netbull

The Art of Artificial Intelligence for Data Breach Management

May 2019

Nikitas Kladakis
Information Security Director

Agenda

- Cyber Security Challenges
- The Art of Artificial Intelligence for Data Breach Management

Cybersecurity Challenges

netbull

Technology Evolution - IoT

Global Interconnection

Complex Infrastructure

Demanding Business

Compliance & Regulations

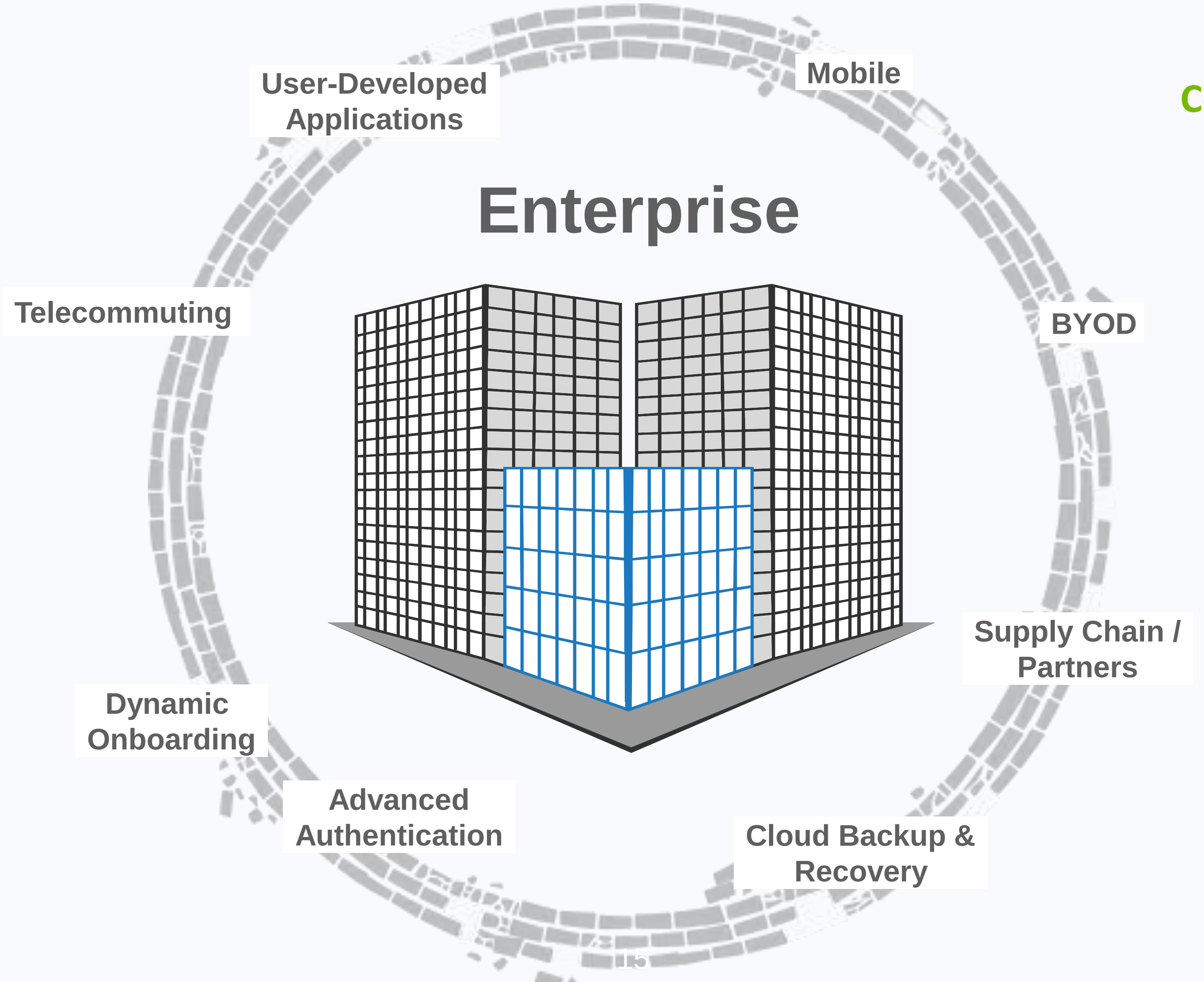
Limited Resources

The Perimeter Has Vanished

Shift to Cloud

Marketo
salesforce.com
NETSUITE
ONE SYSTEM, NO LIMITS.
workday.
servicenow

Consumerization of IT / BYOD



Enterprise

User-Developed Applications

Mobile

Telecommuting

BYOD

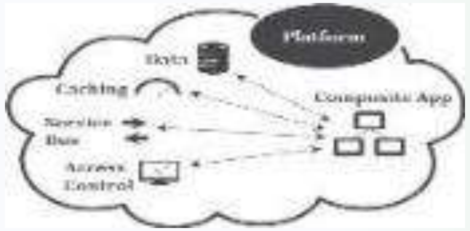
Dynamic Onboarding

Supply Chain / Partners

Advanced Authentication

Cloud Backup & Recovery

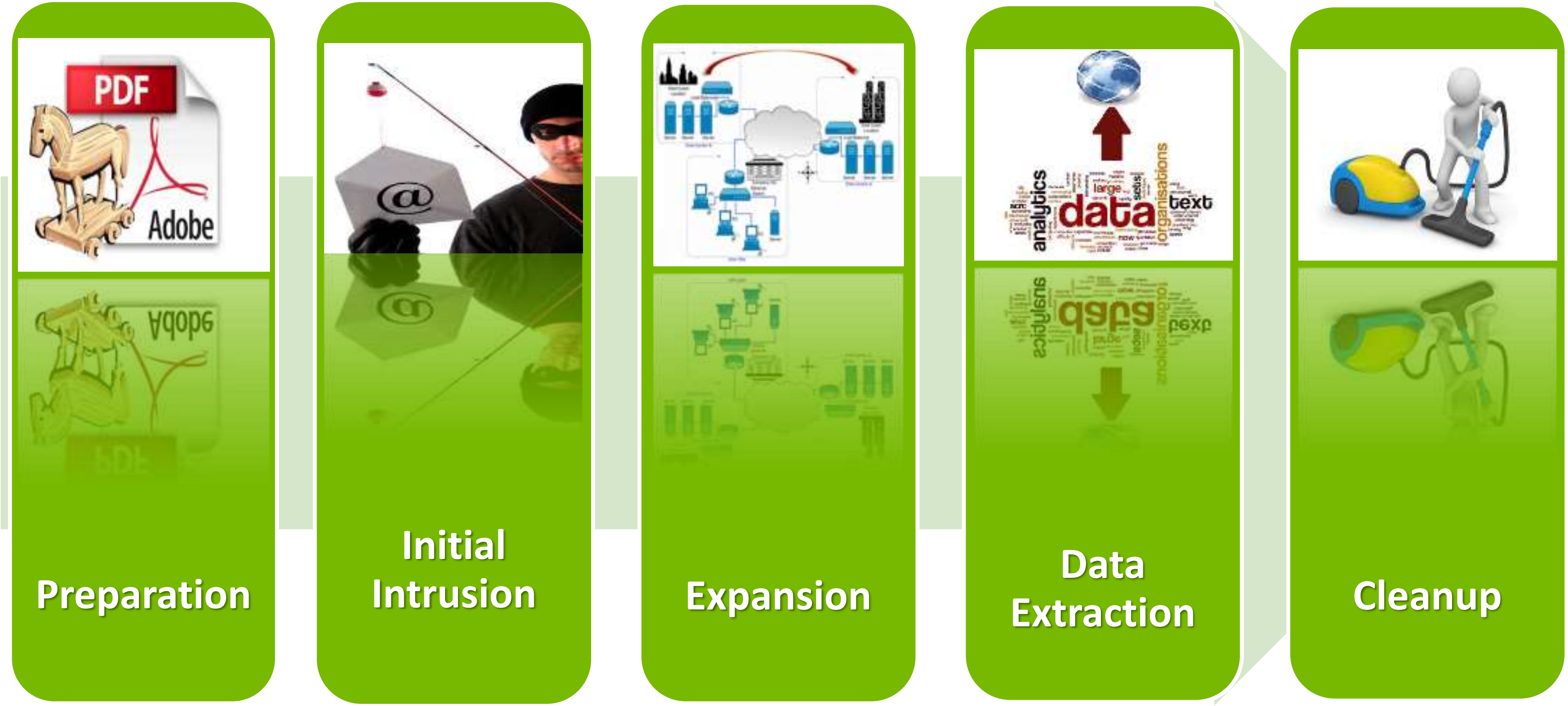
Composite Applications and Application Proliferation



