OTORIO

Industrial cyber risk management solutions

How Machine Learning {ML} Powered Industrial Cybersecurity Boosts Production

Smart Orchestration, Automation & Results

Shiran Kleiderman

Sept. 2019

www.otorio.com

OTORIO

Managed Detection & Response (MDR)

Powered by

Industrial-Native SOAR

(Security Orchestration, Automation & Response)

Shiran Kleiderman
Director of Customer Delivery

Previous experience as CTO of
Dark Web Intelligence & Investigations at
K2 Intelligence / BlueVoyant

Military & private sector experience: Cryptography, Data Science,
Risk Mitigation, Penetration Testing

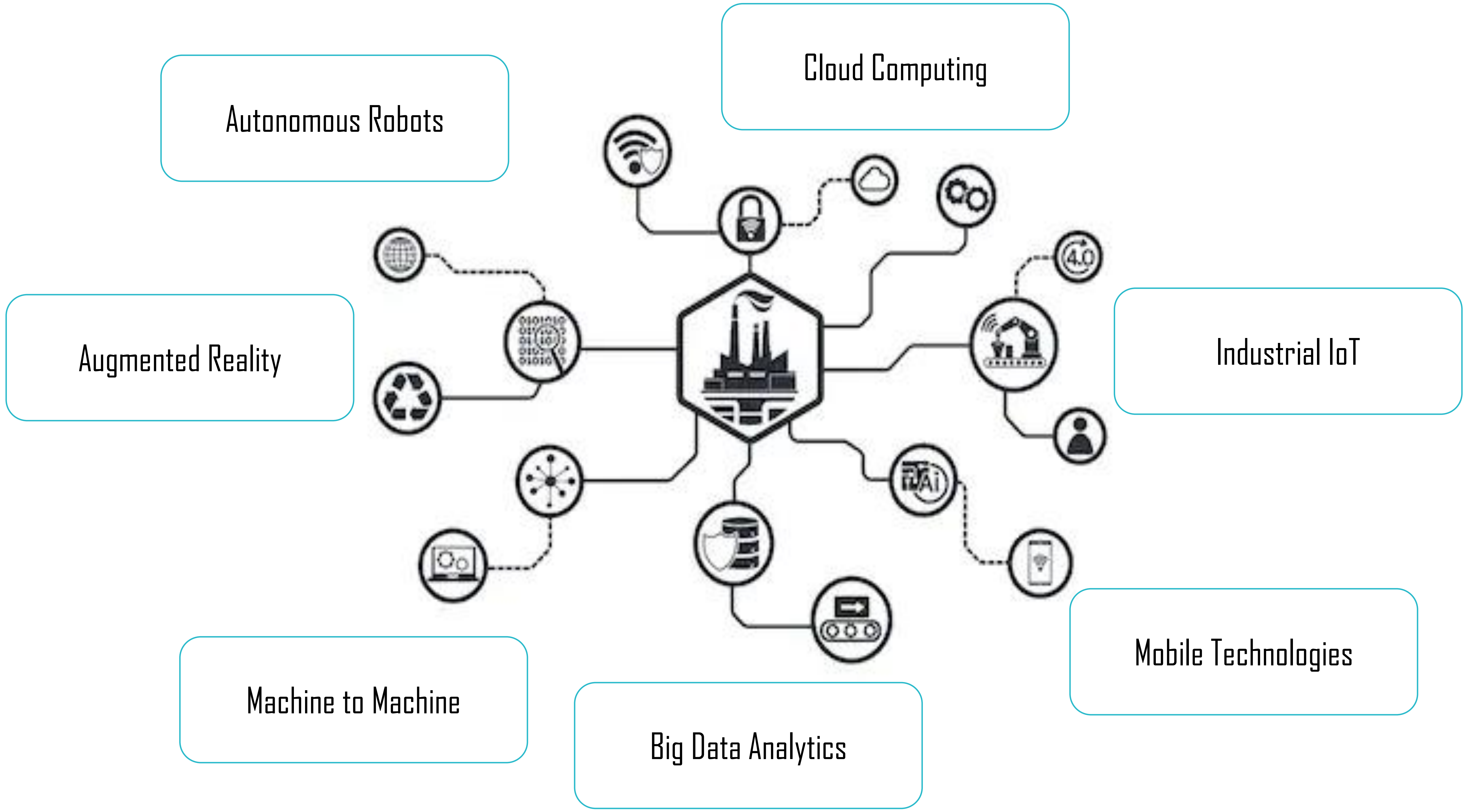
INDUSTRY 4.0 IS AN ECONOMIC GAME CHANGER

