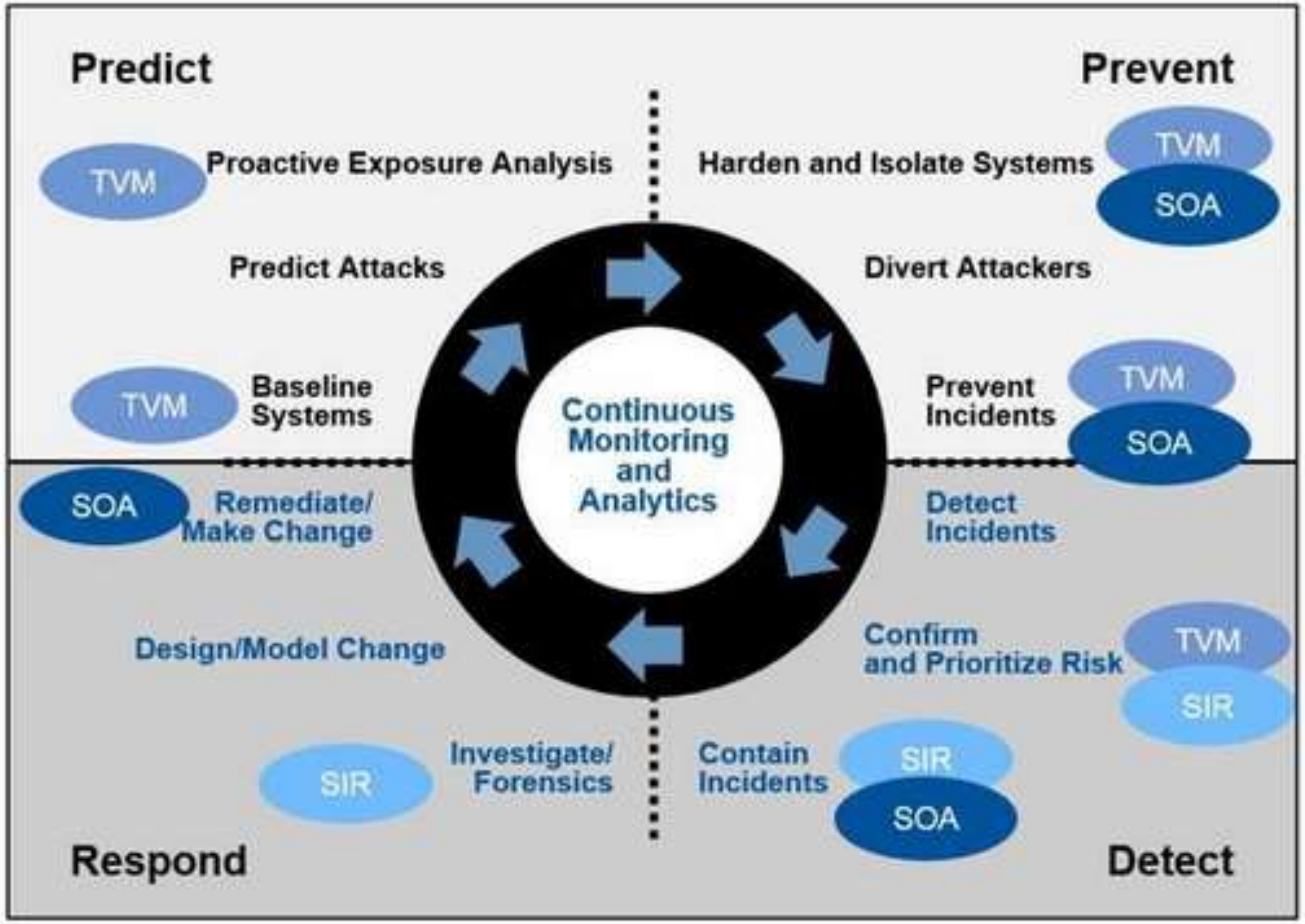
Managed Security Services (based on AI)

netbull

Security Intelligence Center (i-nSOC)



