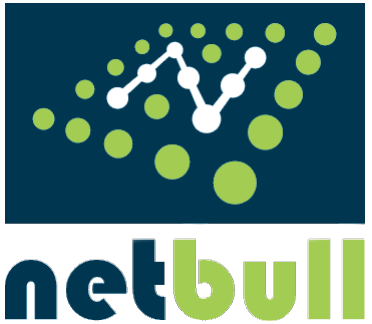
Advance Threat Hunting 24×7: Fighting Cybercrime with Artificial Intelligence



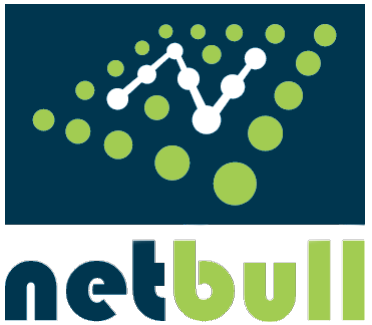
April 2019

Nikitas Kladakis
Information Security Director

Agenda

- Cybersecurity Challenges
- Threat Landscape
- Intelligence Drive Defense

Cybersecurity Challenges



Technology Evolution - IoT

Global Interconnection

Complex Infrastructure

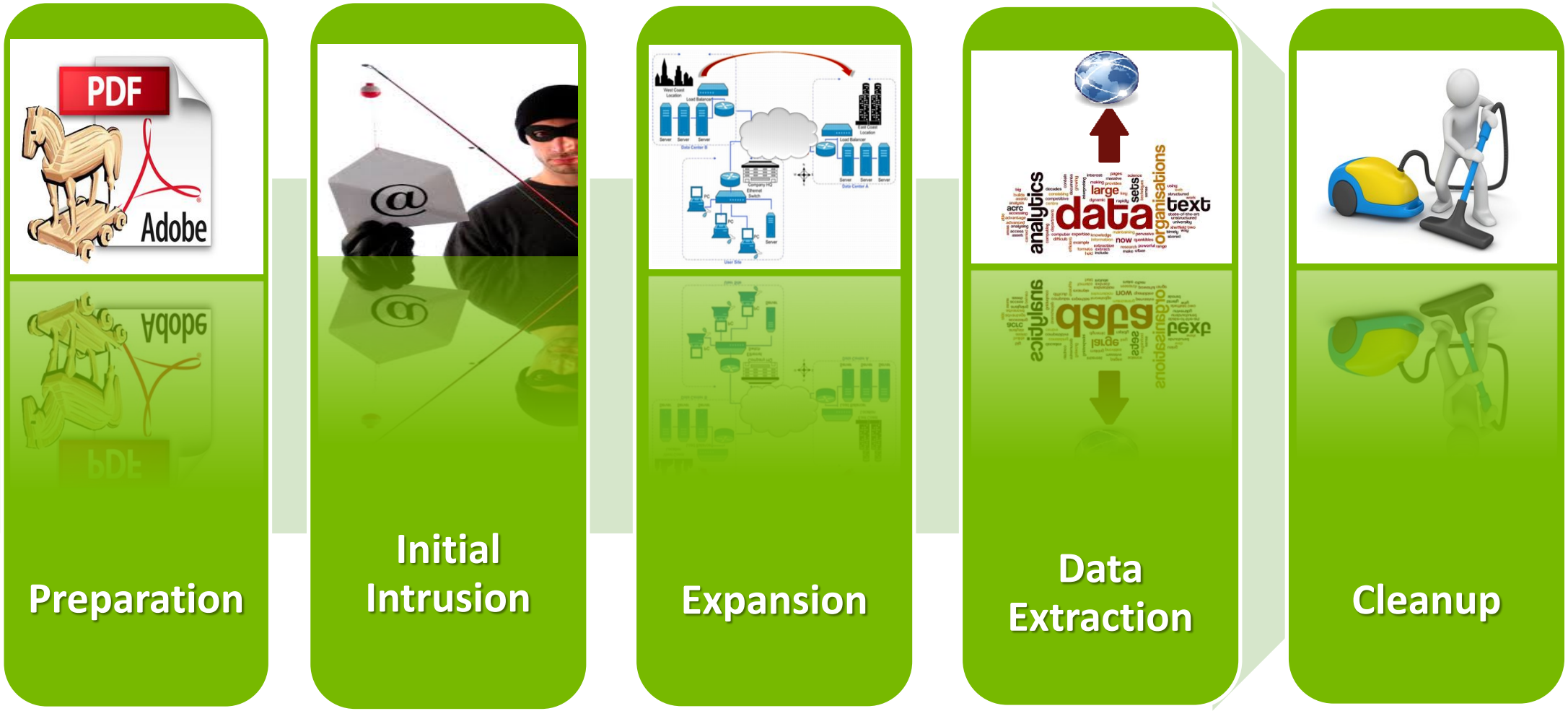
Demanding Business

Compliance & Regulations

Limited Resources

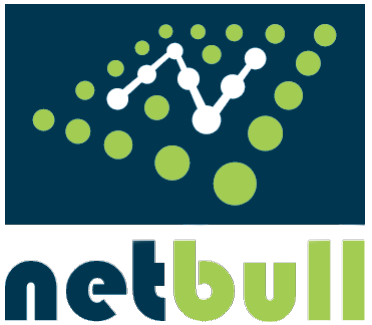
Explosion of Data