Global, Distributed Workforce

Explosion of Data

Sophisticated Attacks



Preparation

Initial Intrusion

Expansion

Data Extraction

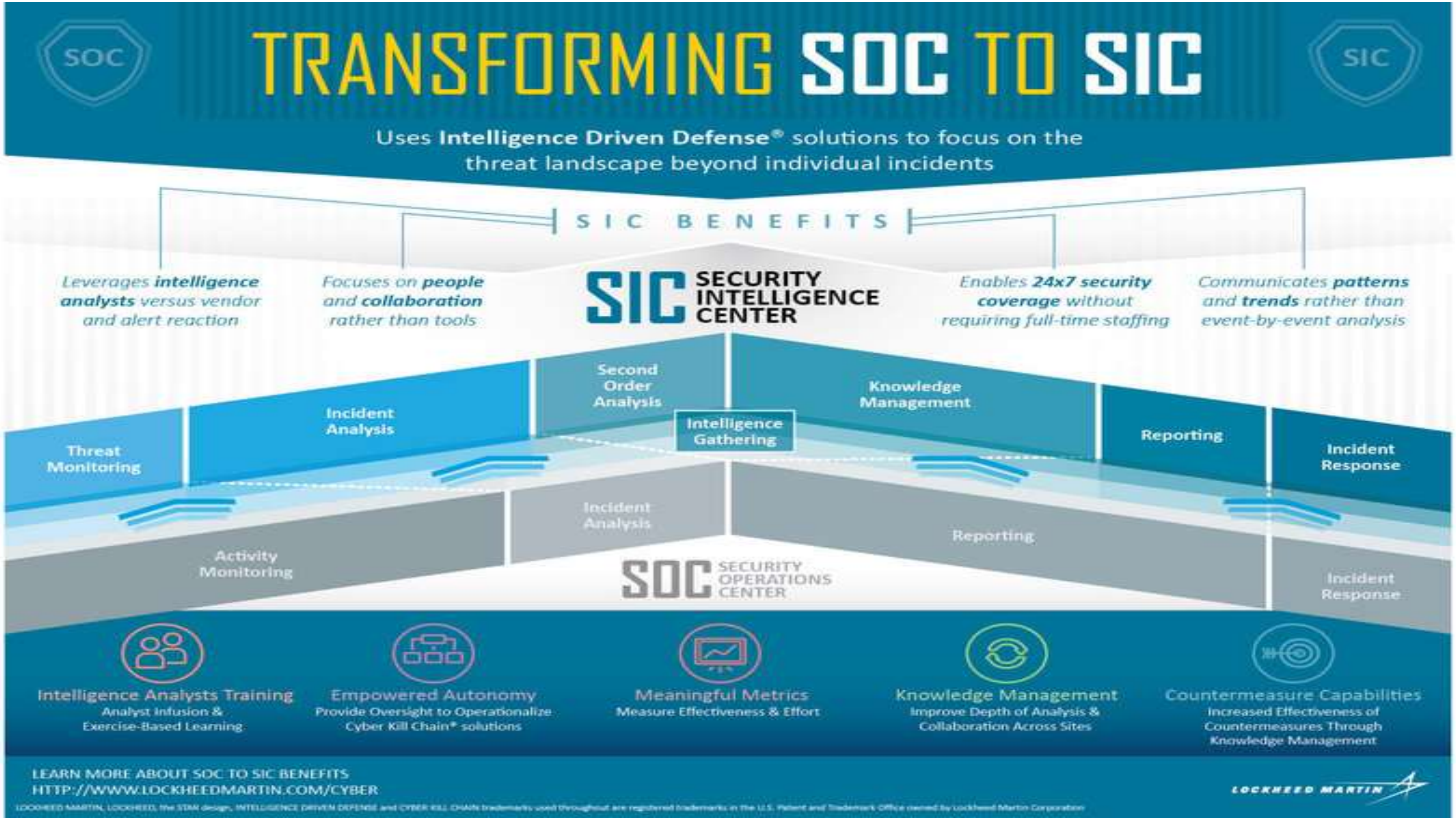
Cleanup

Advance Malware

The Art of Artificial Intelligence for Data Breach Management

netbull

Intelligence Driven SOC



TRANSFORMING SOC TO SIC

Uses **Intelligence Driven Defense®** solutions to focus on the threat landscape beyond individual incidents

SIC BENEFITS

*Leverages **intelligence analysts** versus vendor and alert reaction*

*Focuses on **people** and **collaboration** rather than tools*