Corner Stones of our Intelligence based MSS

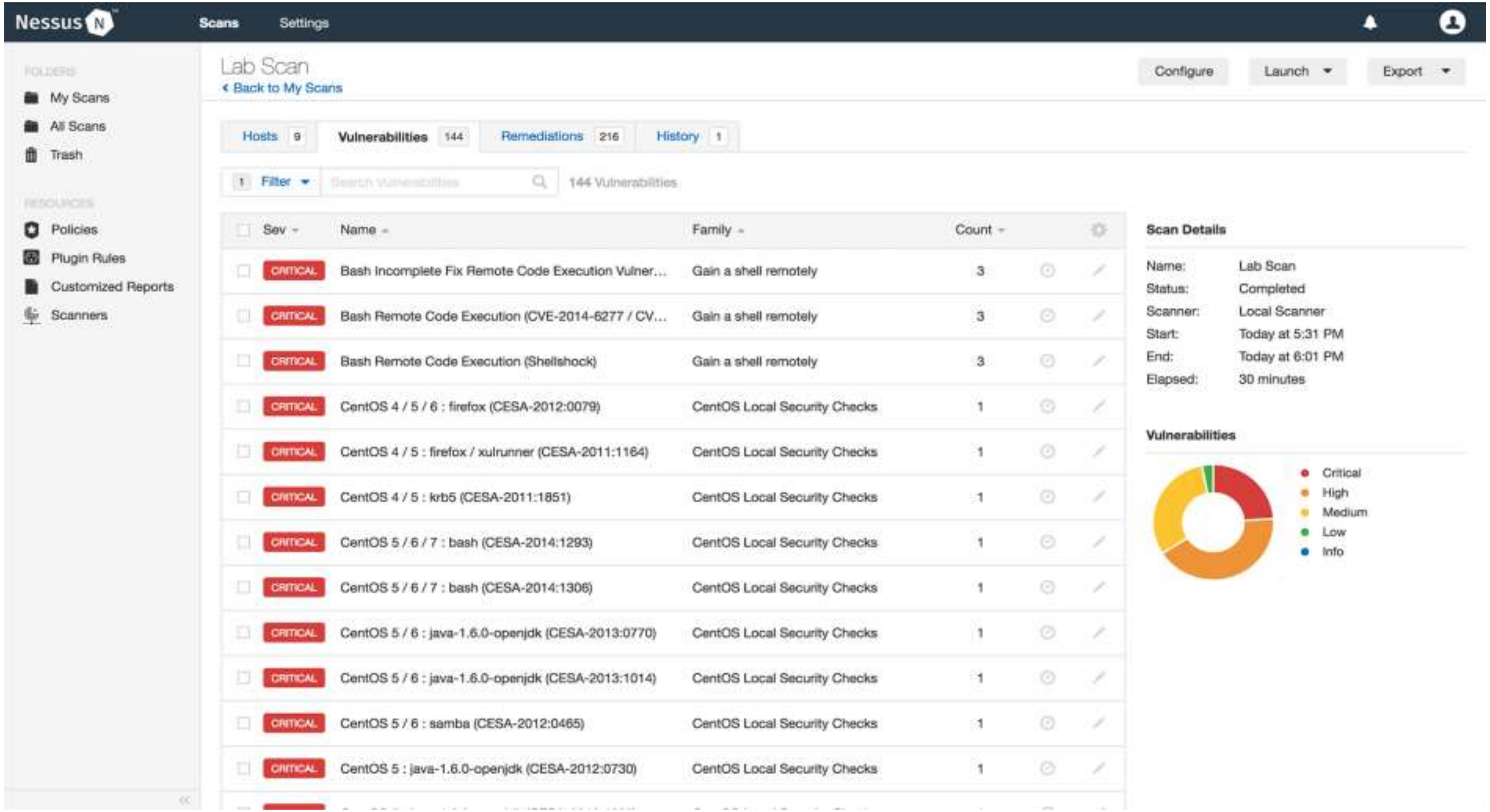


Predict

Threat Intelligence Services

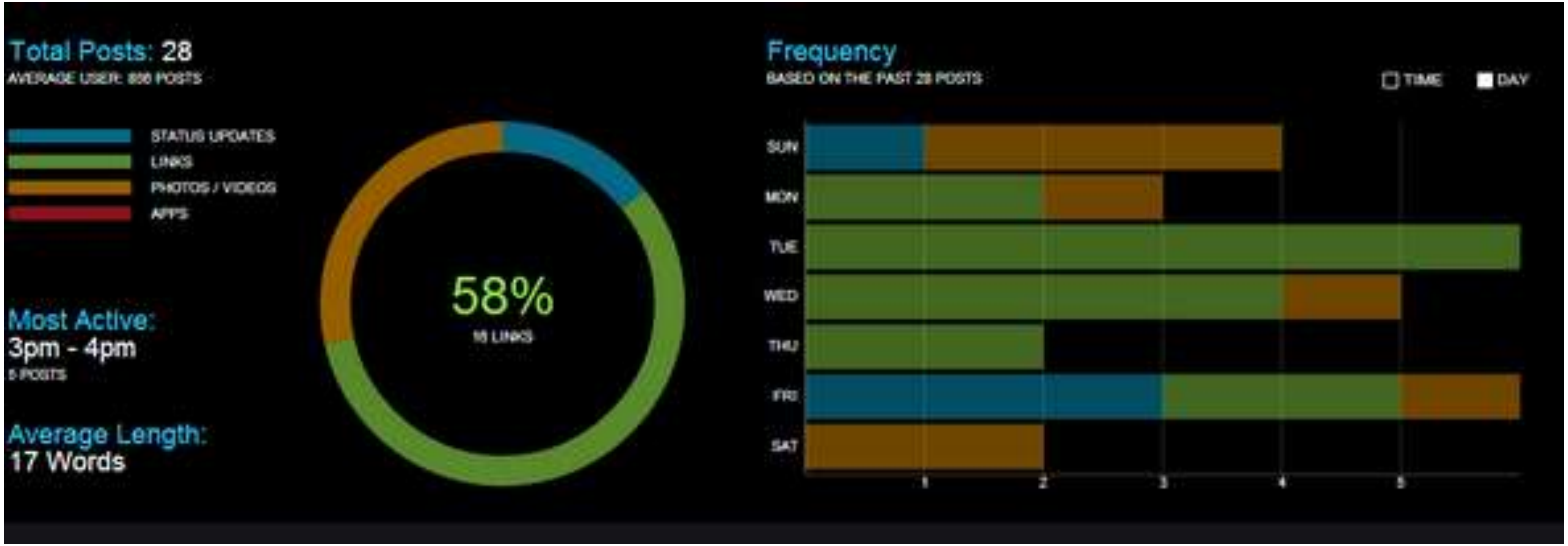
- IP Reputation Feed
- Malicious URLs Feed
- Phishing Feed
- Botnet C&C URLs Feed
- Ransomware URL Feed
- APT IoC Feeds
- DNS Feeds
- IoT URL Feed
- Malicious Hash Feeds
- Social Network Feeds

Vulnerability Assessment Services



Early Warning Intrusion Detection Services (EWS)

