
11 Giugno 2019
Gli scenari di attacco e le strategie di difesa nella Cybersecurity
Museo dell'Ara Pacis, Roma
CYBERTECH
ENGINEERING GROUP
IBM
Gold
Business Partner

SCENARI DI ATTACCO E STRATEGIE DI DIFESA

RICCARDO MORSICANI

Principal Security Architech

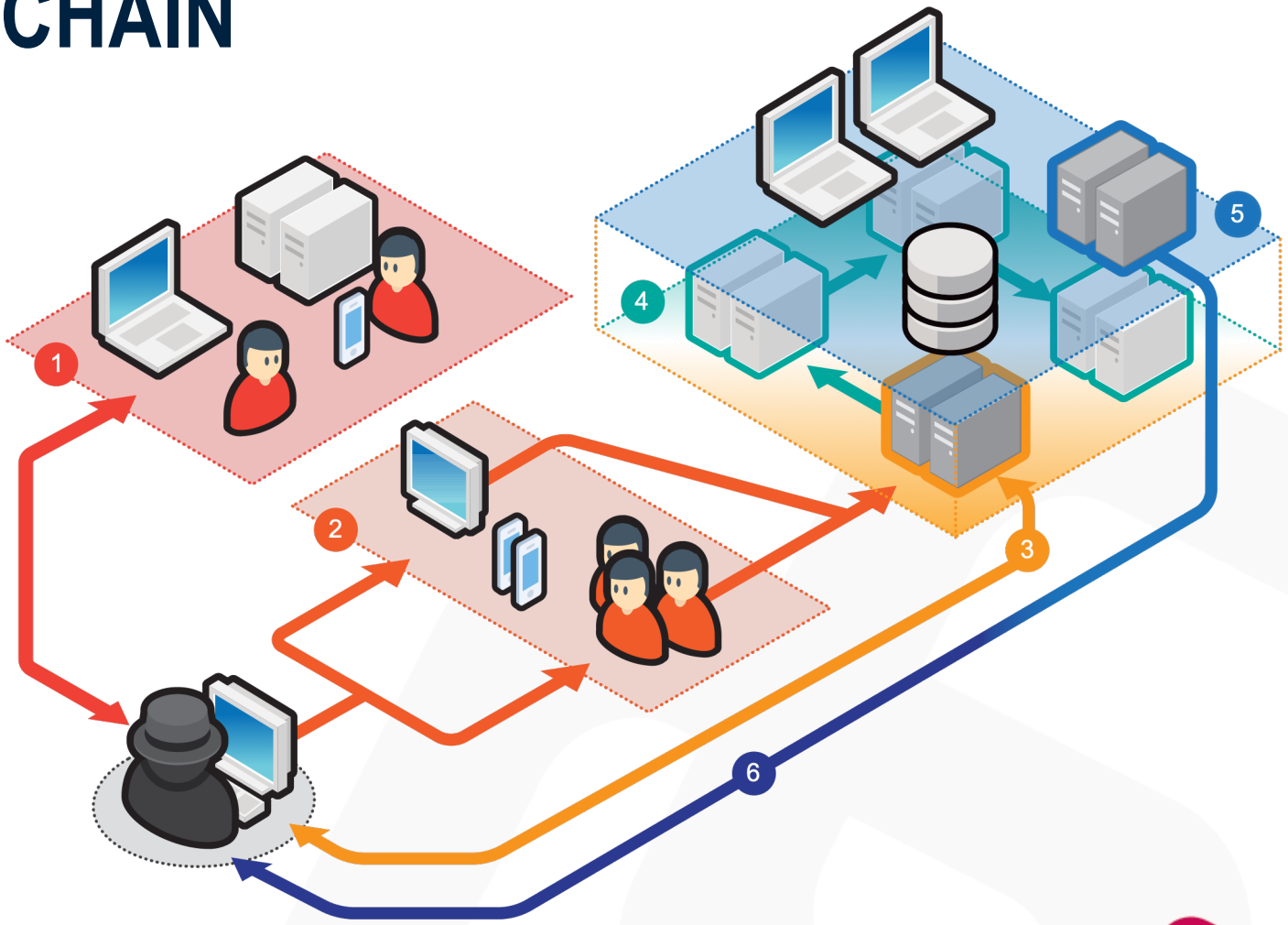

HACKERS HAVE A
HUGE ADVANTAGE
OVER "DEFENDERS".
THEY NEED TO EXPLOIT ONE VULNERABILITY AND DONE
CYBERTECH


CYBERTECH


CLOUD
API & MOBILITY
SOCIAL MEDIA
BIG DATA
INTERNET OF THINGS
INCREASED THREAT SURFACE
TARGETED ATTACKS
INSIDER THREAT
ENABLE THE BUSINESS
PROTECT THE BUSINESS

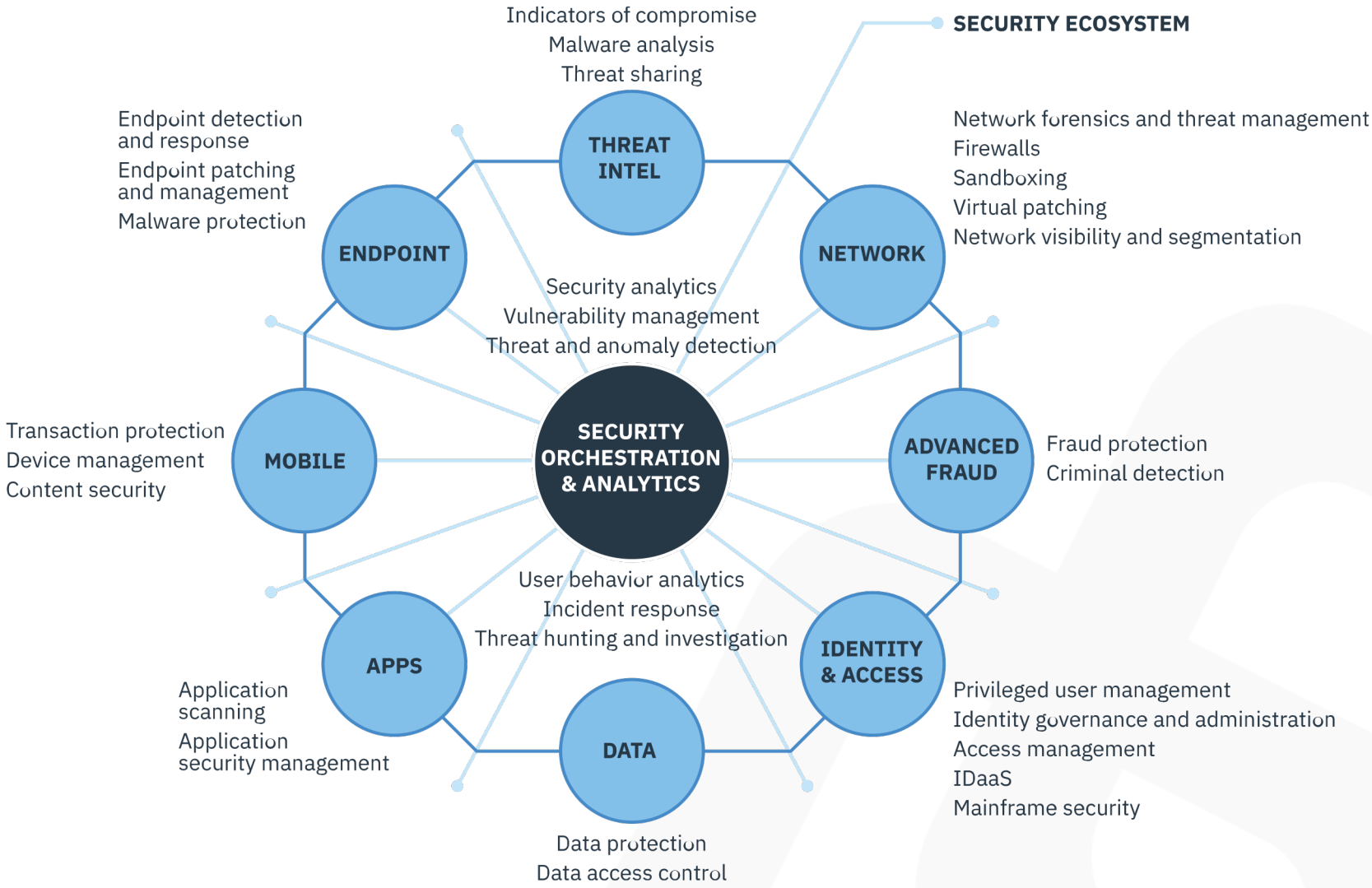
ATTACK KILL CHAIN

1. INTELLIGENCE GATHERING
2. POINT OF ENTRY
3. C&C COMMUNICATION
4. LATERAL MOVEMENT
5. ASSET DISCOVERY
6. DATA EXFILTRATION