Improved efficiency

Improved productivity

Improved quality

Reduced downtime



Autonomous Robots

Cloud Computing

Augmented Reality

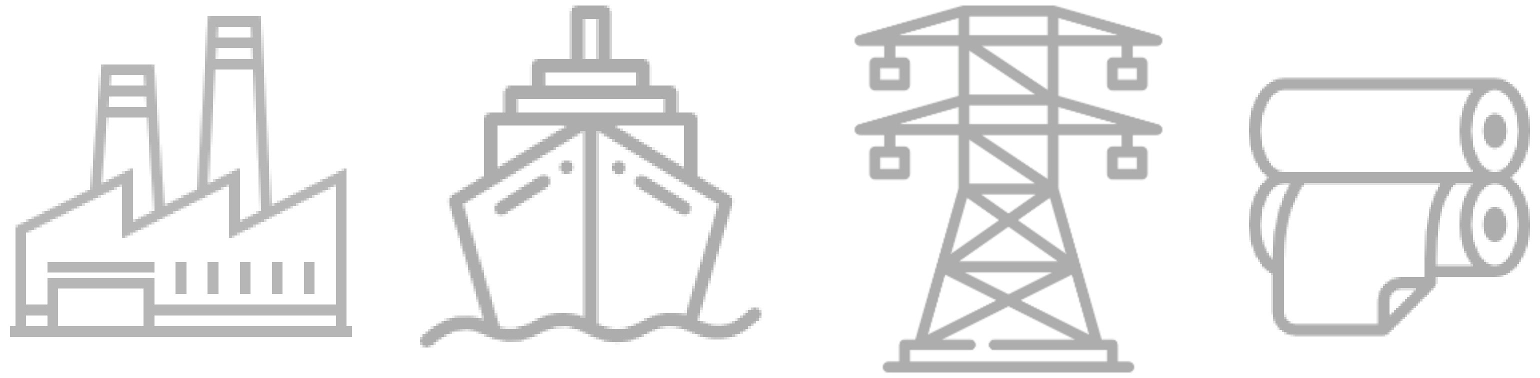
Industrial IoT

Machine to Machine

Big Data Analytics

Mobile Technologies

…AND SO ARE THE THREATS



2010 STUXNET

2014 HAVEX

2016 BlackEnergy 3

2017 TRISIS

2017 NotPetya

Shamoon 3 2018

LockerGoga 2019

INDUSTRIAL SECURITY IS FACING A BIG CHALLENGE

Cyber-attack surface increased by digital transformation

Difficulty in establishing a coherent & clear picture; asset management & security posture

Cybersecurity isn't built into production devices, machinery

Existing OT cybersecurity solutions are reactive and not preemptive

Lack of cybersecurity skills on the production floor

Need For
"Secure Production/Engineering Lifecycle"

EFFECTIVE INDUSTRIAL CYBERSECURITY IS:

SIMPLE

(1)

COLLABORATIVE

(2)