Digital Risk Monitor Services

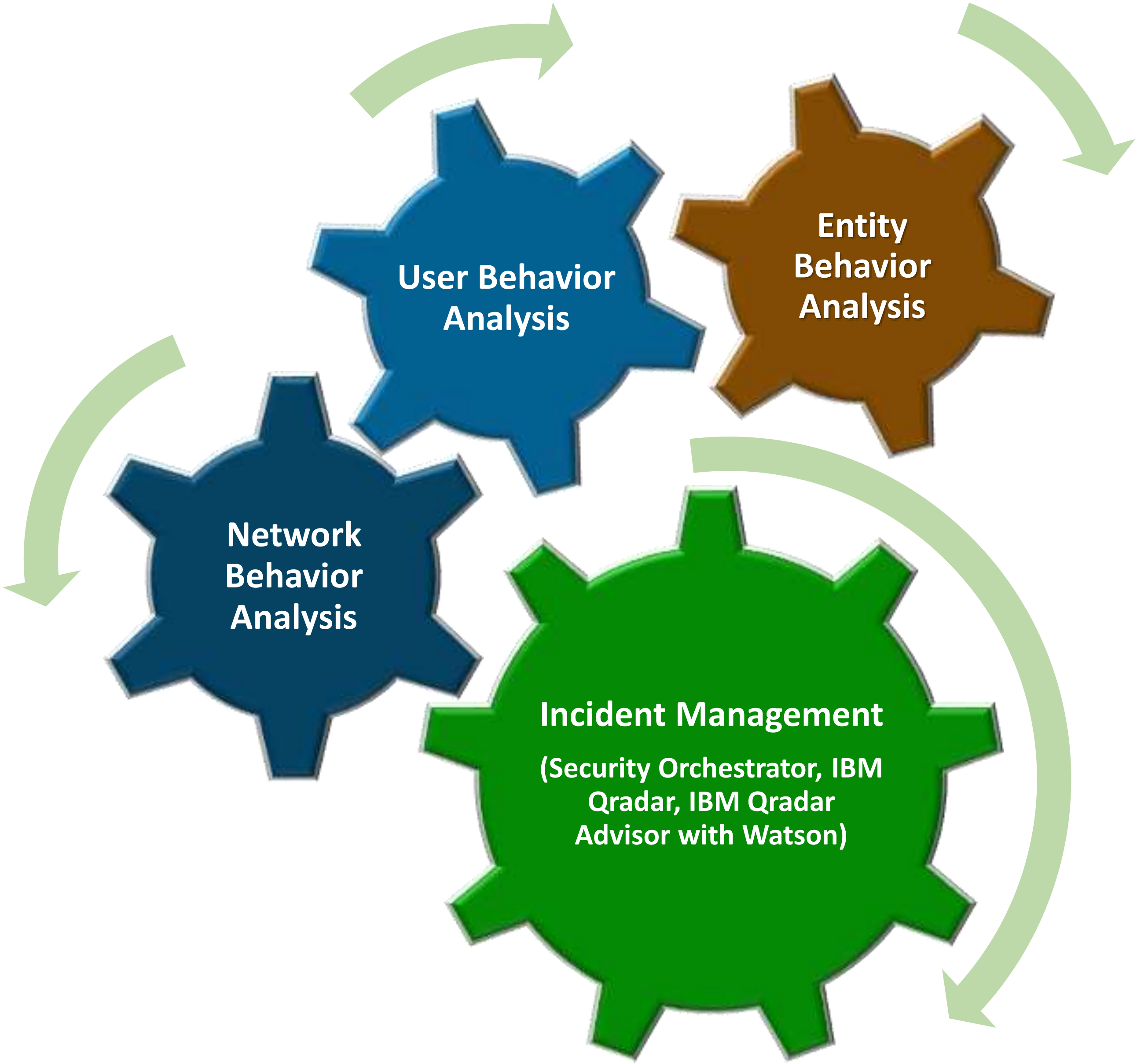


Prevent