*Enables **24x7 security coverage** without requiring full-time staffing*

*Communicates **patterns** and **trends** rather than event-by-event analysis*

Intelligence Analysts Training
Analyst Infusion & Exercise-Based Learning

Empowered Autonomy
Provide Oversight to Operationalize Cyber Kill Chain® solutions

Meaningful Metrics
Measure Effectiveness & Effort

Knowledge Management
Improve Depth of Analysis & Collaboration Across Sites

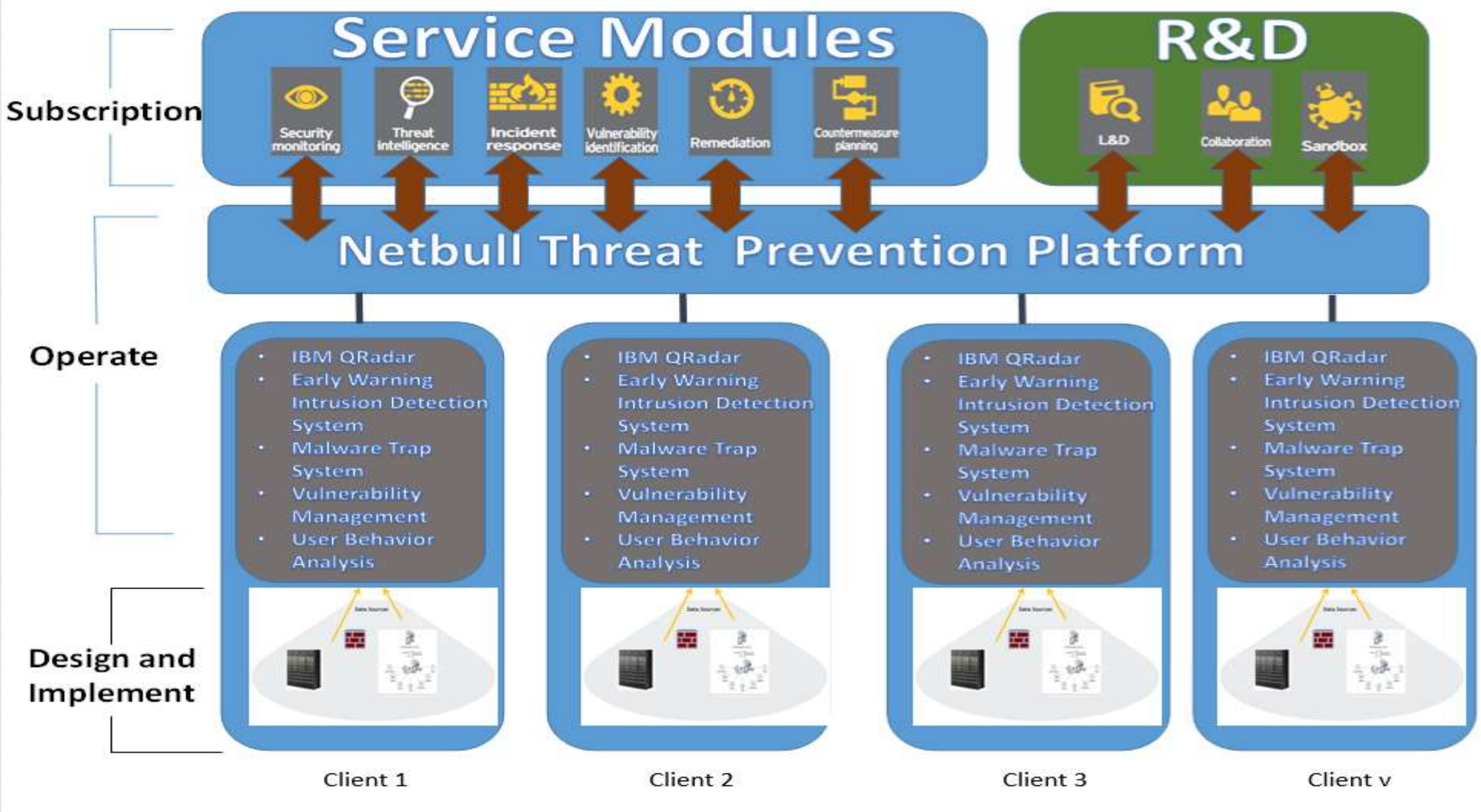
Countermeasure Capabilities
Increased Effectiveness of Countermeasures Through Knowledge Management