CYBER SECURITY FRAMEWORK

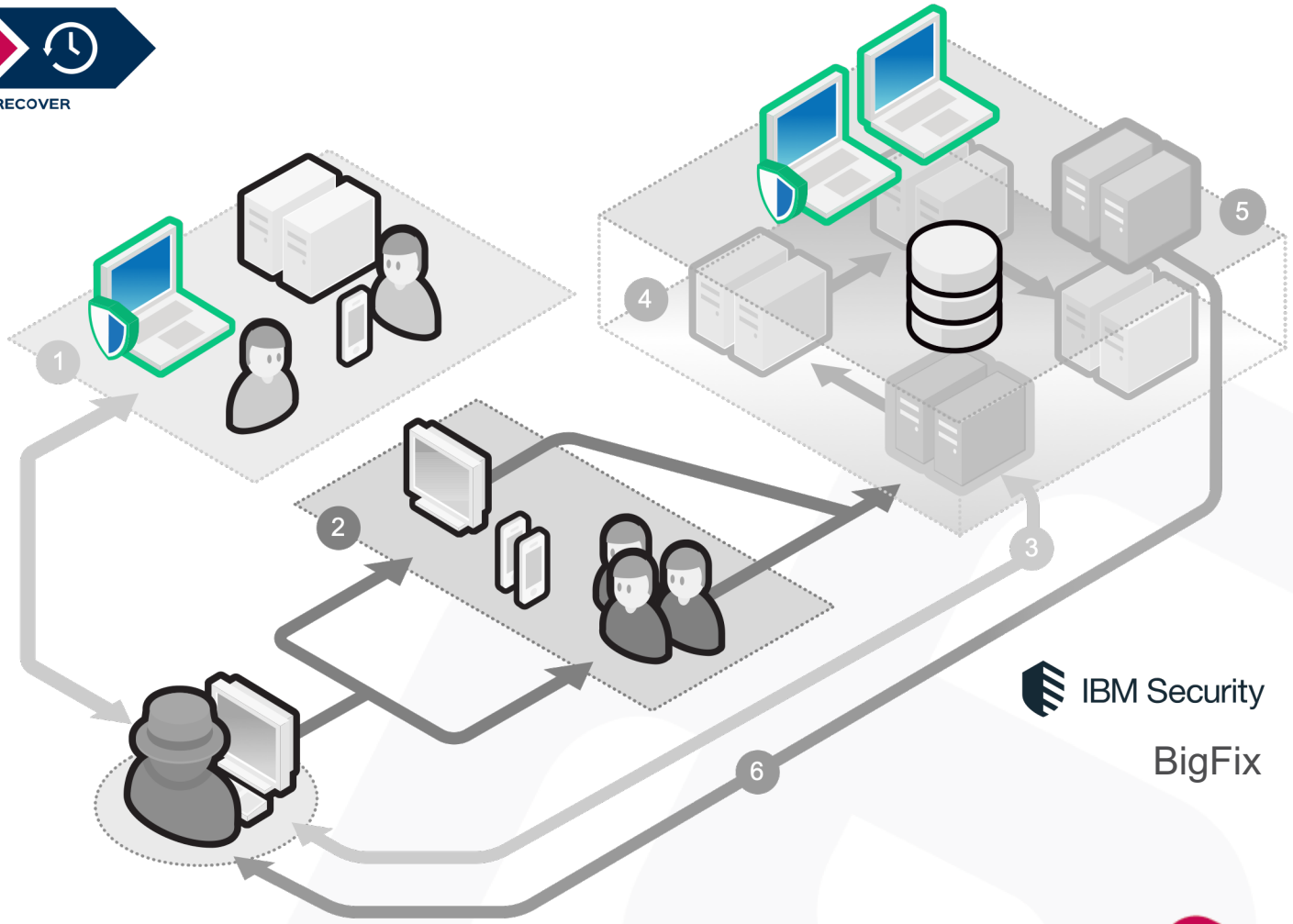
CYBER SECURITY FRAMEWORK


SECURITY ECOSYSTEM
Indicators of compromise
Malware analysis
Threat sharing
THREAT INTEL
Endpoint detection and response
Endpoint patching and management
Malware protection
ENDPOINT
Network forensics and threat management
Firewalls
Sandboxing
Virtual patching
Network visibility and segmentation
NETWORK
Security analytics
Vulnerability management
Threat and anomaly detection
SECURITY ORCHESTRATION & ANALYTICS
Transaction protection
Device management
Content security
MOBILE
ADVANCED FRAUD
Fraud protection
Criminal detection
User behavior analytics
Incident response
Threat hunting and investigation
APPS
Application scanning
Application security management
IDENTITY & ACCESS
Privileged user management
Identity governance and administration
Access management
IDaaS
Mainframe security
DATA
Data protection
Data access control