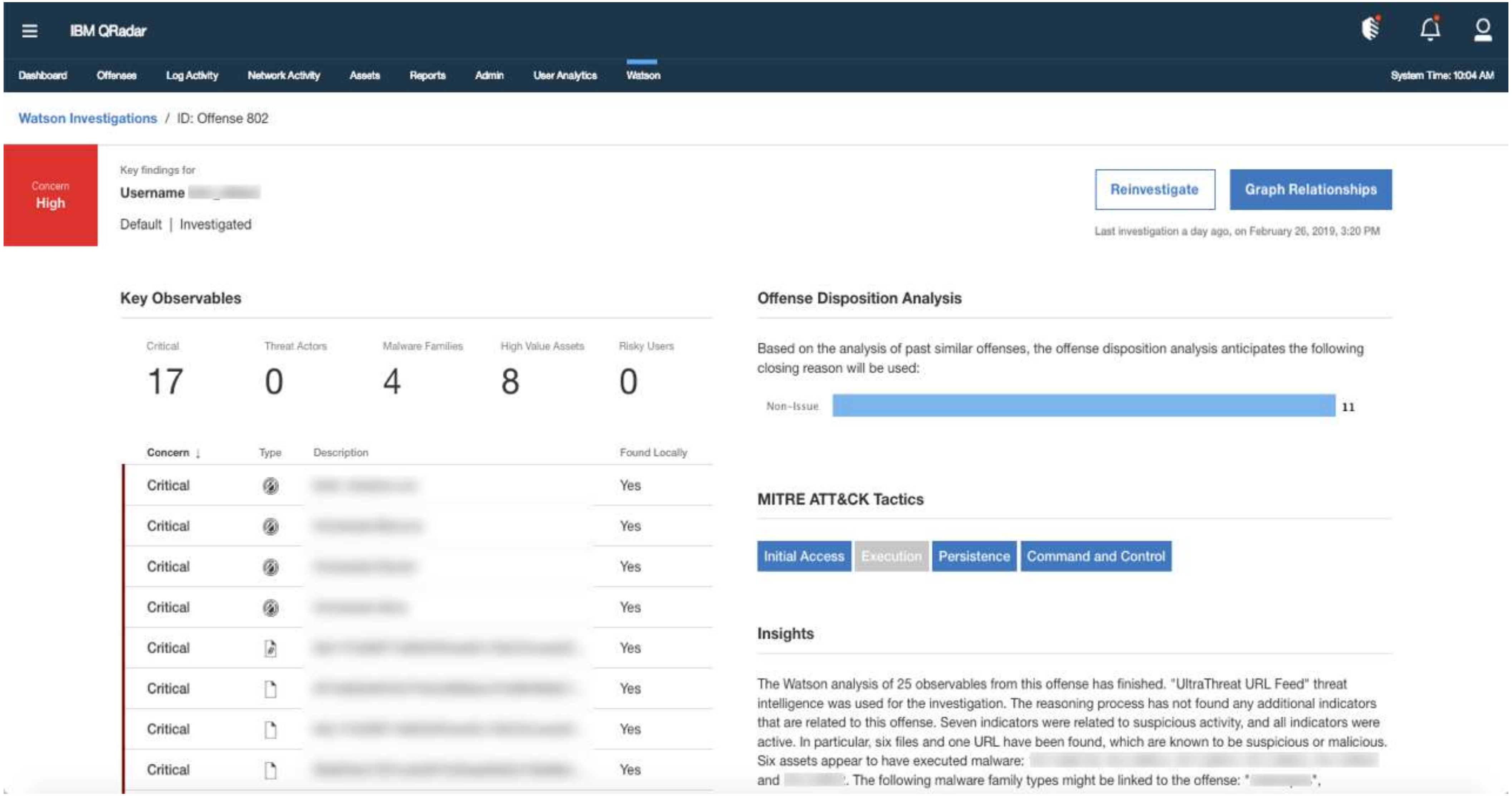
netbull 3D AI Security Architecture

Detect