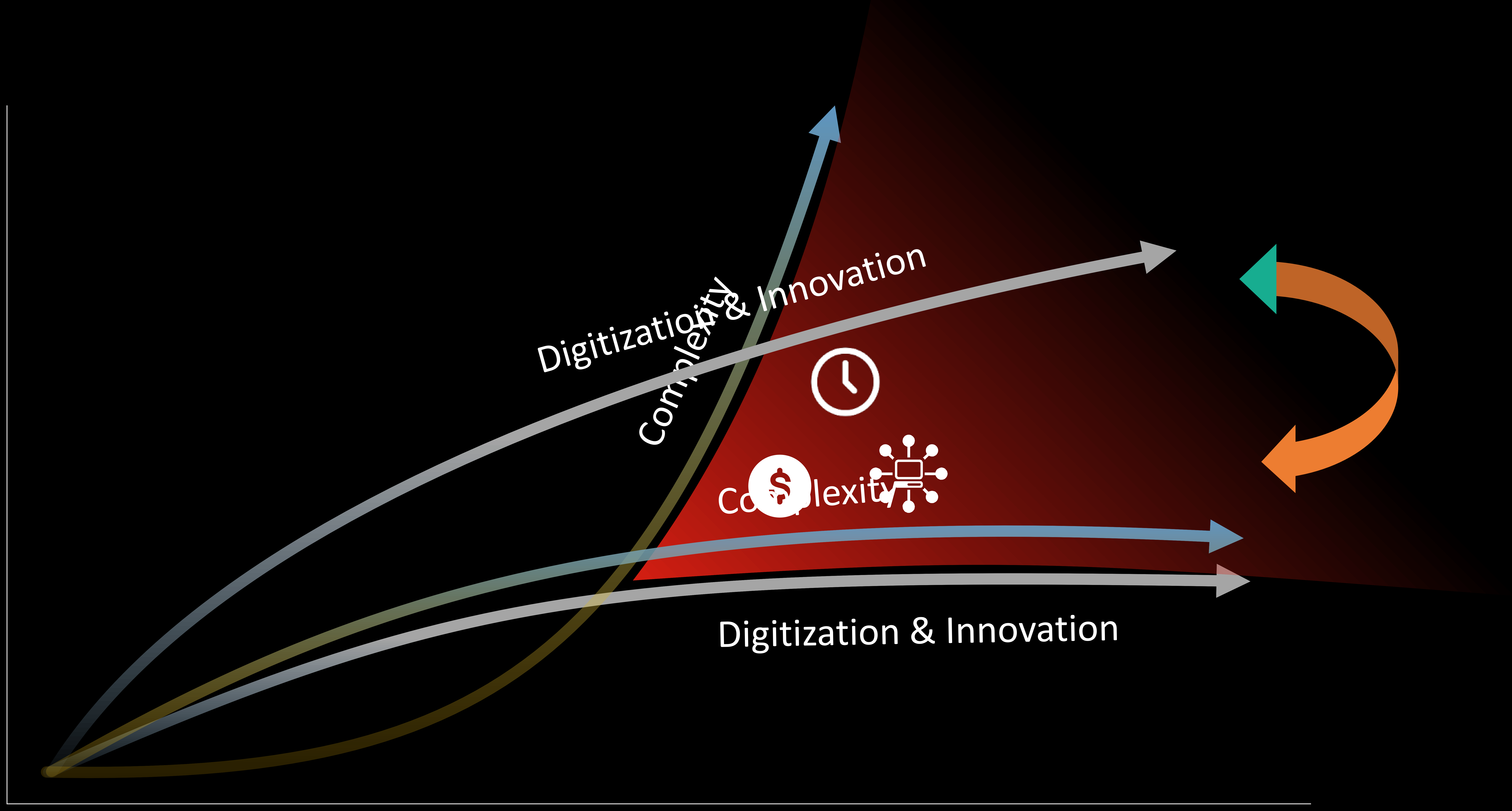
AUTOMATED

(3)

01 SIMPLE

Useable, Seamless

SECURE PRODUCTION BEGINS WITH REDUCING COMPLEXITY



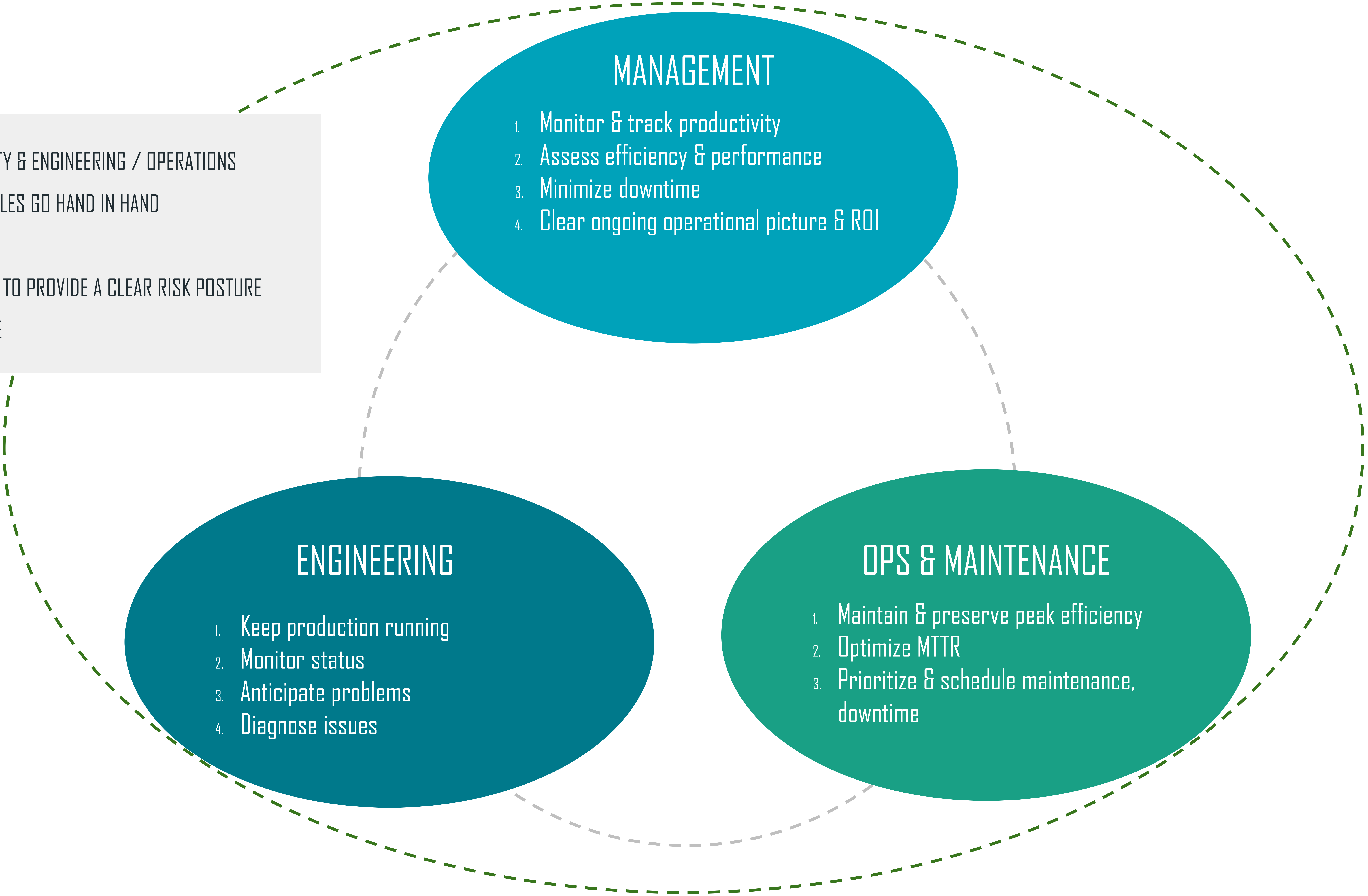
02 COLLABORATIVE

From the Production Floor
to the Boardroom

PRODUCTION & OPERATIONS PERSPECTIVES;