Sophisticated Attacks



Advance Malware

Threat Landscape



Common Source of Cyber Threats

- Nation states
- Terrorists
- Industrial spies
- Organized crime groups
- Hacktivists
- Business competitors
- Disgruntled insiders

Source: "Anonymous at Scientology in Los Angeles" by Vincent Diamante. Originally posted to Flickr as Anonymous at Scientology in Los Angeles.

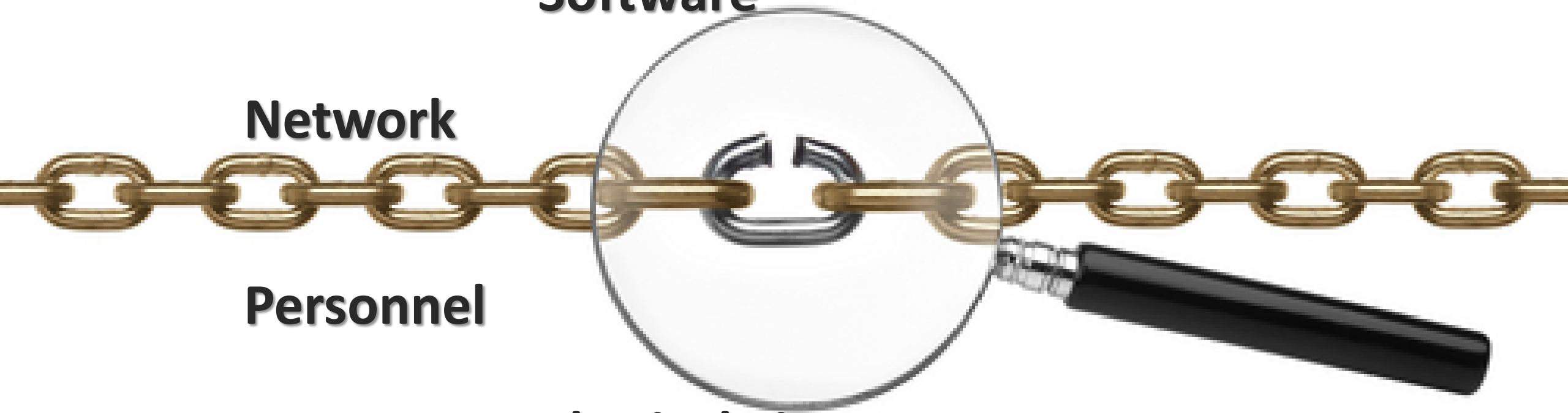
Licensed under CC BY-SA 2.0 via Commons—https://commons.wikimedia.org/wiki/File:Anonymous_at_Scientology_in_Los_Angeles.jpg#/media/File:Anonymous_at_Scientology_in_Los_Angeles.jpg