LEARN MORE ABOUT SOC TO SIC BENEFITS
HTTP://WWW.LOCKHEEDMARTIN.COM/CYBER

LOCKHEED MARTIN, LOCKHEED, the STAR design, INTELLIGENCE DRIVEN DEFENSE and CYBER KILL CHAIN trademarks used throughout are registered trademarks in the U.S. Patent and Trademark Office owned by Lockheed Martin Corporation

Netbull Threat Management Platform

(based on IBM Qradar)



Subscription

Service Modules

Security monitoring

Threat intelligence

Incident response

Vulnerability identification

Remediation

Countermeasure planning

R&D

L&D

Collaboration

Sandbox

Netbull Threat Prevention Platform

Operate

Design and Implement

Client 1

- IBM QRadar
- Early Warning Intrusion Detection System
- Malware Trap System
- Vulnerability Management
- User Behavior Analysis

Client 2

- IBM QRadar
- Early Warning Intrusion Detection System
- Malware Trap System
- Vulnerability Management
- User Behavior Analysis

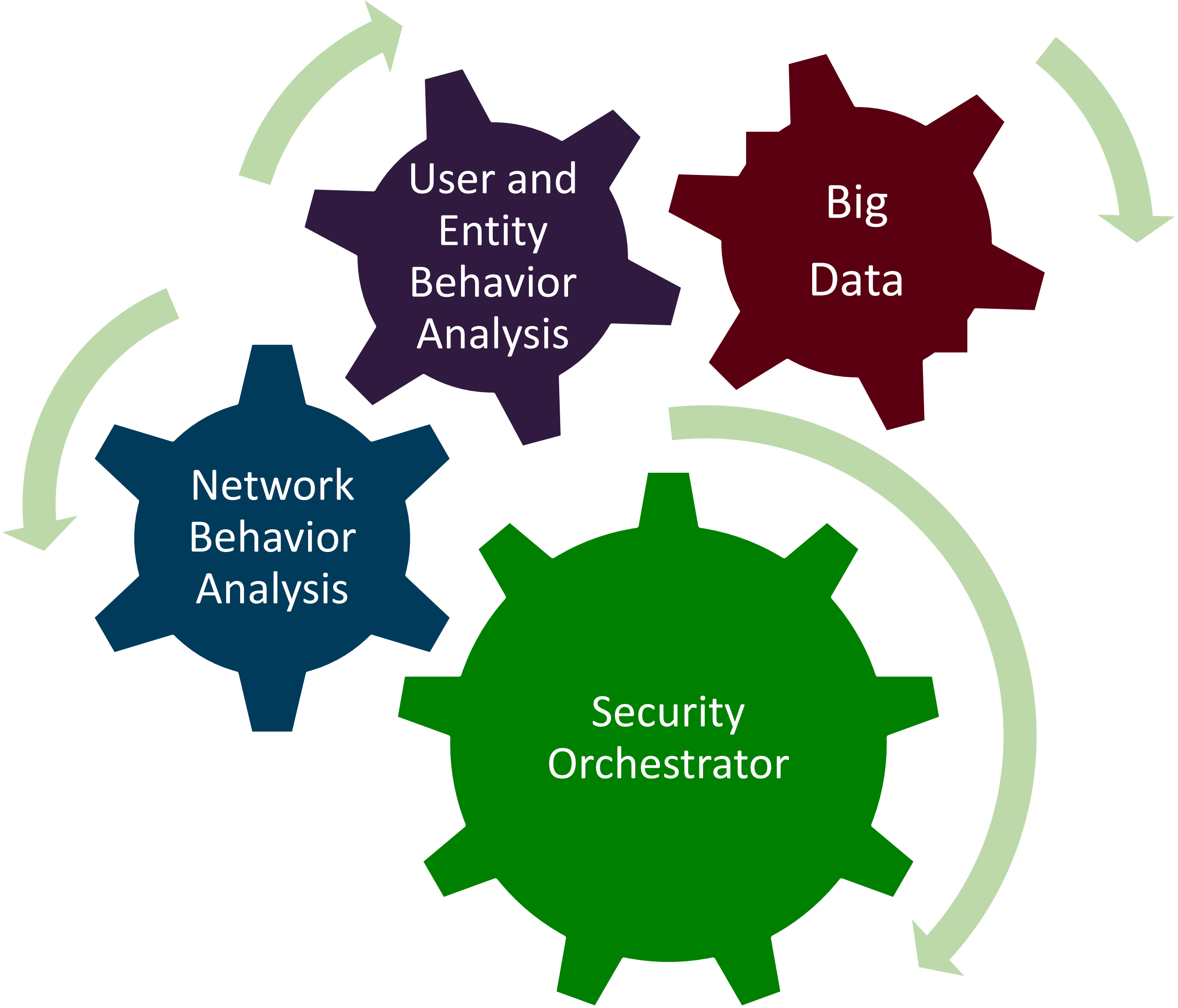
Client 3

- IBM QRadar
- Early Warning Intrusion Detection System
- Malware Trap System
- Vulnerability Management
- User Behavior Analysis

Client v

- IBM QRadar
- Early Warning Intrusion Detection System
- Malware Trap System
- Vulnerability Management
- User Behavior Analysis

Artificial Intelligence



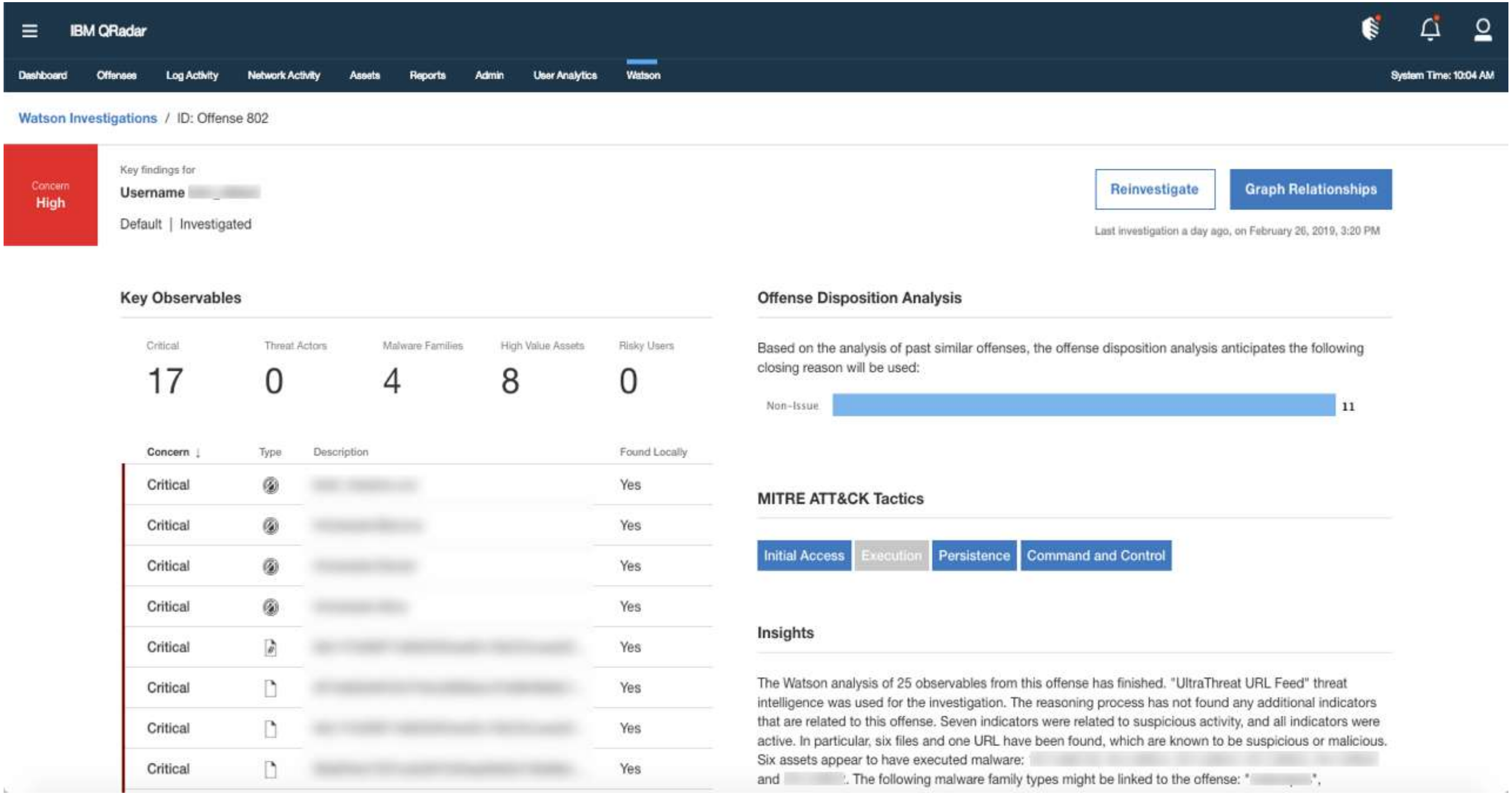
User and Entity Behavior Analysis

Big Data

Network Behavior Analysis

Security Orchestrator

Security Orchestrator (1/2)