ESTABLISHING THE SECURITY LINK / MINDSET

- SECURITY & ENGINEERING / OPERATIONS LIFECYCLES GO HAND IN HAND
- GOAL IS TO PROVIDE A CLEAR RISK POSTURE PICTURE



MANAGEMENT

1. Monitor & track productivity
2. Assess efficiency & performance
3. Minimize downtime
4. Clear ongoing operational picture & ROI

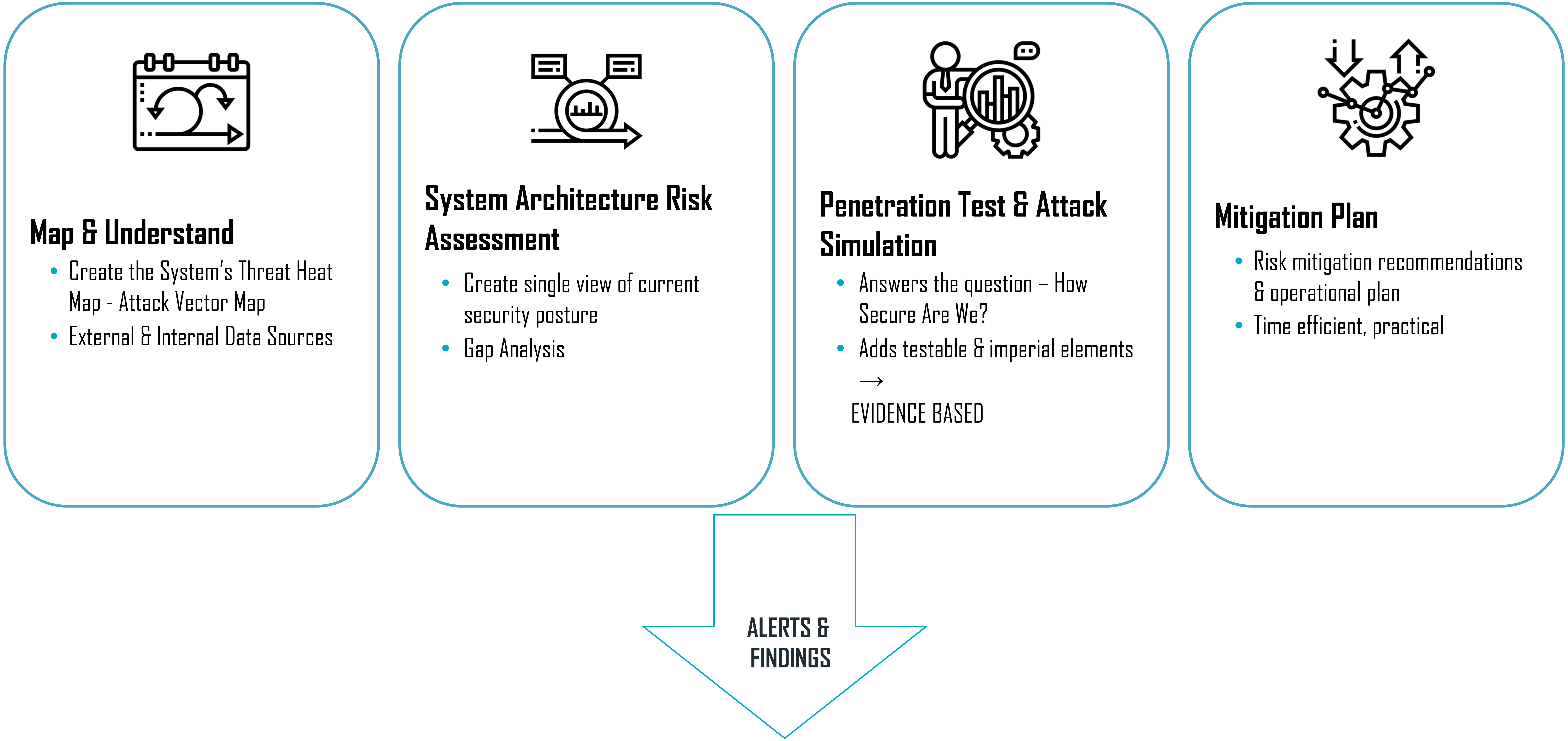
ENGINEERING

1. Keep production running
2. Monitor status
3. Anticipate problems
4. Diagnose issues

OPS & MAINTENANCE

1. Maintain & preserve peak efficiency
2. Optimize MTTR
3. Prioritize & schedule maintenance, downtime

RISK ASSESSMENT & SECURITY ENGINEERING FLOW;
EVIDENCE BASED METHODOLOGY



Map & Understand

- Create the System's Threat Heat Map - Attack Vector Map
- External & Internal Data Sources