Vulnerabilities

Hardware

Software

Network

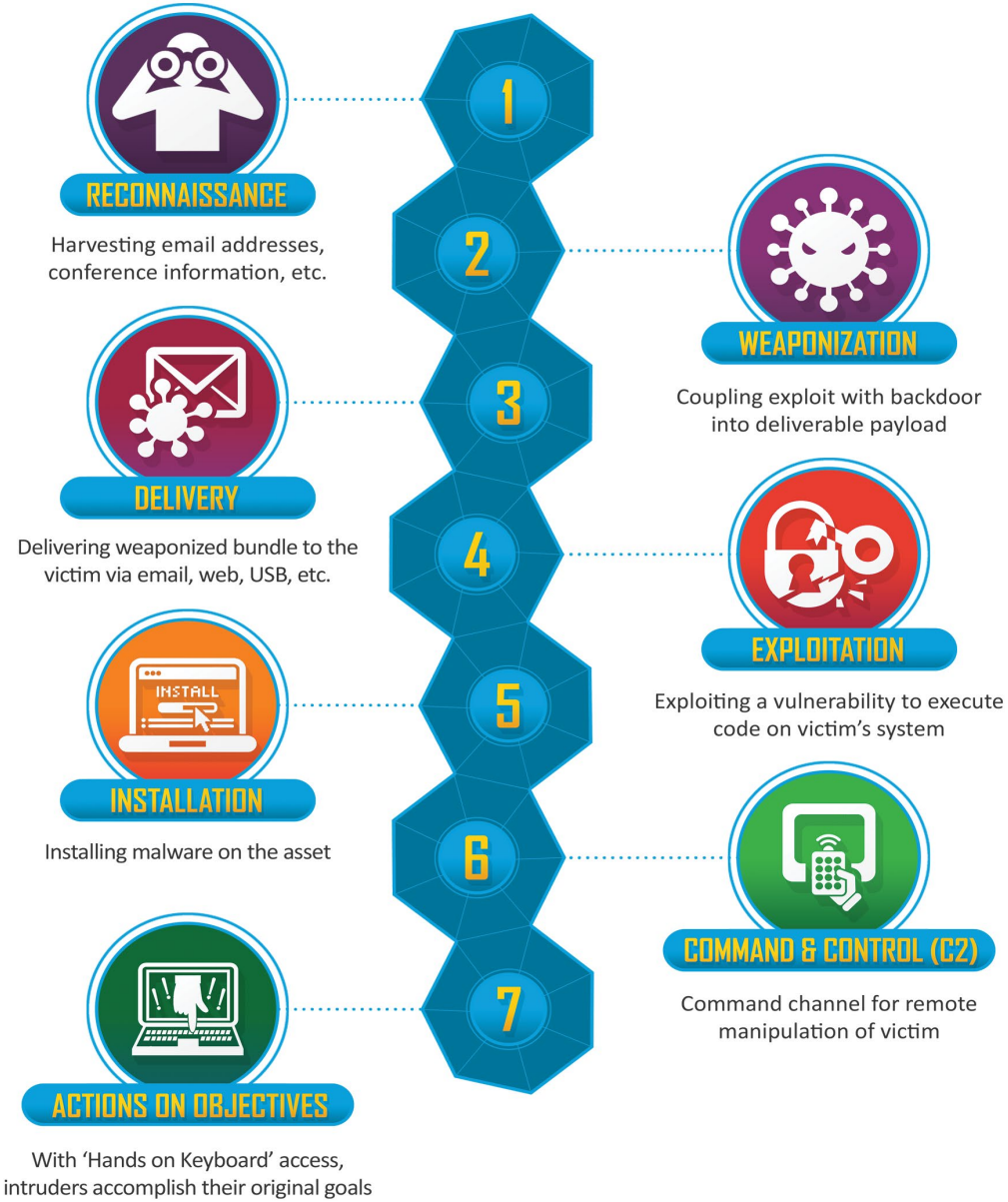


Personnel

Physical Site

Organizational

Cyber Kill Methodology



Developed by Lockheed Martin

Impacts

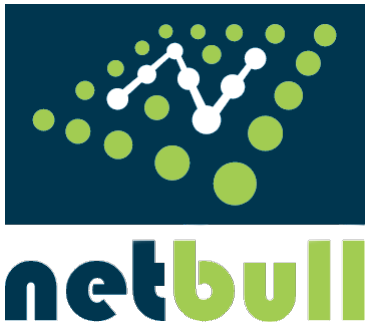
Last week, British Airways announced that the personal and financial information of 380,000 of their passengers had been hacked. Passenger names, home addresses and credit card data were all stolen during the 15-day security breach, catching BA flat-footed.