Watson Investigations / ID: Offense 802

Concern
High

Key findings for
Username [redacted]
Default | Investigated

Last investigation a day ago, on February 26, 2019, 3:20 PM

Key Observables

Critical	Threat Actors	Malware Families	High Value Assets	Risky Users
17	0	4	8	0

Concern ↓	Type	Description	Found Locally
Critical	🌐	[redacted]	Yes
Critical	🌐	[redacted]	Yes
Critical	🌐	[redacted]	Yes
Critical	🌐	[redacted]	Yes
Critical	📄	[redacted]	Yes
Critical	📄	[redacted]	Yes
Critical	📄	[redacted]	Yes
Critical	📄	[redacted]	Yes

Offense Disposition Analysis

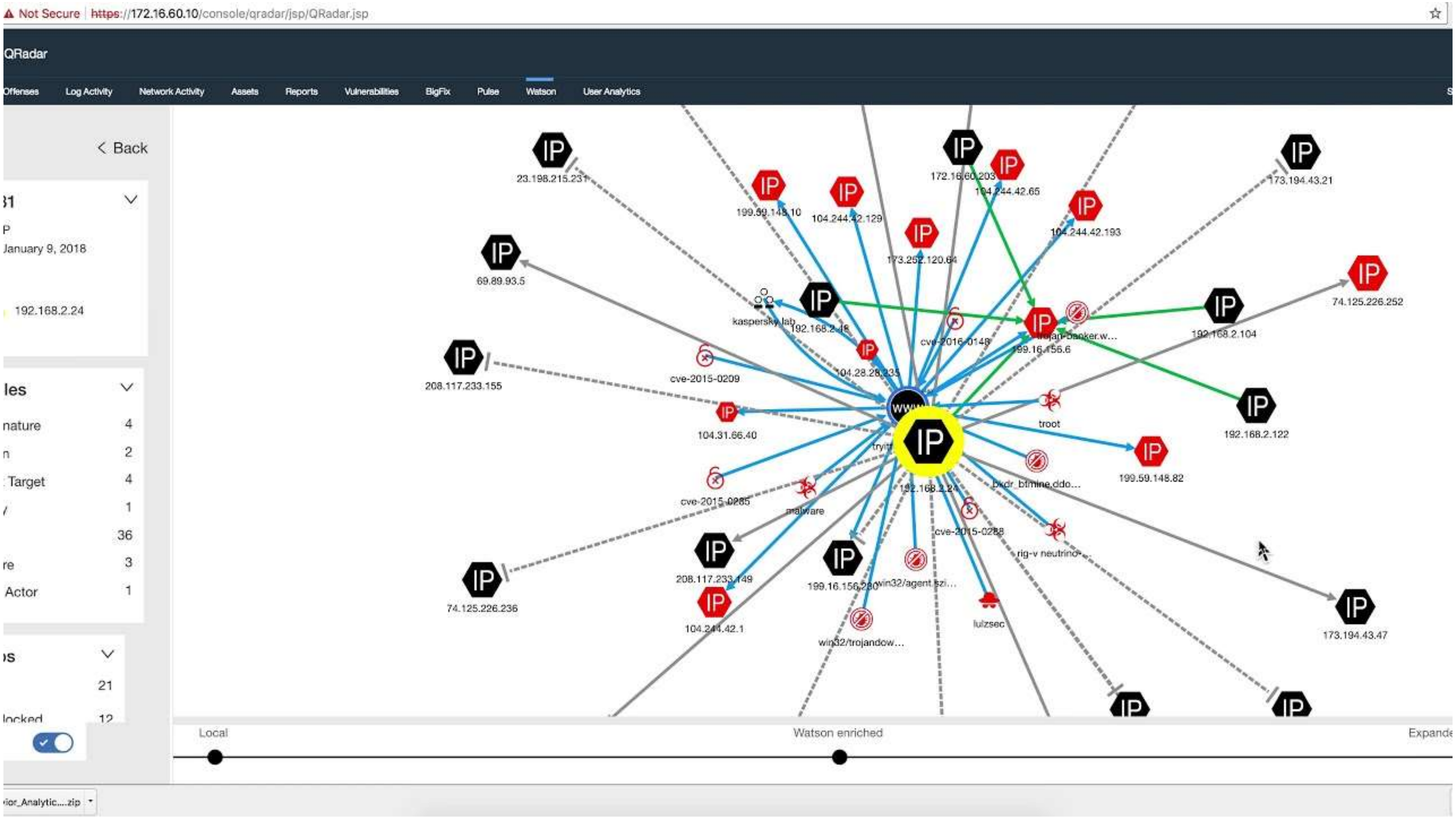
Based on the analysis of past similar offenses, the offense disposition analysis anticipates the following closing reason will be used:

MITRE ATT&CK Tactics

Insights

The Watson analysis of 25 observables from this offense has finished. "UltraThreat URL Feed" threat intelligence was used for the investigation. The reasoning process has not found any additional indicators that are related to this offense. Seven indicators were related to suspicious activity, and all indicators were active. In particular, six files and one URL have been found, which are known to be suspicious or malicious. Six assets appear to have executed malware: [redacted] and [redacted]. The following malware family types might be linked to the offense: "[redacted]",

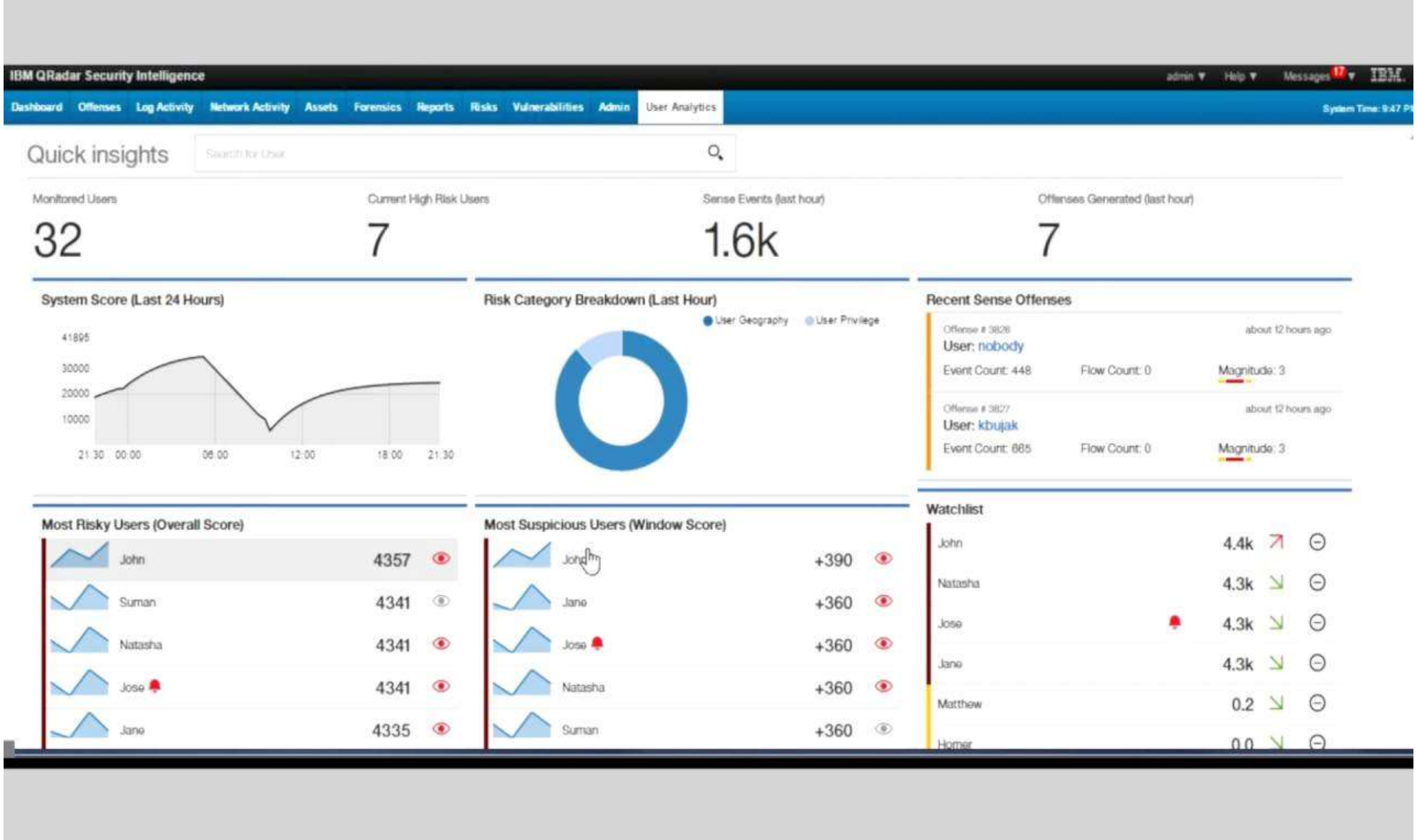
Security Orchestrator (2/2)



Network Behavior Analysis

Fri Aug 11 2017 / 10:18:15
Breach Log
Math / Unusual Data Transfer
Math / Device / Unusual Activity
Math / Unusual Connectivity
Math / Network Profile / Rare Connection from
Math / Device / SMB Directory
DARKTRACE

User Behavior Analysis



Quick insights

Monitored Users	Current High Risk Users	Sense Events (last hour)	Offenses Generated (last hour)
32	7	1.6k	7

System Score (Last 24 Hours)

Risk Category Breakdown (Last Hour)

Recent Sense Offenses

Offense # 3828 about 12 hours ago
User: nobody
Event Count: 448 Flow Count: 0 Magnitude: 3

Offense # 3827 about 12 hours ago
User: kbujak
Event Count: 665 Flow Count: 0 Magnitude: 3

Most Risky Users (Overall Score)