NIST FRAMEWORK

ENDPOINT

- ENDPOINT DETECTION AND RESPONSE
- ENDPOINT PACHING AND MANAGEMENT
- MALWARE PROTECTION
- ASSET DISCOVERY & INVENTORY

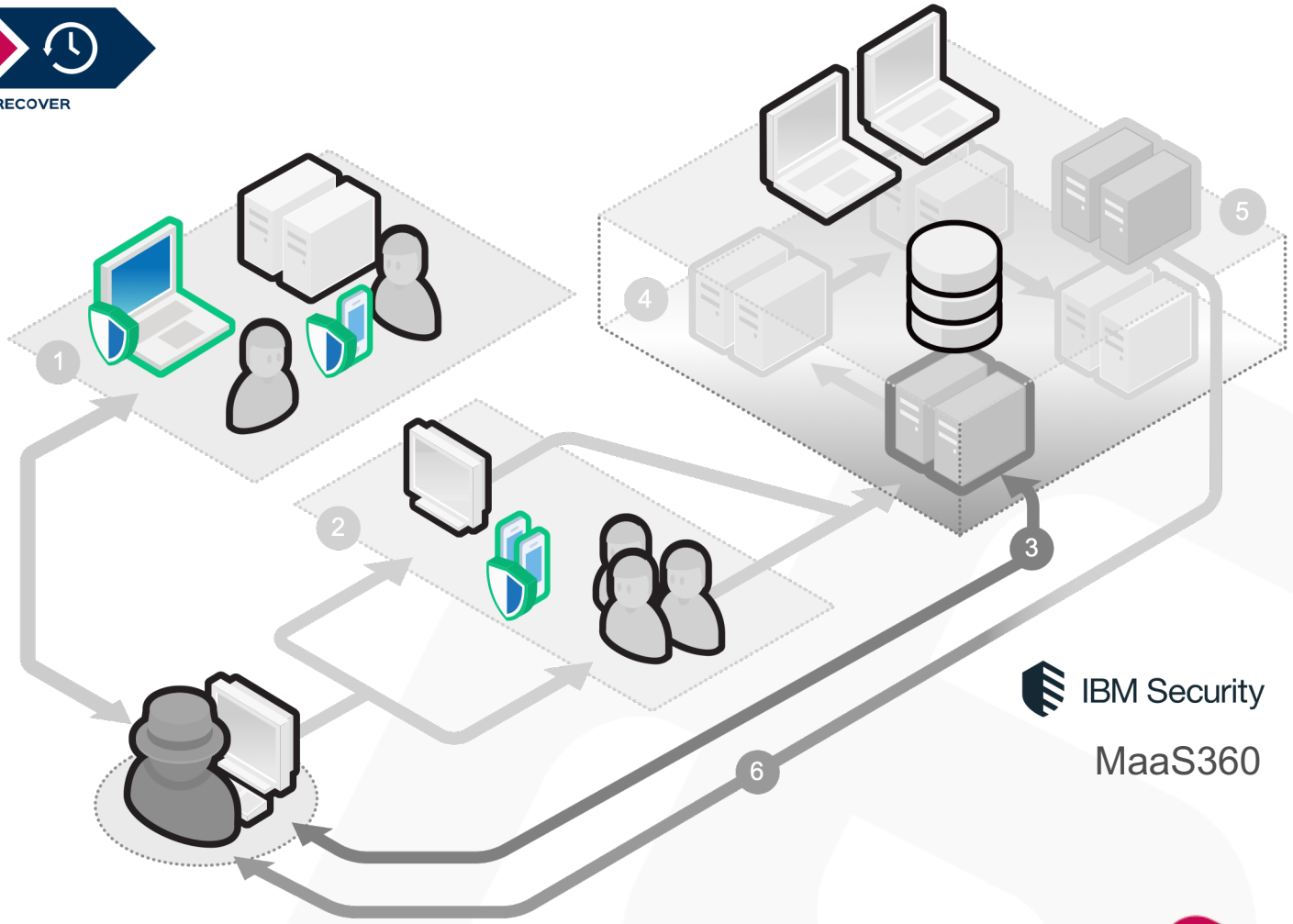


IBM Security
BigFix

NIST FRAMEWORK

MOBILE

- DEVICE MANAGEMENT (**MDM**)
- APP & CONTENT SECURITY (**MAM**)
- ENTERPRISE MOBILITY MANAGEMENT (**EMM**)
- TRANSACTION PROTECTION



IBM Security

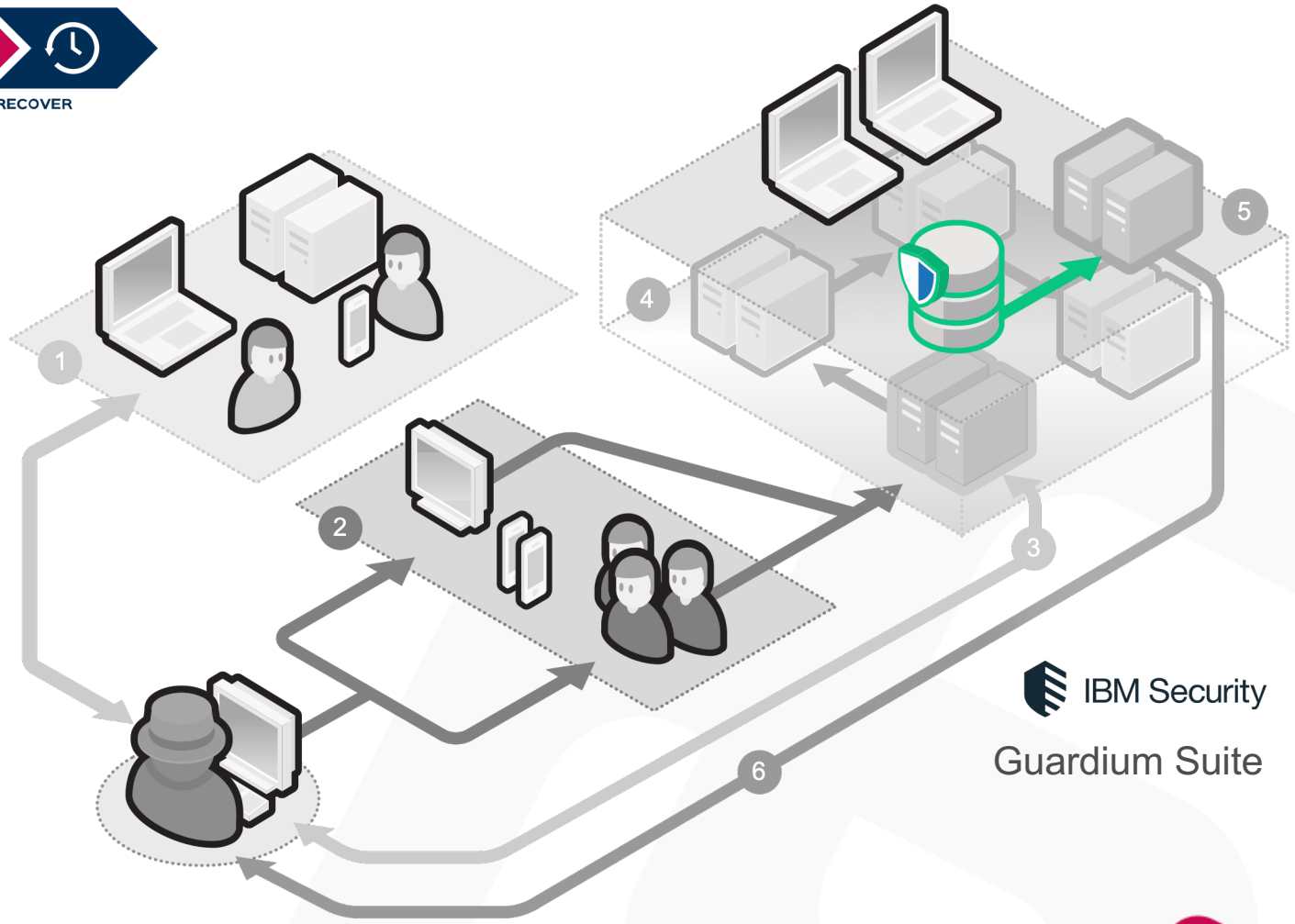
MaaS360

NIST FRAMEWORK

IDENTIFY PROTECT DETECT RESPOND RECOVER

DATA

- DATA DISCOVERY & CLASSIFICATION
- DATA PROTECTION
- DATA ACCESS CONTROL
- DATA RISK GOVERNANCE
- DATA ENCRYPTION & KEY-MANAGER
- DATA LOSS PREVENTION
- DATA ACTIVITY MONITORING (DAM - FAM)