System Architecture Risk Assessment

- Create single view of current security posture
- Gap Analysis

Penetration Test & Attack Simulation

- Answers the question – How Secure Are We?
- Adds testable & imperial elements

→ EVIDENCE BASED

Mitigation Plan

- Risk mitigation recommendations & operational plan
- Time efficient, practical

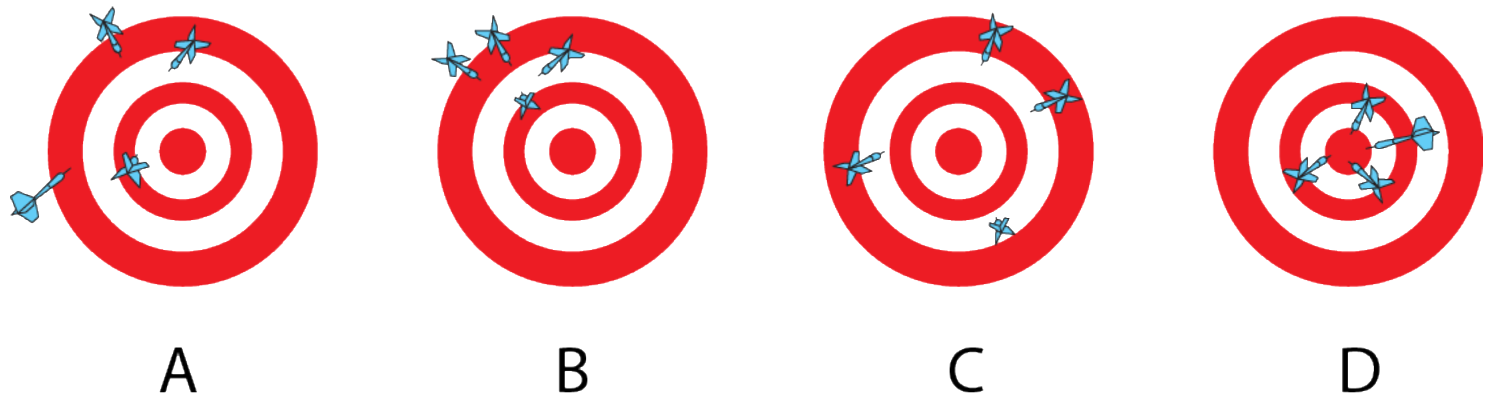
ALERTS & FINDINGS

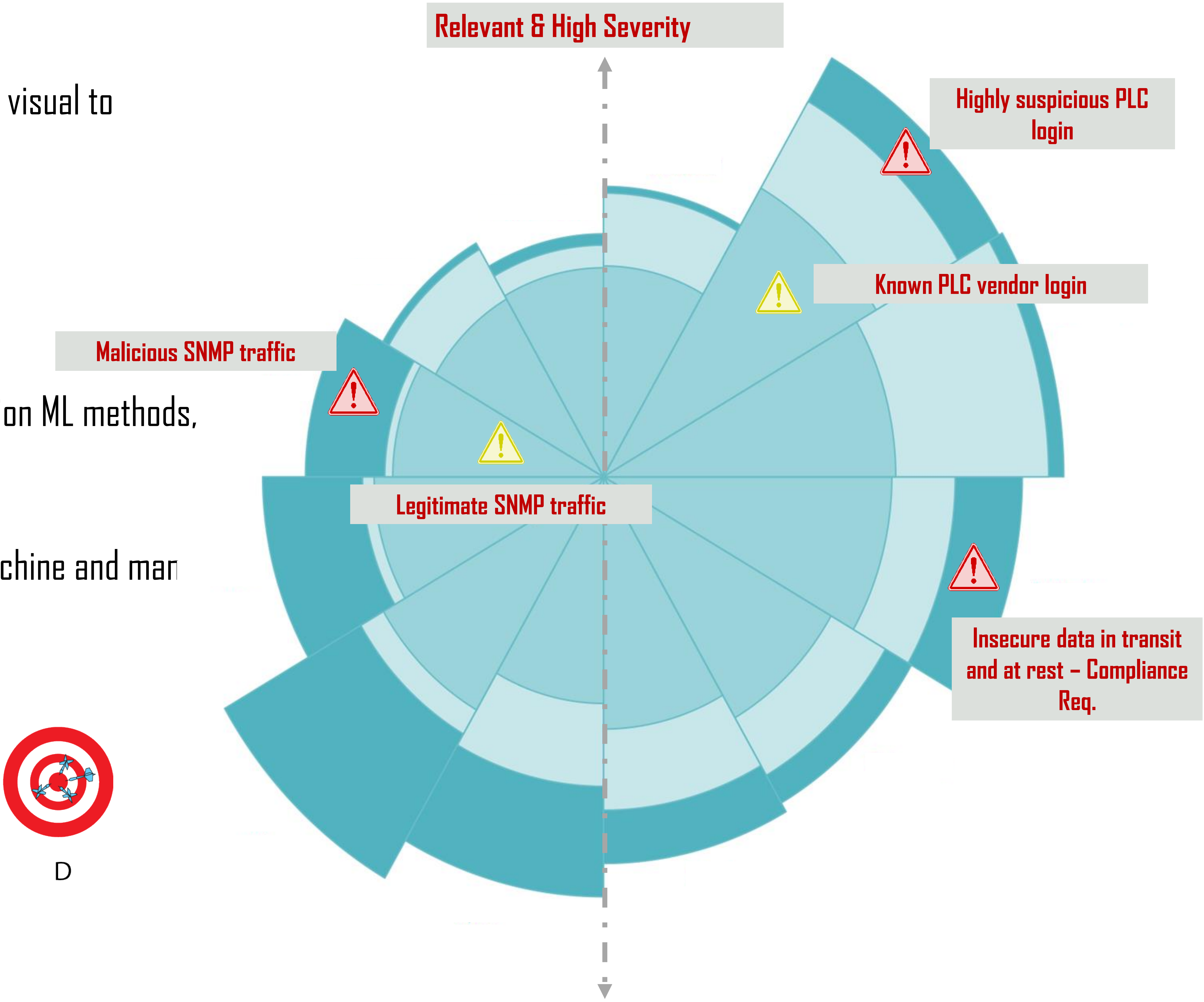
CYBER QUALIFICATION: ALERT & INSIGHT MANAGEMENT

- Florence Nightingale chart used as a data visual to organize alerts by:
  1. Relevance = qualifies as a finding?
  2. Severity, threat level
  3. Topic, context