John	4357
Suman	4341
Natasha	4341
Jose	4341
Jane	4335

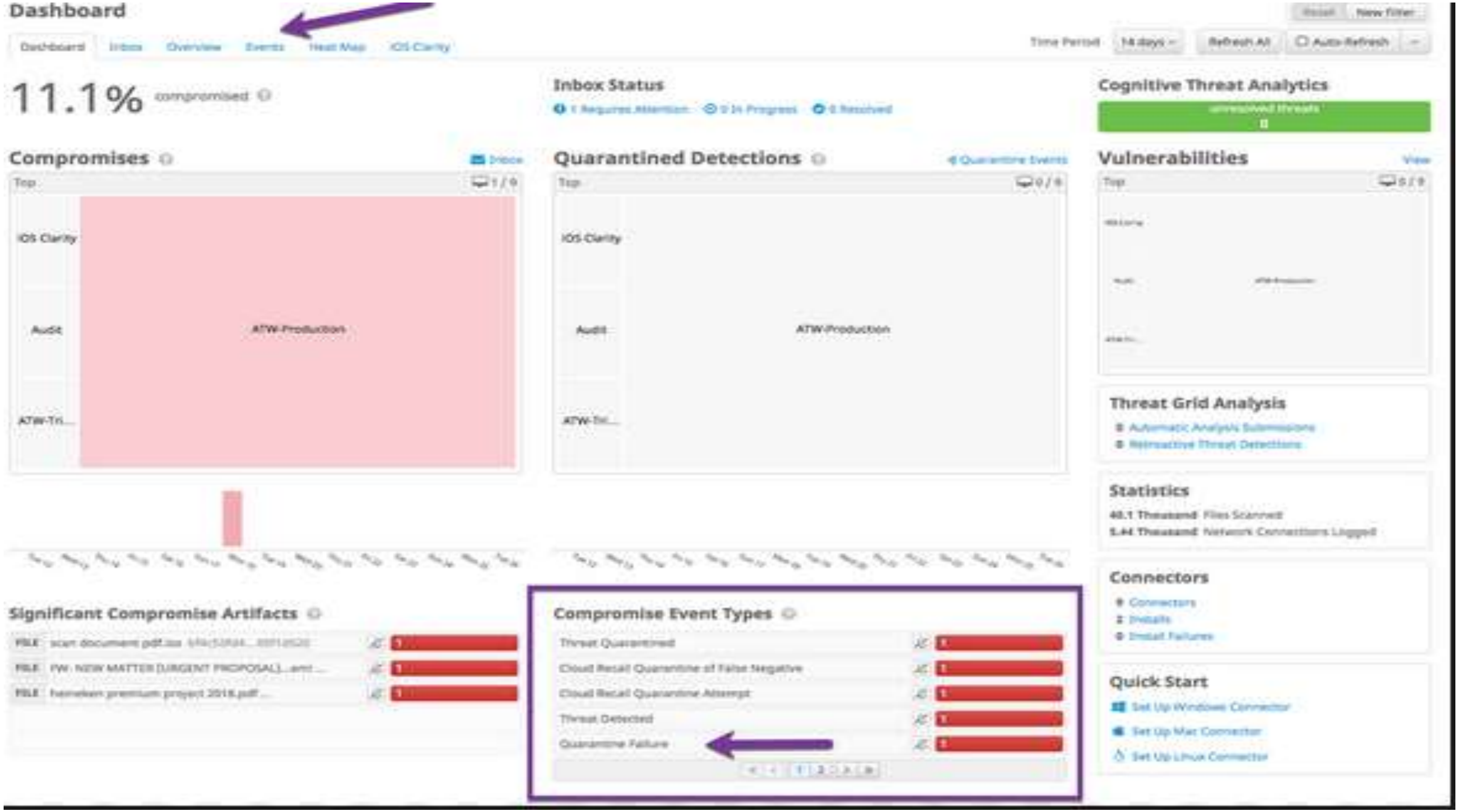
Most Suspicious Users (Window Score)

John	+390
Jane	+360
Jose	+360
Natasha	+360
Suman	+360

Watchlist

John	4.4k ↗
Natasha	4.3k ↘
Jose	4.3k ↘
Jane	4.3k ↘
Matthew	0.2 ↘
Homer	0.0 ↘

Entity Behavior Analysis



11.1% compromised

Inbox Status

1 Requires Attention · 0 In Progress · 0 Resolved

Cognitive Threat Analytics

unresolved threats 0

Compromises

Quarantined Detections

Vulnerabilities

Threat Grid Analysis

- Automatic Analysis Submissions
- Retroactive Threat Detections

Statistics

40.1 Thousand Files Scanned

1.44 Thousand Network Connections Logged

Connectors

- Connectors
- Installs
- Install Failures

Quick Start

- Set Up Windows Connector
- Set Up Mac Connector
- Set Up Linux Connector

Significant Compromise Artifacts

FILE	scan document pdf.iso [illegible]	1
FILE	FW: NEW MATTER [URGENT PROPOSAL]...eml ...	1
FILE	heineken premium project 2018.pdf ...	1

Compromise Event Types

Threat Quarantined	1
Cloud Recall Quarantine of False Negative	1
Cloud Recall Quarantine Attempt	1
Threat Detected	1
Quarantine Failure	1

Thank you for the attention!

n.Kladakis@netbull.gr