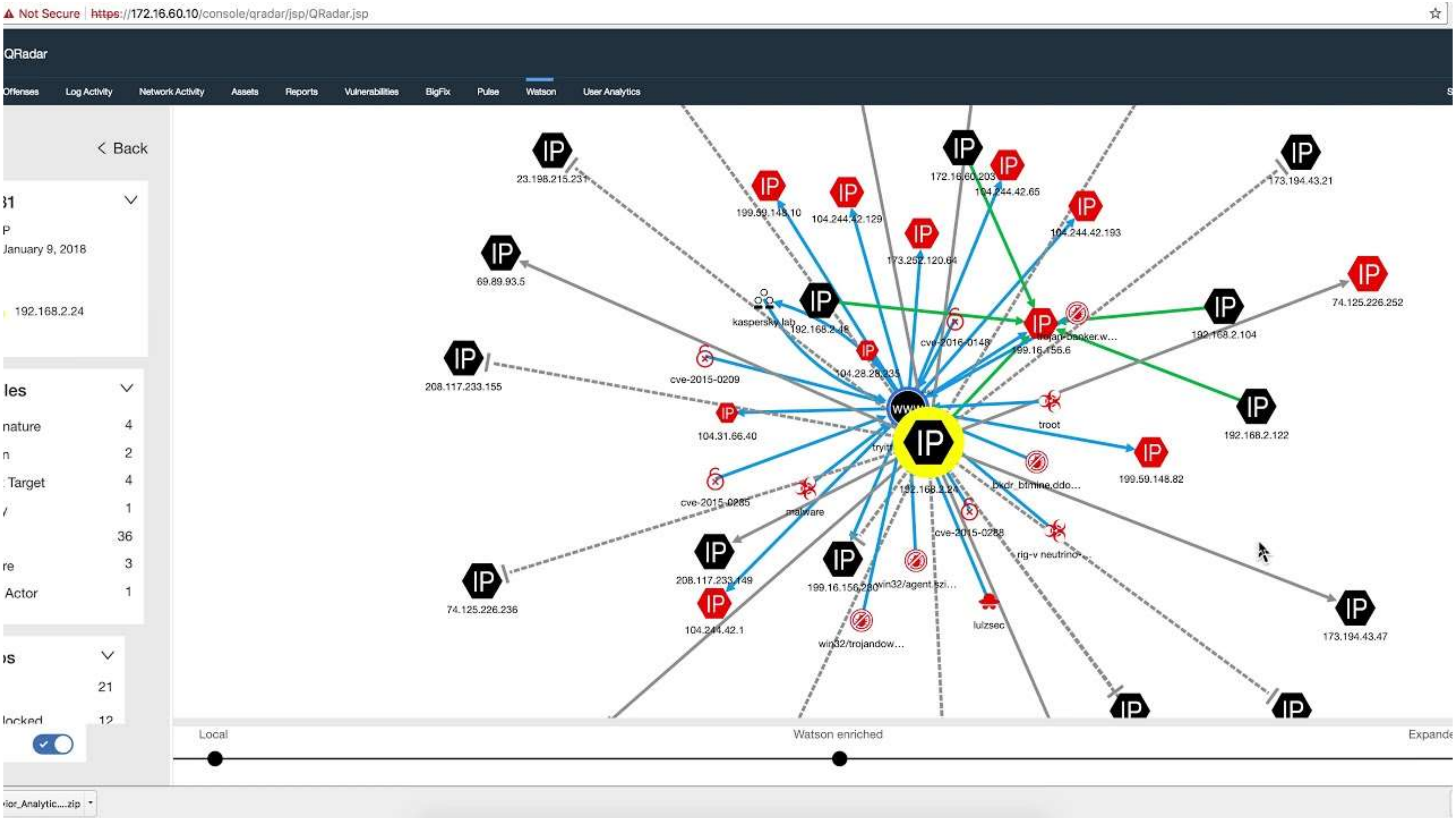
AI Building Blocks



IBM Qradar Advisor with Watson (1/2)