- Cyber Qualification utilizes Outlier Detection ML methods, and an Ensemble ML approach

- Semi-supervised Machine Learning by machine and man




Relevant & High Severity

Highly suspicious PLC login

Known PLC vendor login

Malicious SNMP traffic

Legitimate SNMP traffic

Insecure data in transit and at rest – Compliance Req.

03 AUTOMATED

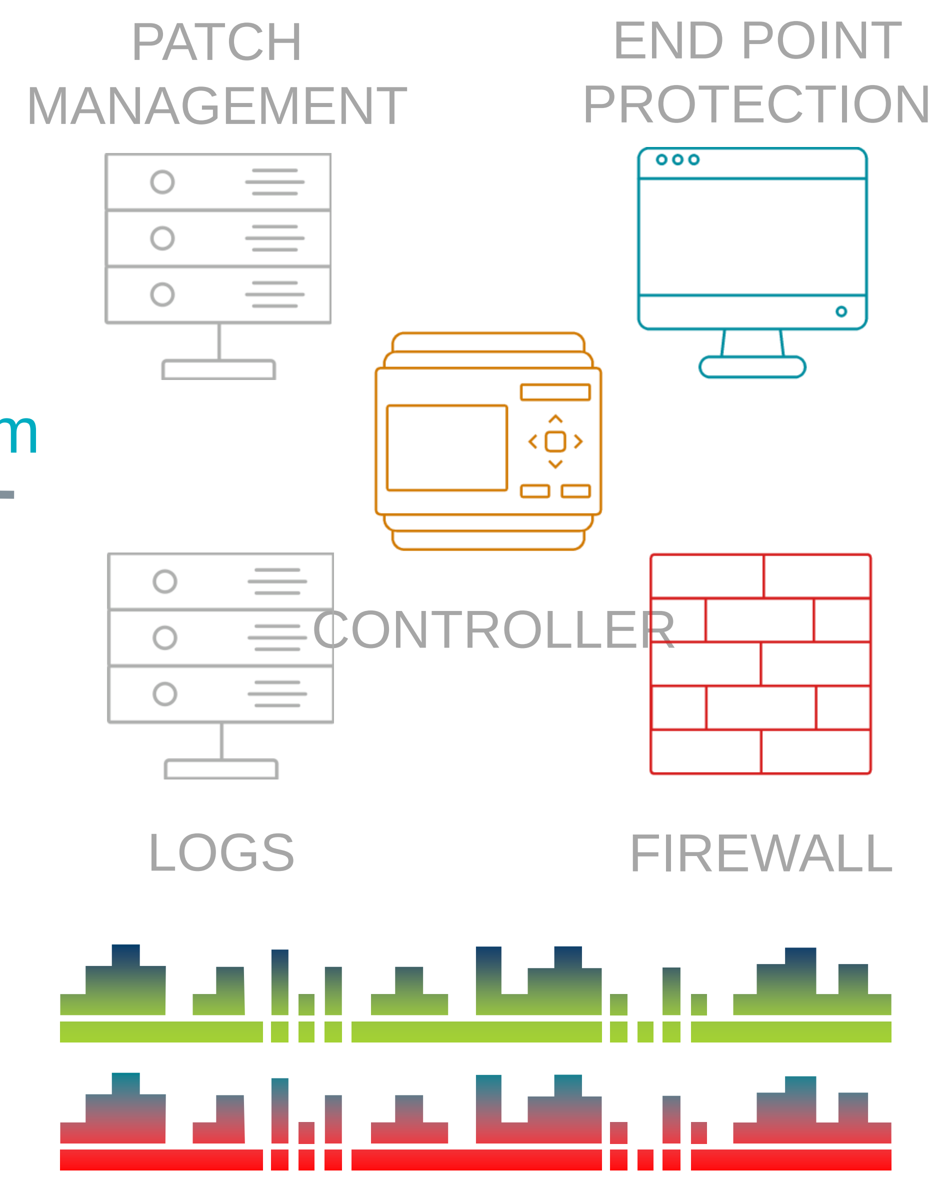
Concrete Insights & Results

CONTINUOUS SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

PRODUCTION FLOOR BLUEPRINT → **ATTACK GRAPH ANALYSIS**

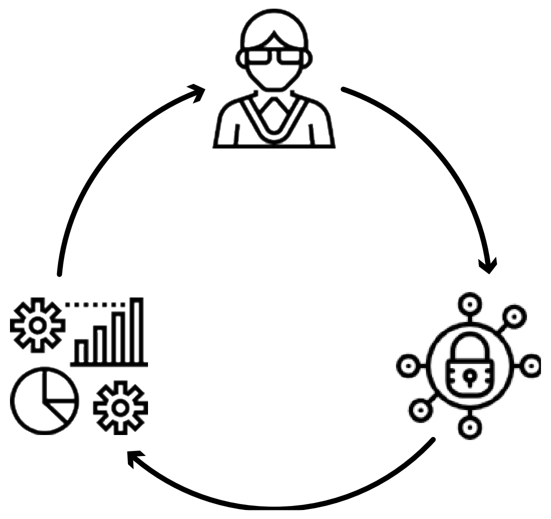
Attack Vectors

PRODUCTION FLOOR DATA SOURCES



Ongoing Stream