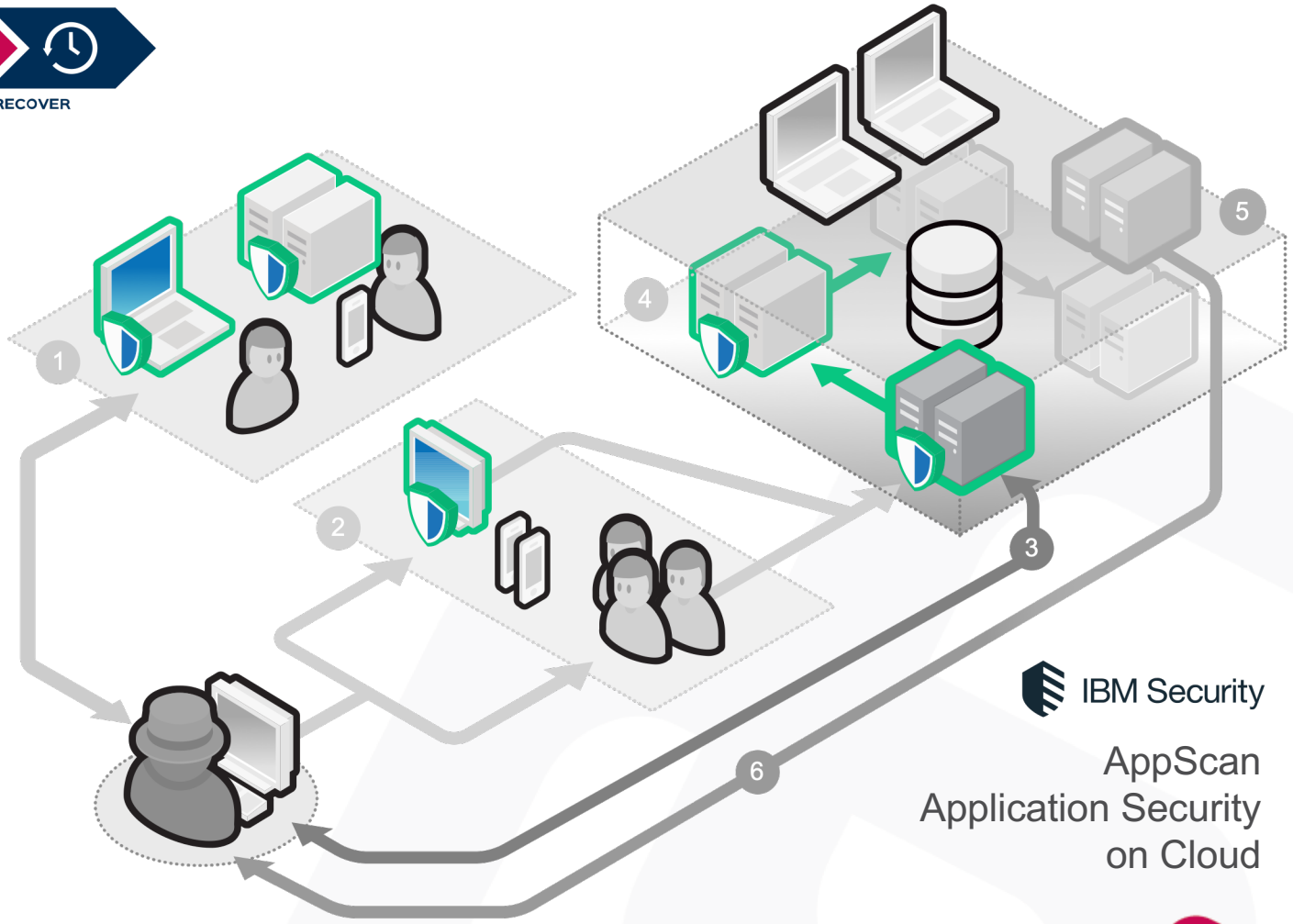
IBM Security

Guardium Suite

NIST FRAMEWORK

APPS

- APPLICATION SCANNING (SAST, DAST, MAST)
- APPLICATION SECURITY MANAGEMENT
- SOURCE CODE REVIEW



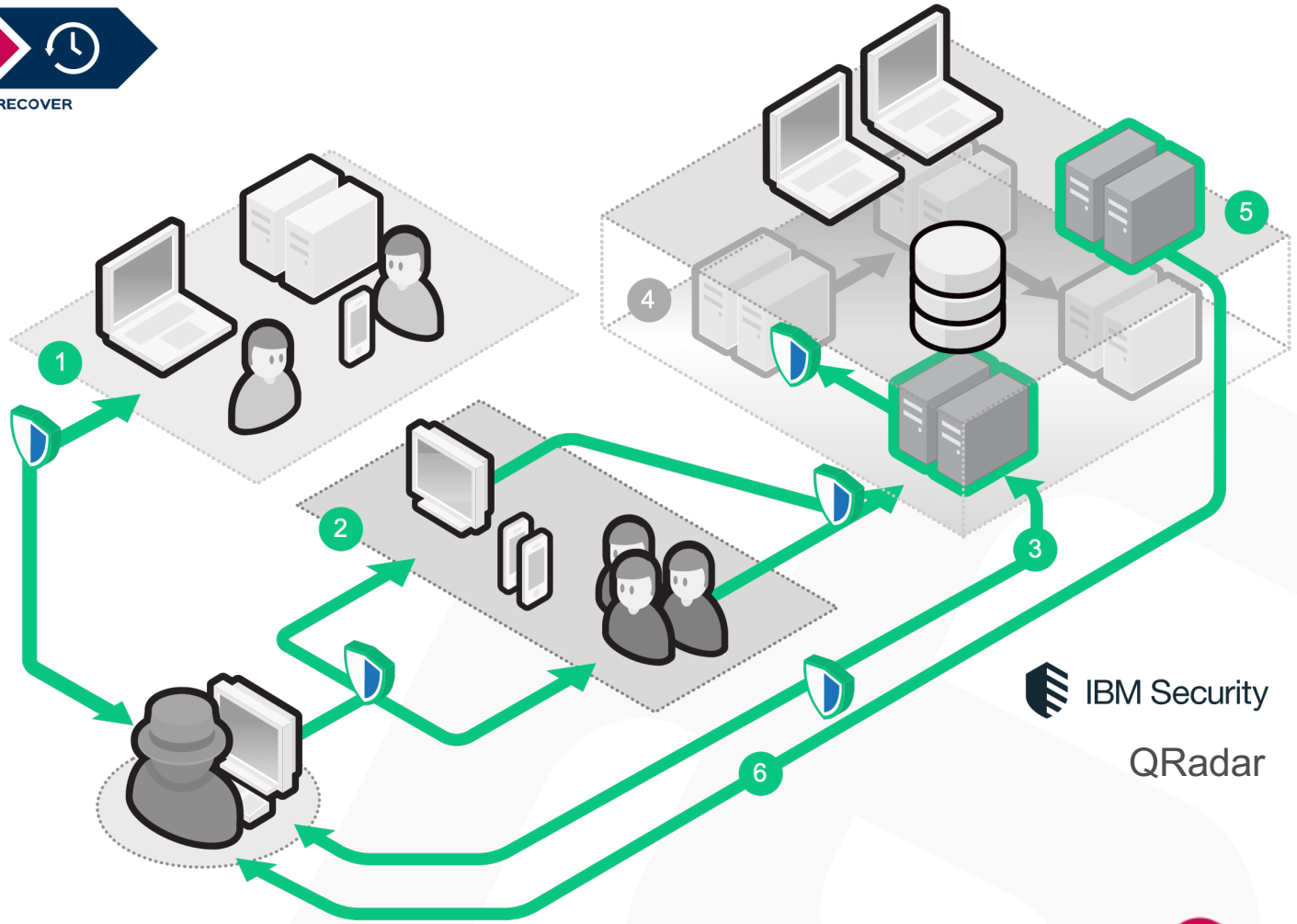
IBM Security

AppScan
Application Security
on Cloud

NIST FRAMEWORK

NETWORK