The Goods BY Vox

A massive breach of Marriott guest data that was thought to have affected around 500 million people may have had a smaller impact than initial reports suggested, but also exposed the passport numbers of several million people, the company **announced on Friday**.

Marriott first disclosed the breach on November 30, saying hackers targeted its Starwood reservation system and accessed the personal information of hundreds of millions of guests who had stayed in the hotel chain's properties since 2014.

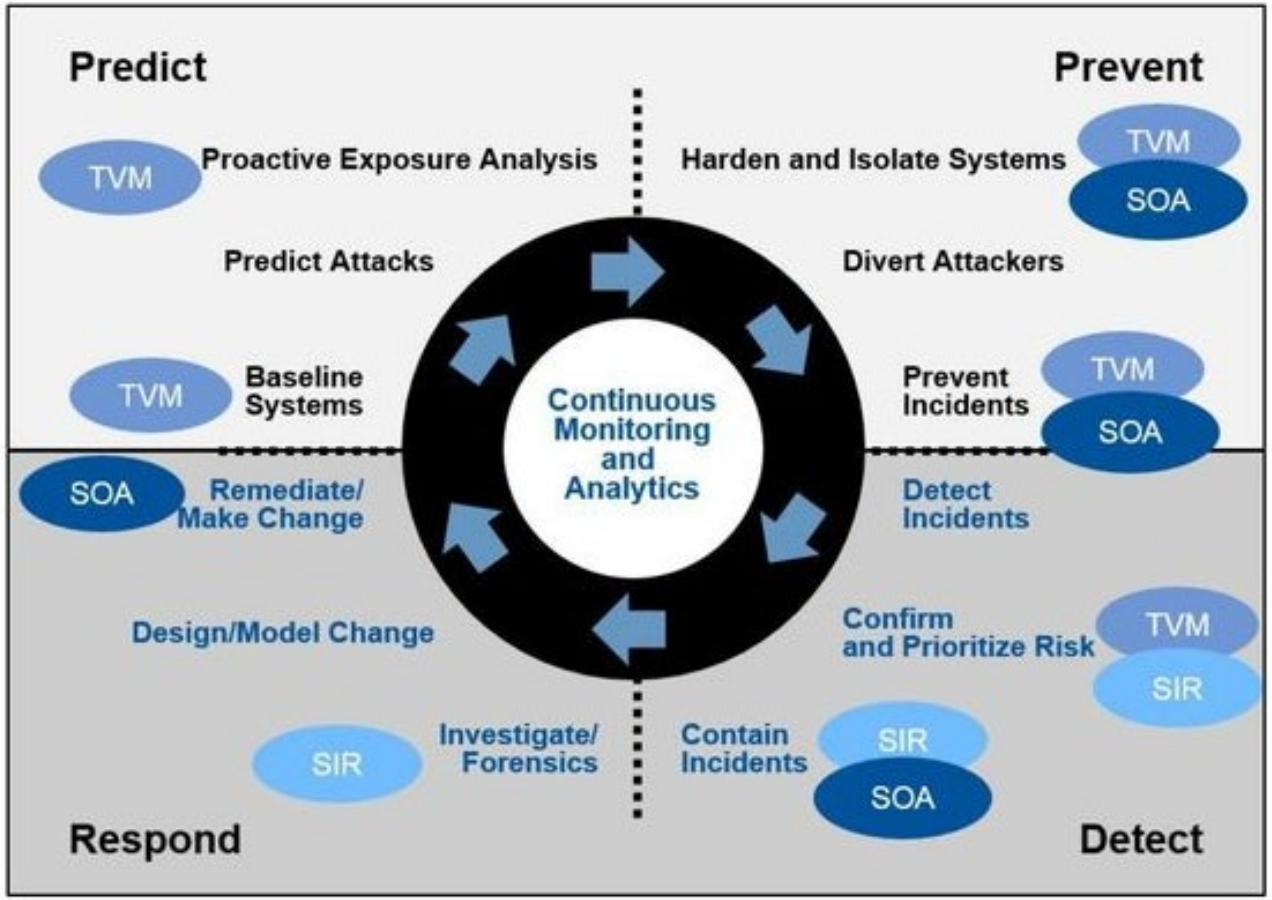
Intelligence Driven Defense



Intelligence Driven Defense

Developed by Lockheed Martin

Centralize Operations: Intelligence Driven SOC



Monitor Threats: Advance Threat Hunting

- Threat hunting involves searching through large volumes of data to identify bad actors and threats to an organization's IT infrastructure

- The goal is to prevent attacks before they happen and eliminate or minimize their effects