EXPERT RESEARCH TEAM ENRICHMENT



Threat Intelligence

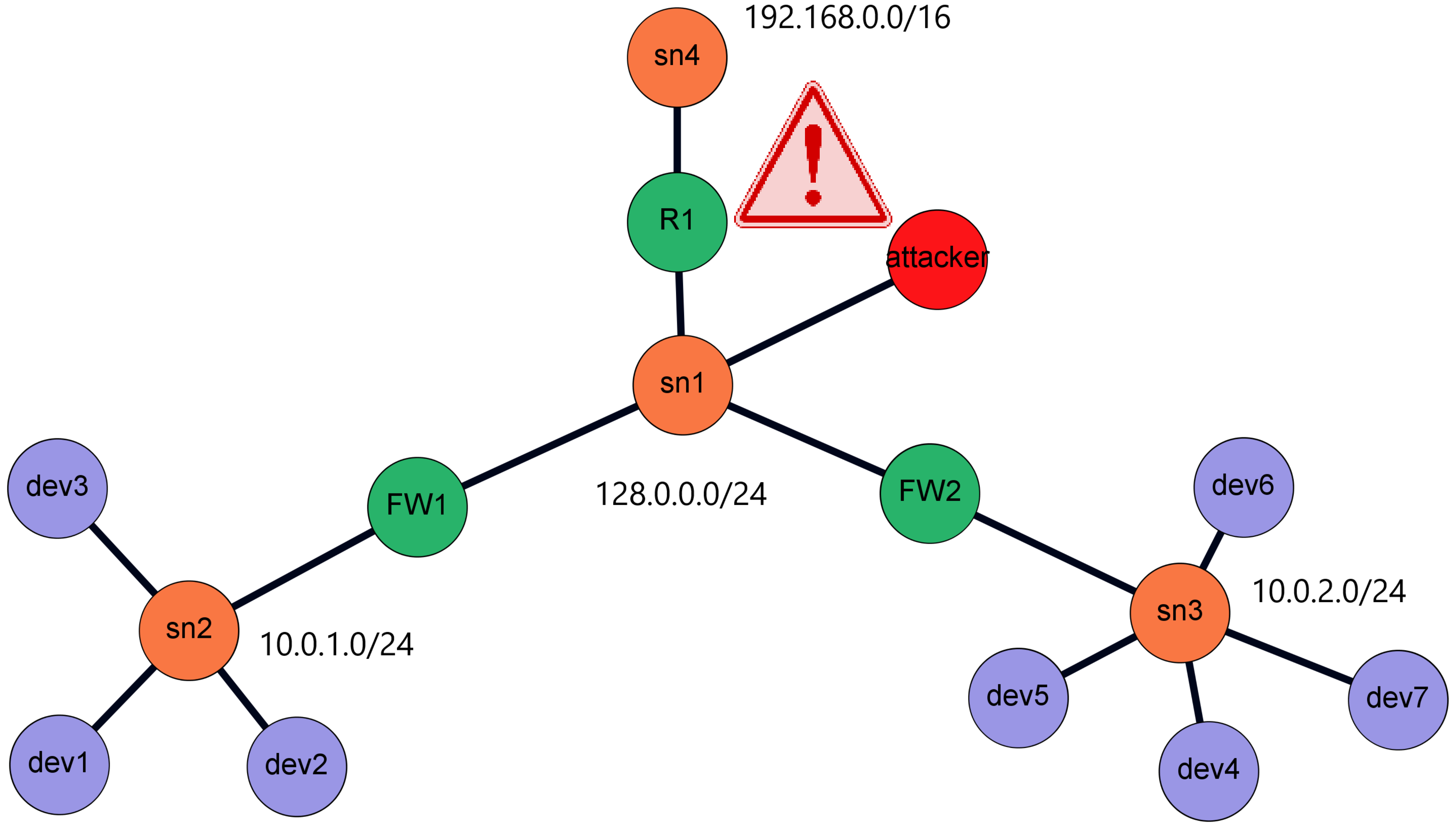
Company specific and sectorial analysis & insights

KEY OUTPUT:

1. Security risk assessment
2. Clear mitigation steps for each risk
3. Prioritized action items for risk reduction
4. Automated alert/findings enrichment & response

ATTACK GRAPH ANALYSIS

- A Production Floor Blueprint is created
- Network and vulnerability data are cross correlated using an Attack Graph ML model
- The attack graph represents all possible ways in which an attacker can gain access to a specific asset
- Specific attack vectors and paths are pinpointed