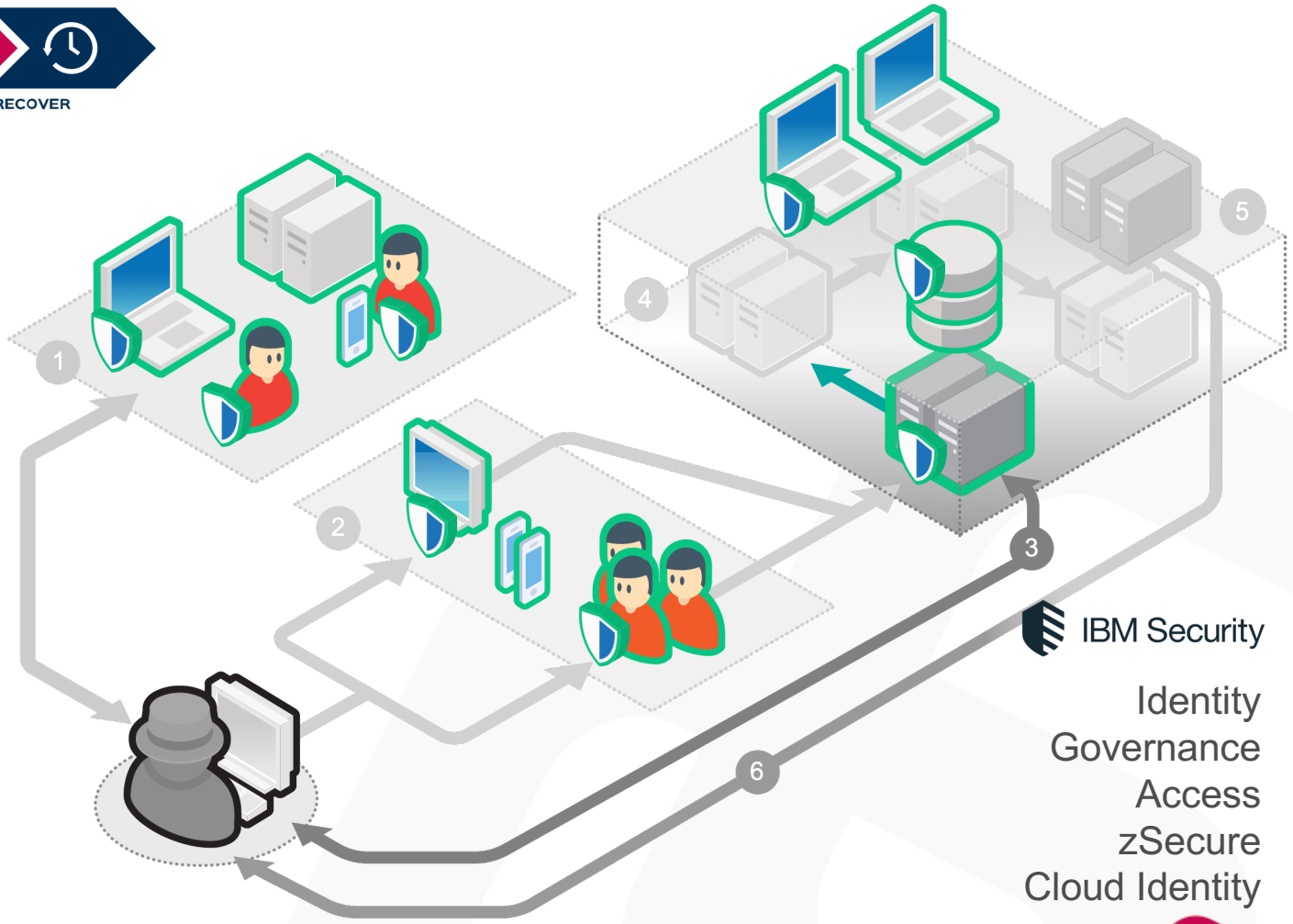
- NETWORK MONITORING & FORENSICS
- NETWORK THREAT MANAGEMENT
- BEHAVIOURAL ANALISYS
- NETWORK VISIBILITY AND SEGMENTATION



NIST FRAMEWORK

IAaG

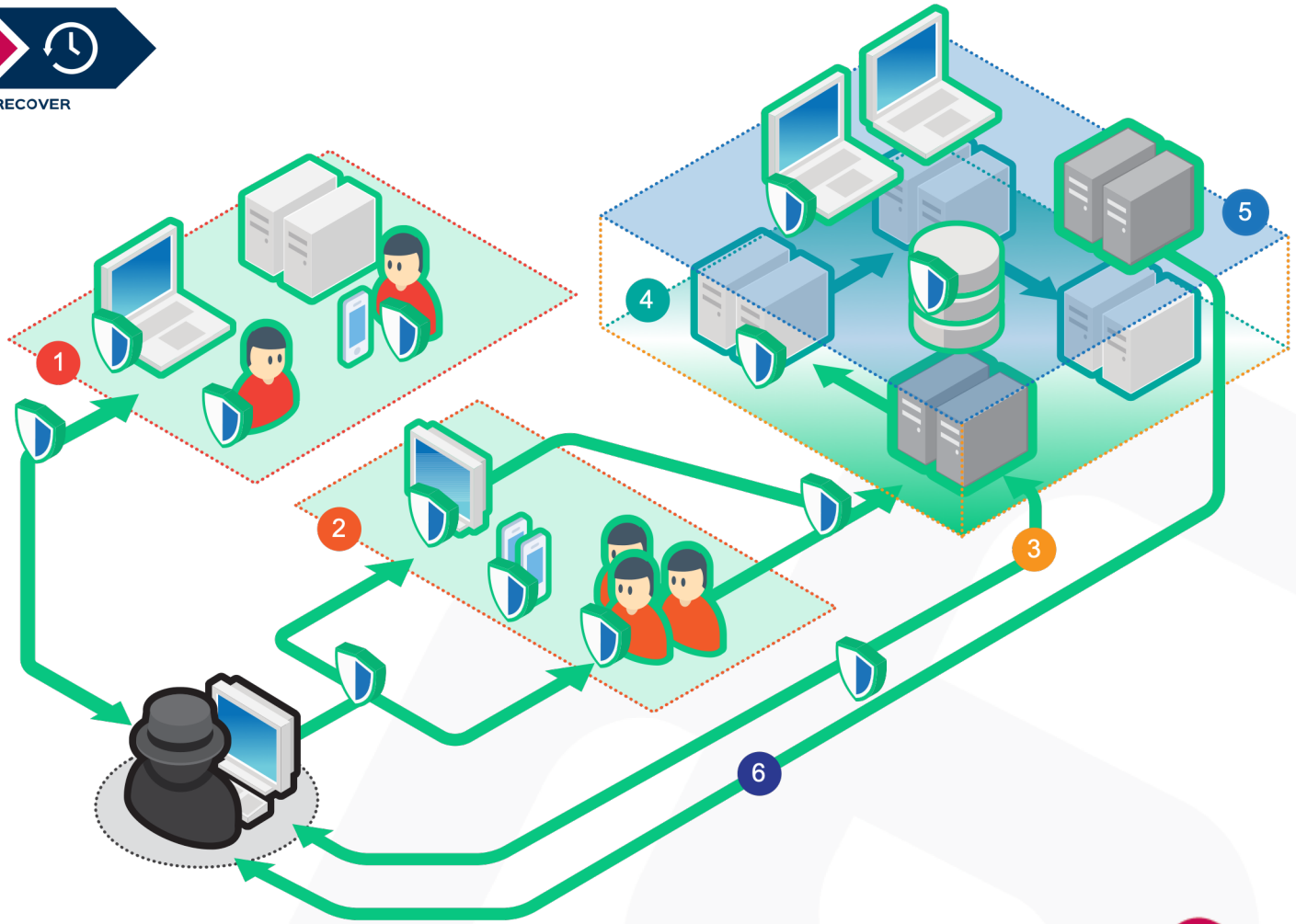
- PRIVILEGED USER MANAGEMENT
- IDENTITY GOVERNANCE AND ADMINISTRATION
- ACCESS MANAGEMENT
- MAINFRAME SECURITY
- IDaaS