Threat Hunting Technologies / Services

Artificial Intelligence

Threat Intelligence

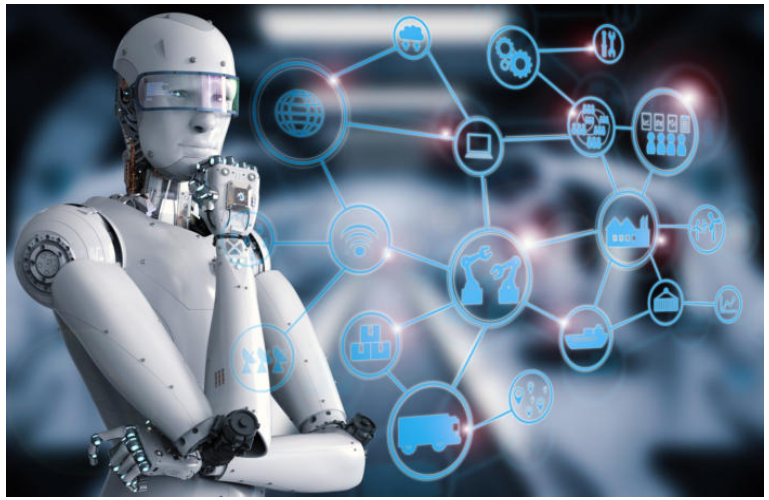
Endpoint Detection and Response

Malware Analysis

Vulnerability Analysis

Social Media feeds

What is AI?



Artificial Intelligence (AI): a software that perform tasks normally requiring human intelligence, such as decision-making

AI Building Blocks

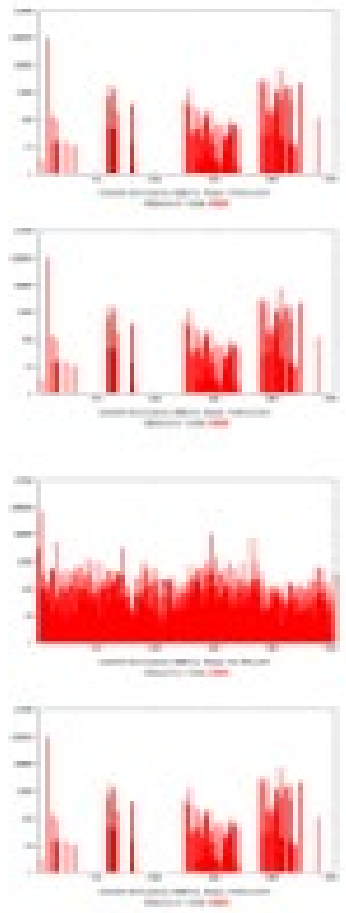
- Big Data
- Machine and Deep Learning Algorithms
  - ✓ Network Behavior Analysis (NBA)
  - ✓ Users and Endpoint Behavior Analysis (UEBA)

Network Behavior Analysis (NBA)

- Network behavior analysis (NBA) analyze traffic and noting unusual actions or departures from normal operation
- After establishing a benchmark for normal traffic, the NBA program passively monitors network activity and flags unknown, new or unusual patterns that might indicate the presence of a threat.
- NBA can also monitor and record trends in bandwidth and protocol use