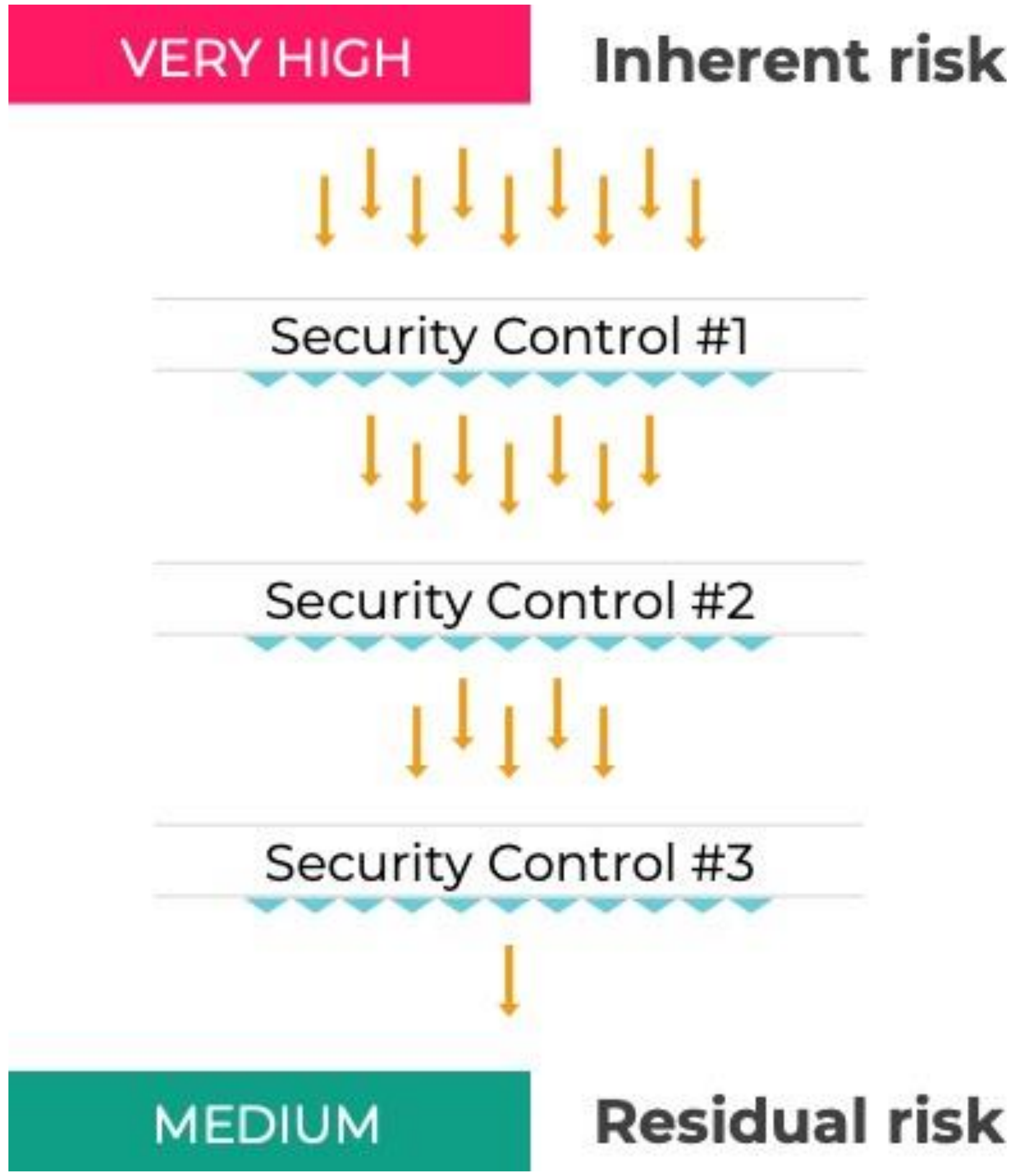


Issue ID	Device ID	IP	Vulnerability ID	Port	Protocol	Type
0	dev1	10.0.1.1	vul1	1	TCP	Remote Exploit
1	dev1	10.0.1.1	vul2	2	TCP	Remote Exploit
2	dev2	10.0.1.2	vul1	3	TCP	Remote Exploit
3	dev3	10.0.1.3	vul3	3	TCP	Remote Exploit
4	dev4	10.0.2.4	vul4	2	UDP	Remote Exploit
5	dev4	10.0.2.4	vul3	10	TCP	Remote Exploit
6	dev5	10.0.2.5	vul5	5	TCP	Remote Exploit
7	dev6	10.0.2.6	vul6	6	TCP	Remote Exploit
8	dev7	10.0.2.7	vul7	-	-	Local Exploit

ATTACK GRAPH CONCRETE ASSESSMENT & MITIGATION RECOMMENTATIONS

(1) Evaluated security control within the network:	(2) Inherent risk:
Access Controls, Remote Access	VERY HIGH
Application Security (incl. SDLC)	HIGH
Firmware Integrity Controls	VERY HIGH
Network Security	HIGH

(3) Risk reduction process:



(4) GOAL =
REDUCED RISK

FORWARD LOOKING DEFENSE APPROACH

Key Goals: Production & Machine Resiliency

Supported by Secure Engineering & Automation

OTORIO

Industrial cyber risk management solutions

STAY SAFE & SECURE

Shiran Kleiderman

OTORIO | Industrial Cybersecurity

+972-505454123

shiran.kleiderman@otorio.com

www.otorio.com