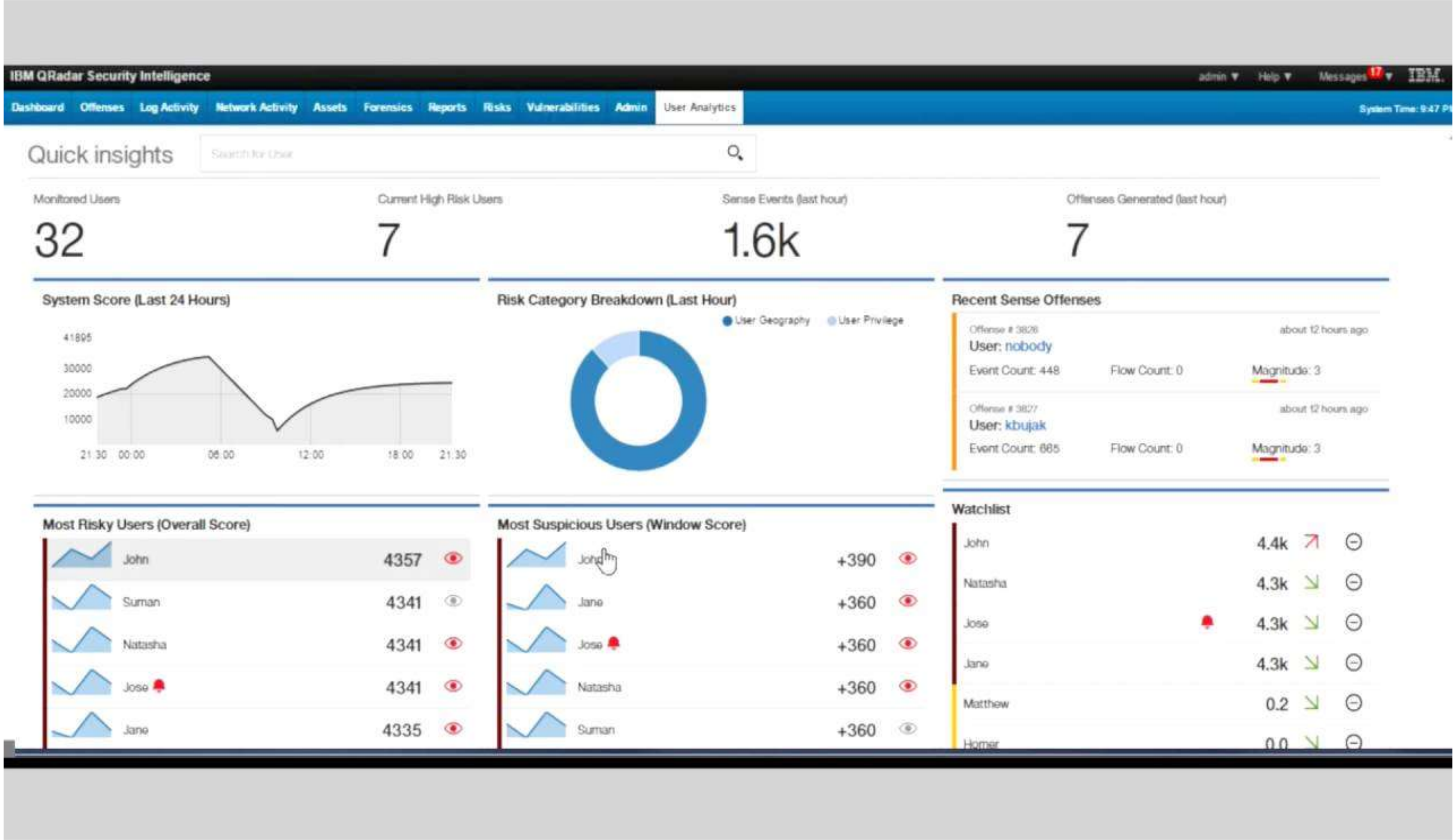


IBM QRadar Advisor with Watson (2/2)