IBM Security

Identity
Governance
Access
zSecure
Cloud Identity

NIST FRAMEWORK



NIST FRAMEWORK

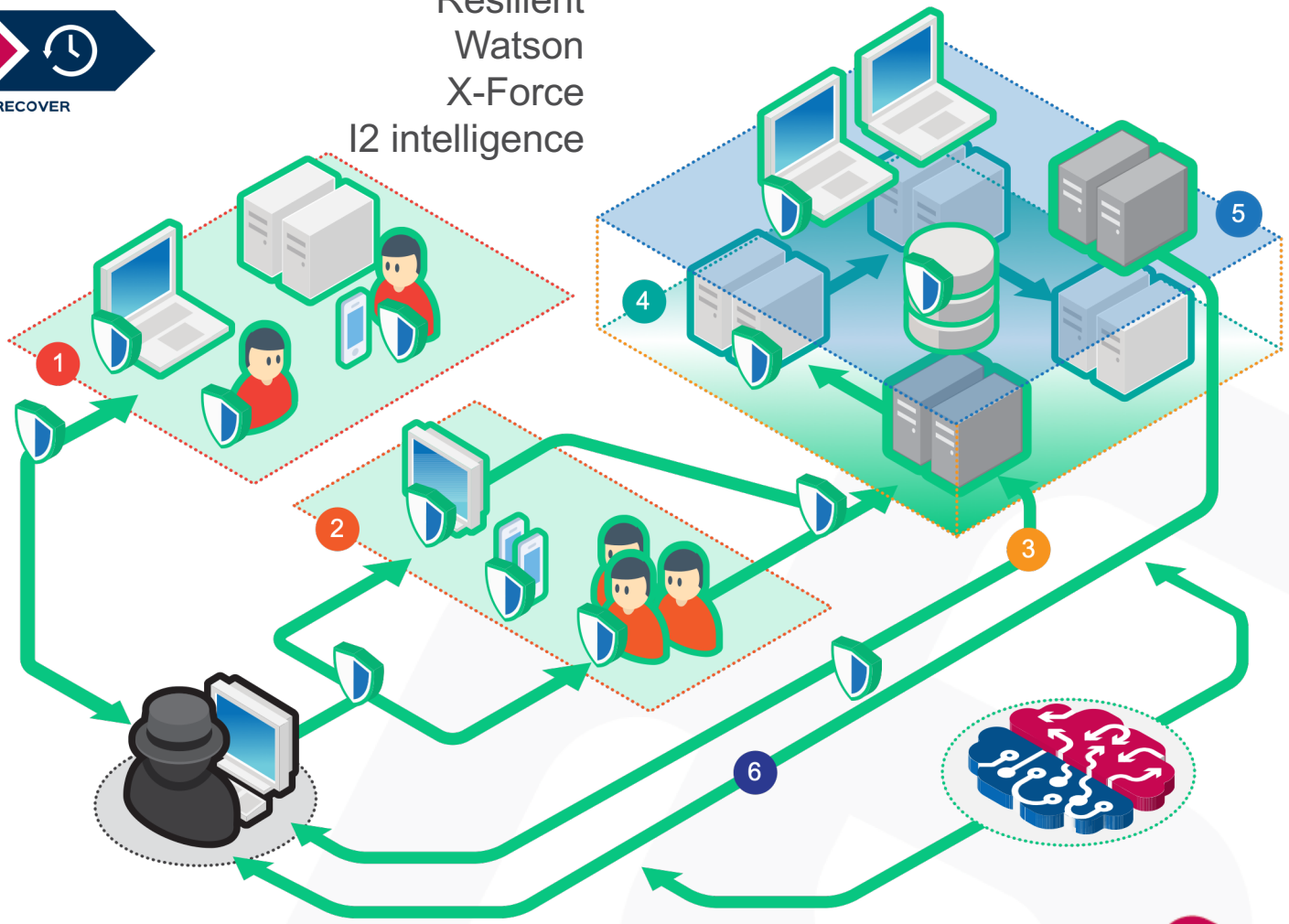
QRadar
Resilient
Watson
X-Force
I2 intelligence

IBM Security

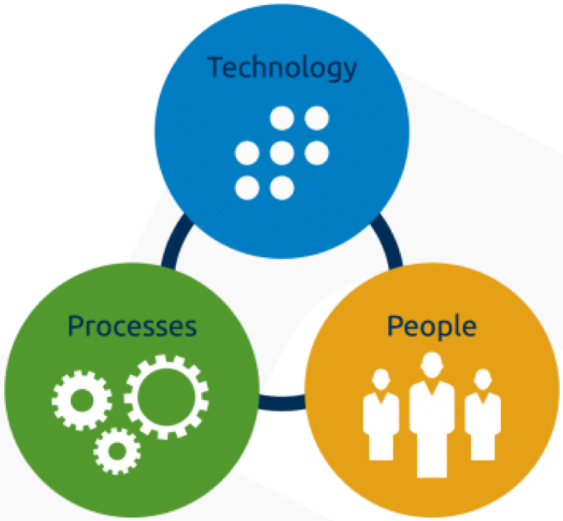
SOAR

THREAT INTEL

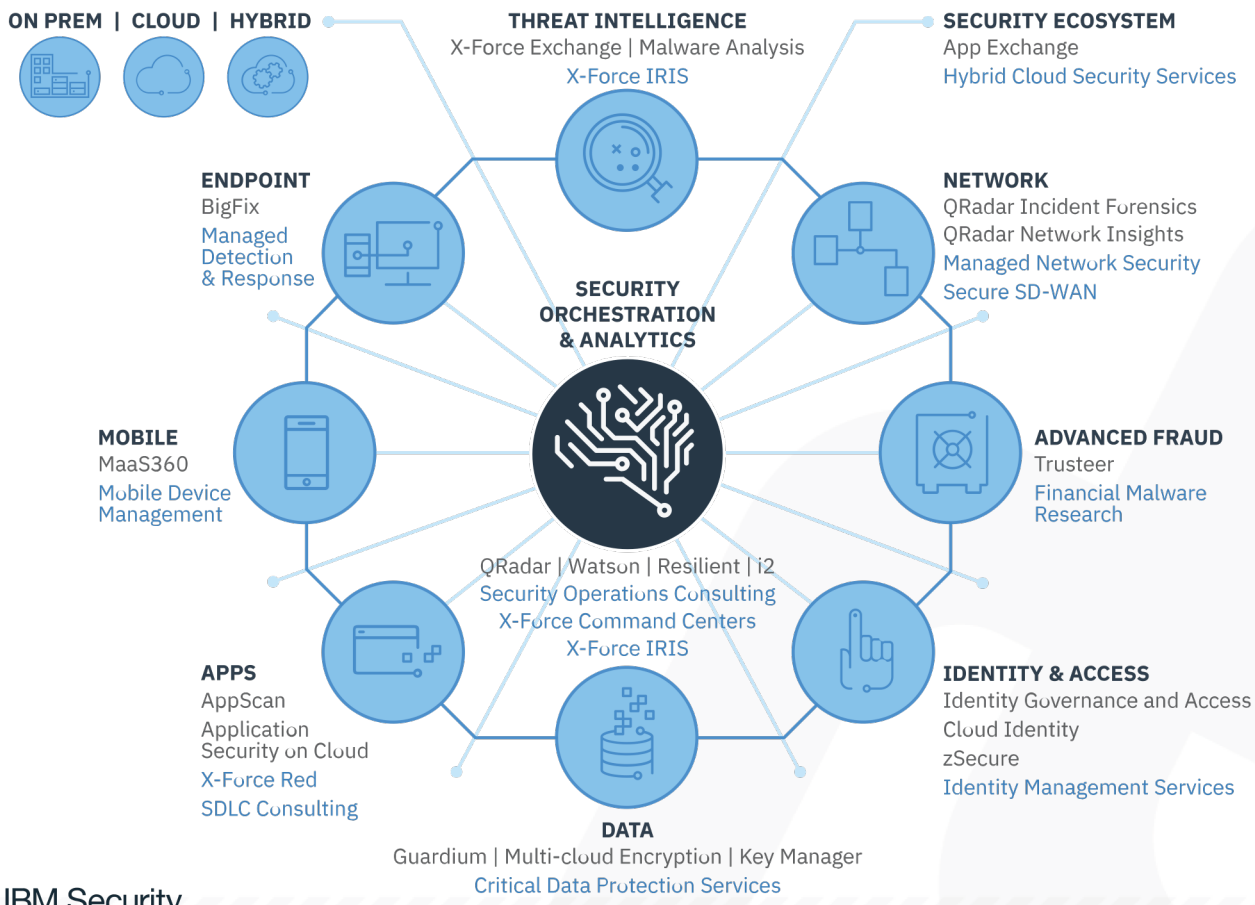
- THREAT AND ANOMALY DETECTION
- BEHAVIOR ANALYTICS
- SECURITY ANALYTICS
- VULNERAVILITY MANAGEMENT
- INCIDENT RESPONSE
- HUNTING AND INVESTIGATION