NBA Operation

- **NBA use:**
  - Data volume (octets, packets)
  - Flows (number, duration, size, service type)
  - Communication matrix (src/dst IP, src/dst ports)
  - Packets (size, flags)



NBA use cases

- DoS/DDoS attacks
- Large Outbound Transfer
- New Services
- Unusual Communication

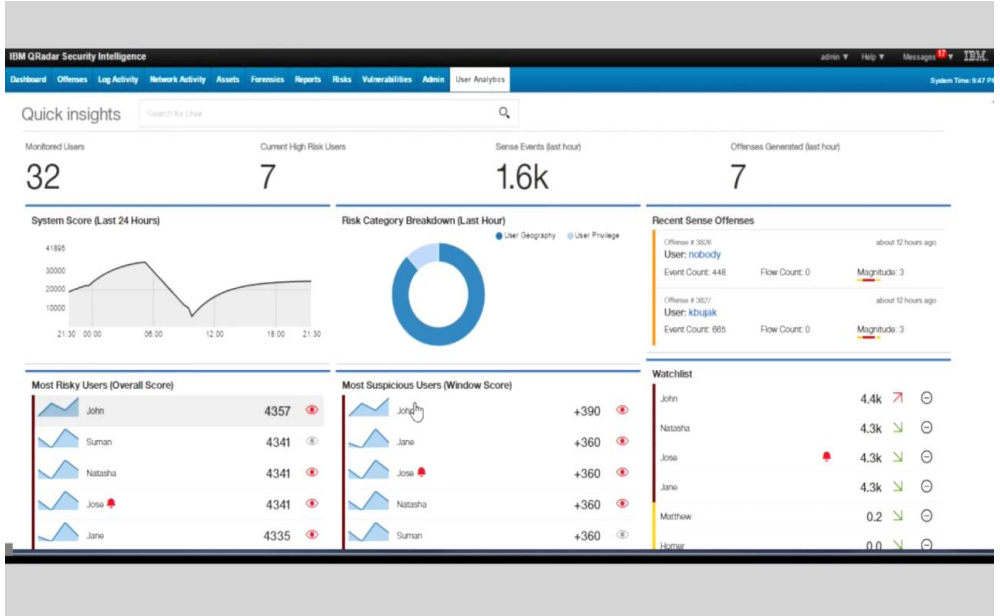
Users and Endpoint Behavior Analysis (UEBA)

- UEBA analyzes user and device activity to detect malicious insiders and determine if a user's credentials or a device have been compromised

- UEBA adds user and device context to network, log, vulnerability and threat data to more quickly and accurately detect attacks

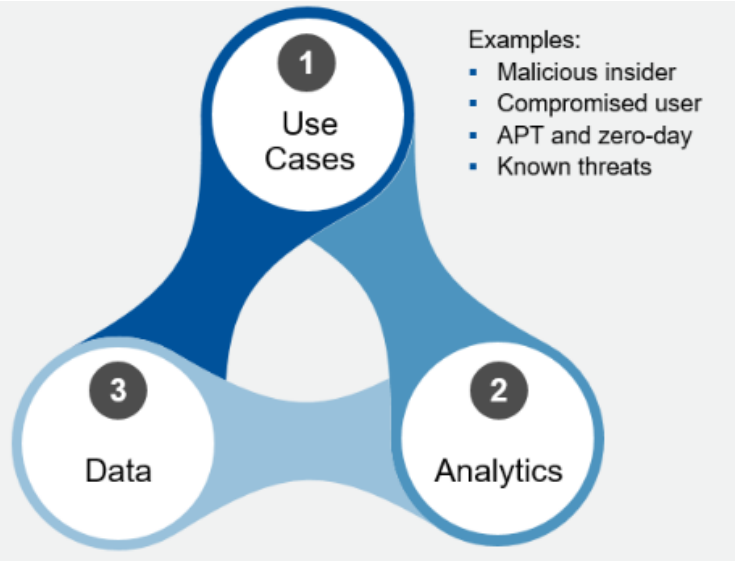
UEBA Operation

- **UEBA use:**
  - Traffic around access, authentication, and account changes
  - User behavior on the network
  - Endpoint and application agent & logs, such as from Windows or Linux, and SAAS applications
  - Endpoint Behavior