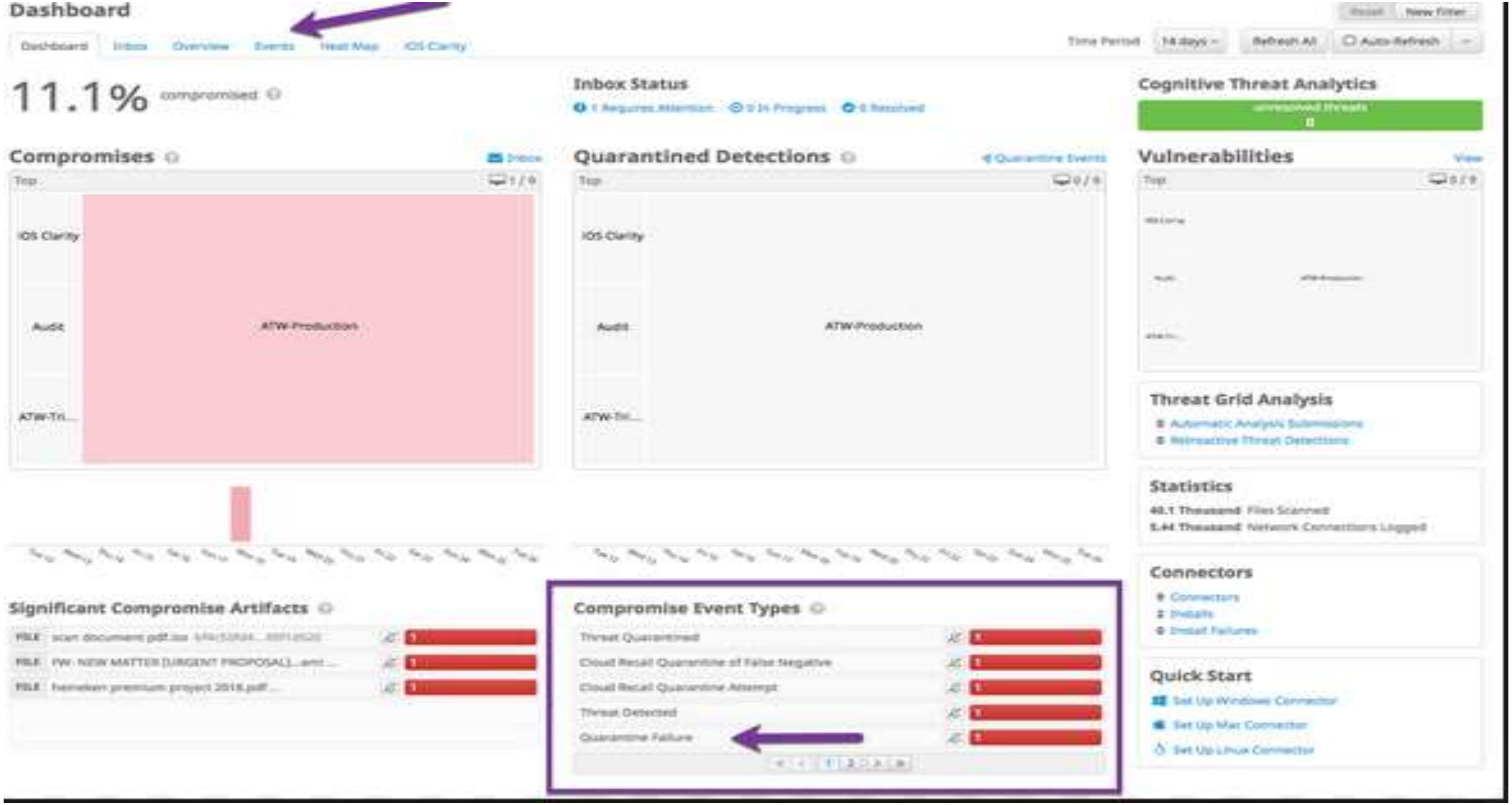


Network Behavior Analysis

User Behavior Analysis



Entity Behavior Analysis



Respond

NB Responding Services

- Incident Management

- Computer Forensics

Thank you for the attention!

n.Kladakis@netbull.gr