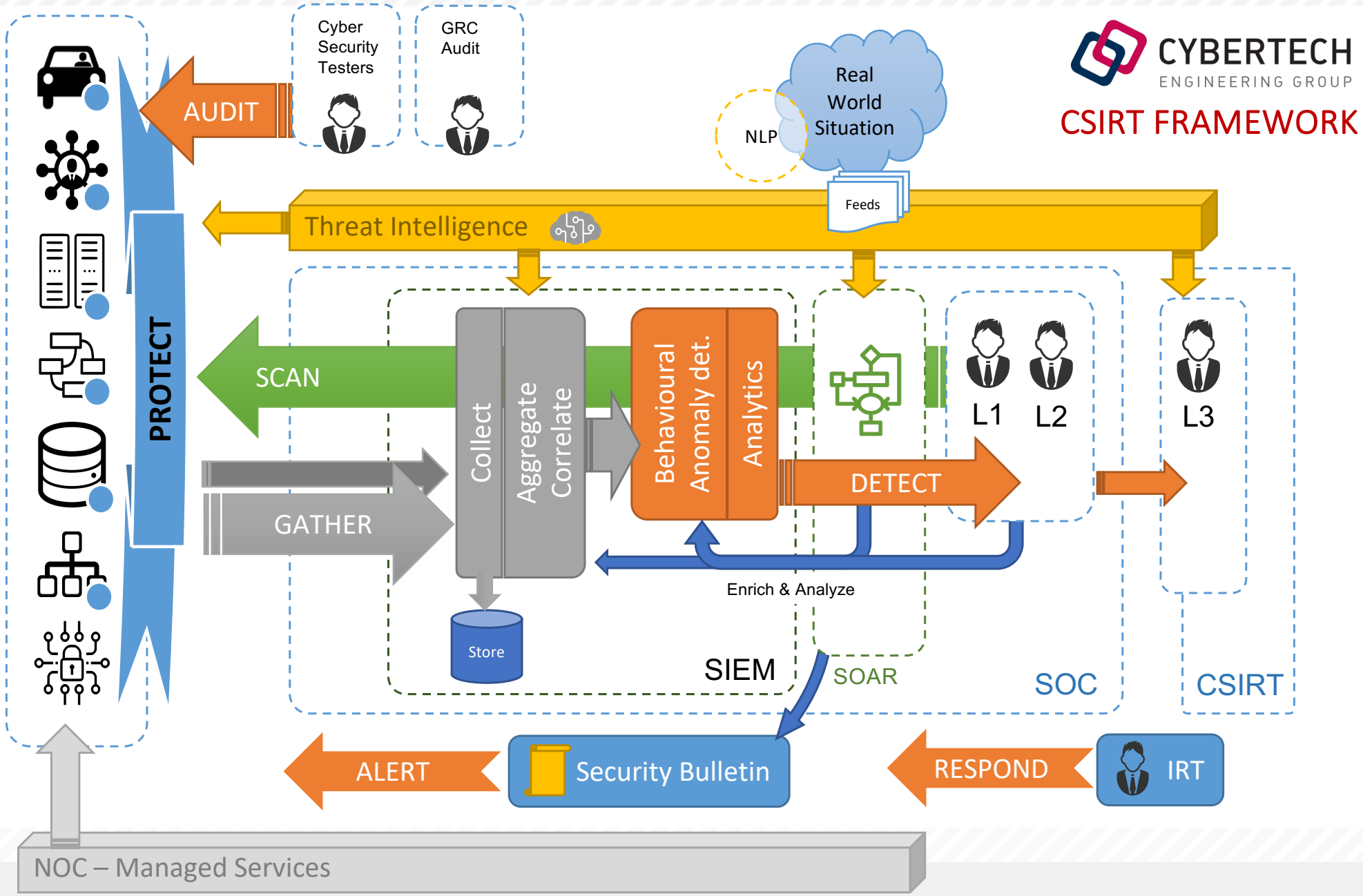
PEOPLE - PROCESS - TECHNOLOGY



IBM IMMUNE SYSTEM



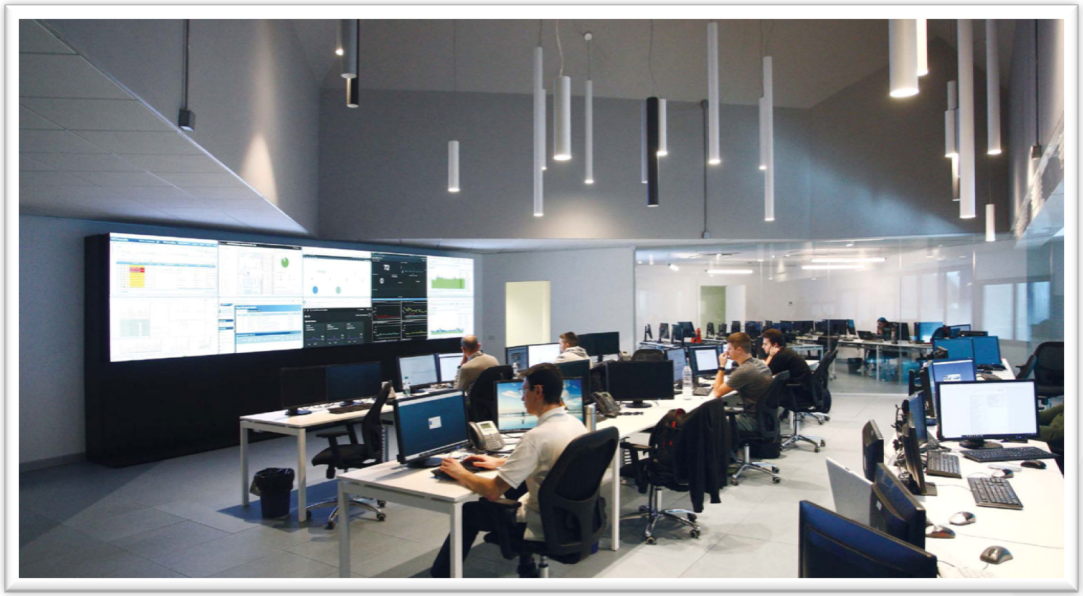
IBM Security

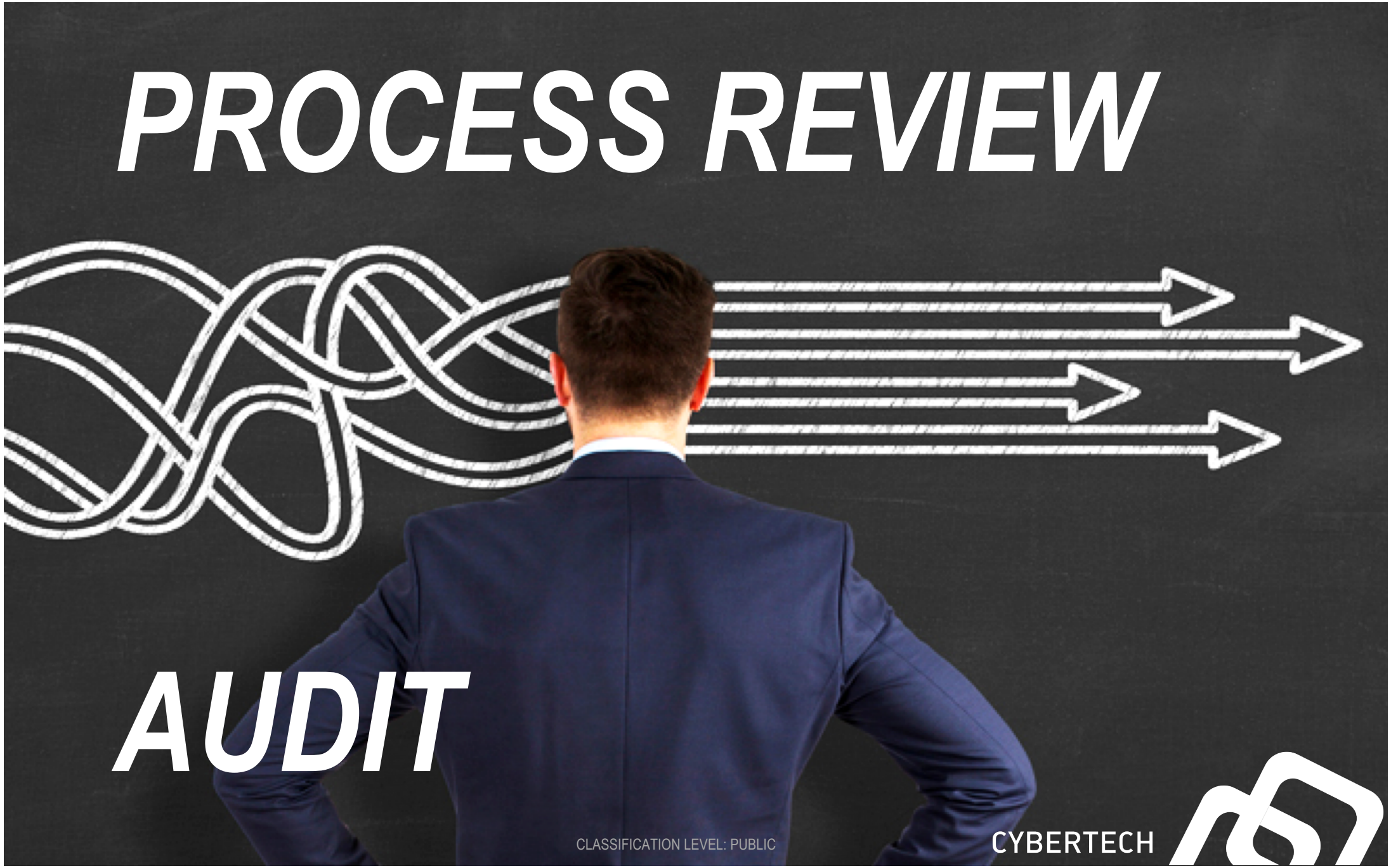

CYBERTECH
ENGINEERING GROUP
CSIRT FRAMEWORK
Cyber Security Testers
GRC Audit
AUDIT
Real World Situation
NLP
Feeds
Threat Intelligence
PROTECT
SCAN
GATHER
Collect
Aggregate
Correlate
Behavioural Anomaly det.