UEBA use cases

- Large Outbound Transfer by High Risk User
- User Account Created and Deleted in a Short Period
- High Risk User Access to Critical Asset
- Replication Request from a Non-Domain Controller
- User Access from Multiple Hosts
- 0-day Malware Detection
- non Malware Detection



Knowledge Management

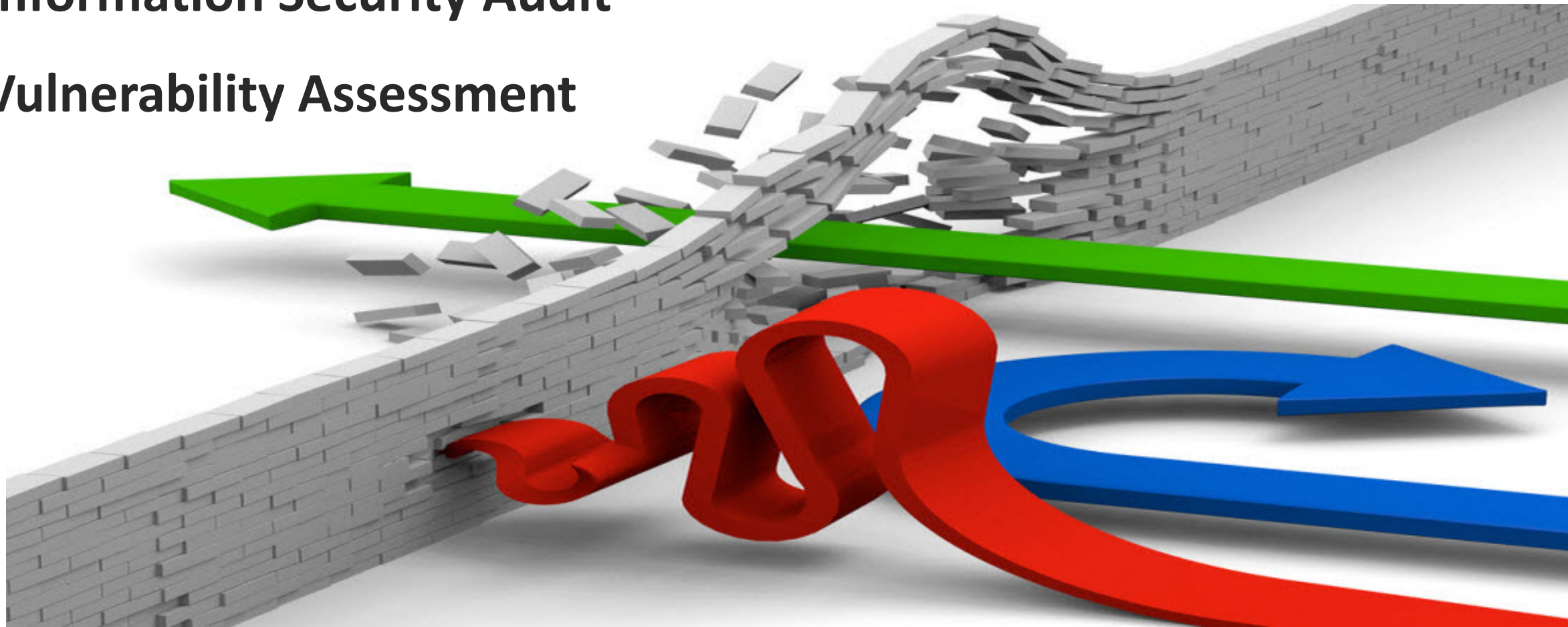
- Threat Intelligence Management
- Cyber Analyst Training
- Cyber Threat Analysis Services

Proactively Defend: Analysis and Mitigation (powered by nSA)

nSA: netbull 3D* Security Architecture

Measurement and Accountability

- Penetration Test
- Information Security Audit
- Vulnerability Assessment



Thank you for the attention!

n.Kladakis@netbull.gr