Analytics
DETECT
L1
L2
L3
Enrich & Analyze
Store
SIEM
SOAR
SOC
CSIRT
ALERT
Security Bulletin
RESPOND
IRT
NOC – Managed Services

SOC / CSIRT

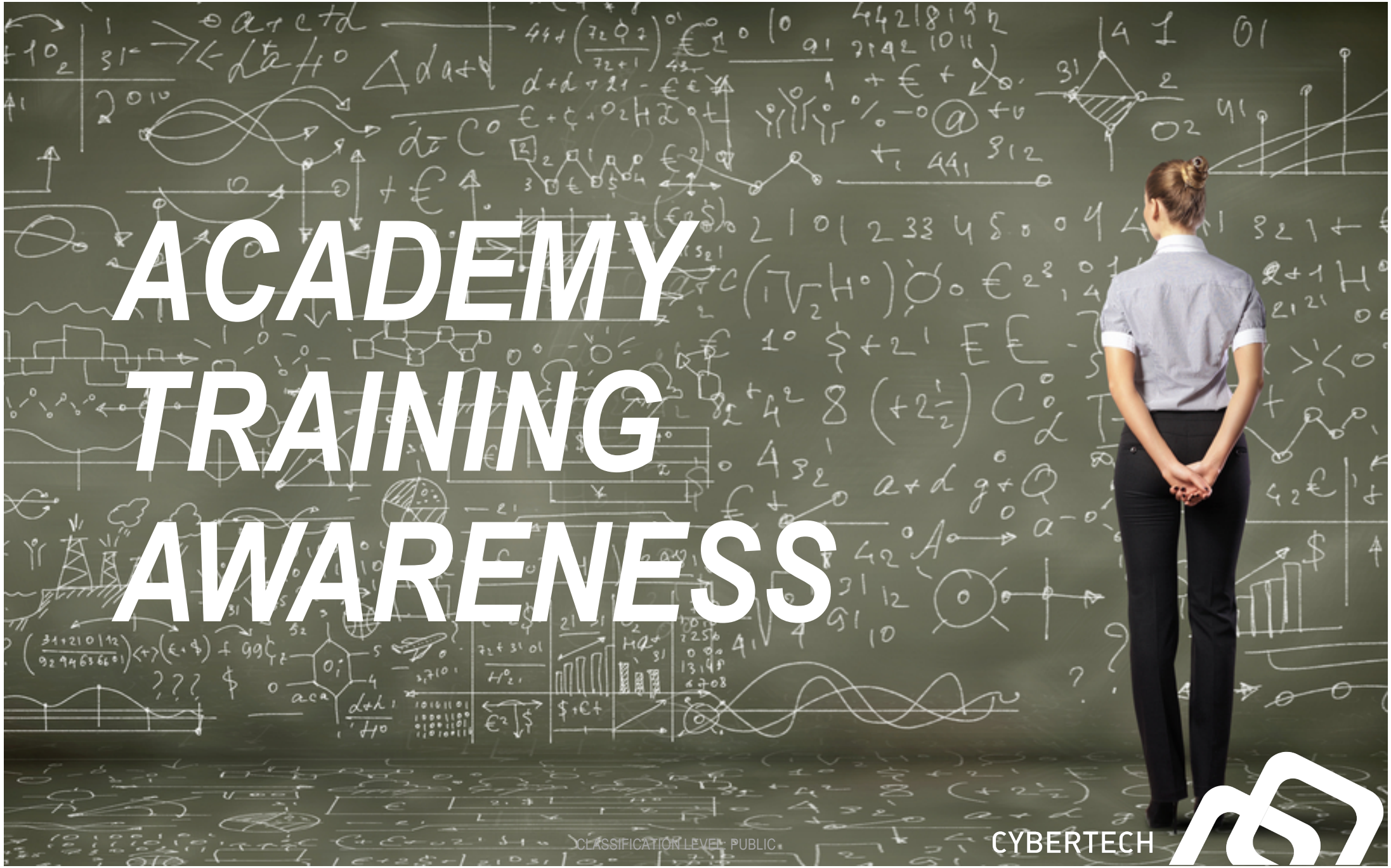
CYBERTECH
ENGINEERING GROUP

ENGINEERING





CYBERTECH


ACADEMY
TRAINING
AWARENESS
CLASSIFICATION LEVEL: PUBLIC
CYBERTECH


IT'S ONLY A MATTER
OF ONE SINGLE
WRONG CLICK
CYBERTECH


GRAZIE PER
L'ATTENZIONE
CYBERTECH