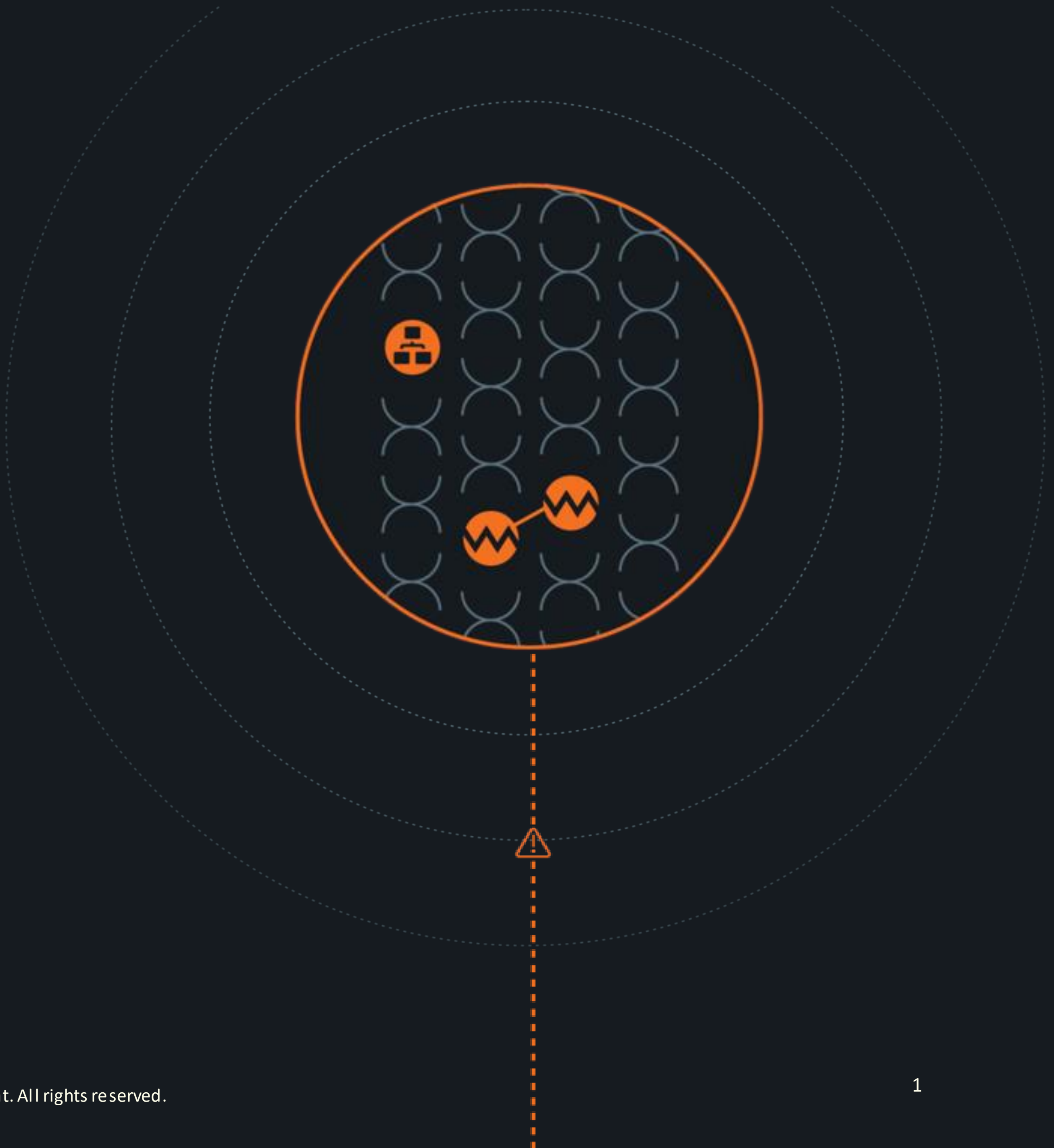
EXALENS®

Cybersecurity in the Plant



Speaker

Dr Ryan Heartfield

Exalens

CTO / Chief Scientist, Co-Founder

Background

>10 years in the cybersecurity industry across Government, private sector and academia.

Primary focus:

- Network security
- AI-assisted threat / anomaly detection for Cyber-Physical systems
- Human-centric cyber defence.

Agenda

- Cyber attacks Vs. Cyber faults and their impact in the connected factory (and why you should care).
- Upcycling physical process monitoring for cybersecurity to see the "bigger picture"
- How "Virtual Analyst" technology can force-multiply your IT and OT teams and enable them to work better together to reduce downtime.

Toward
Smart Factories

Industry 3.0

Replacement of various manual labour with digital production system e.g., robotics, PLC line automation.

Industry "3.5"

Some level of data-driven insights, predictive analytics, sensor fusion, line automation, etc (most manufacturing companies are somewhere here).

Industry 4.0

AI-driven predictive maintenance, self-healing, automated process optimisation and improvement

The Problem

Increased Connectivity

Opens the factory up to the "outside world" (enterprise IT systems, Cloud services, remote access, etc.)

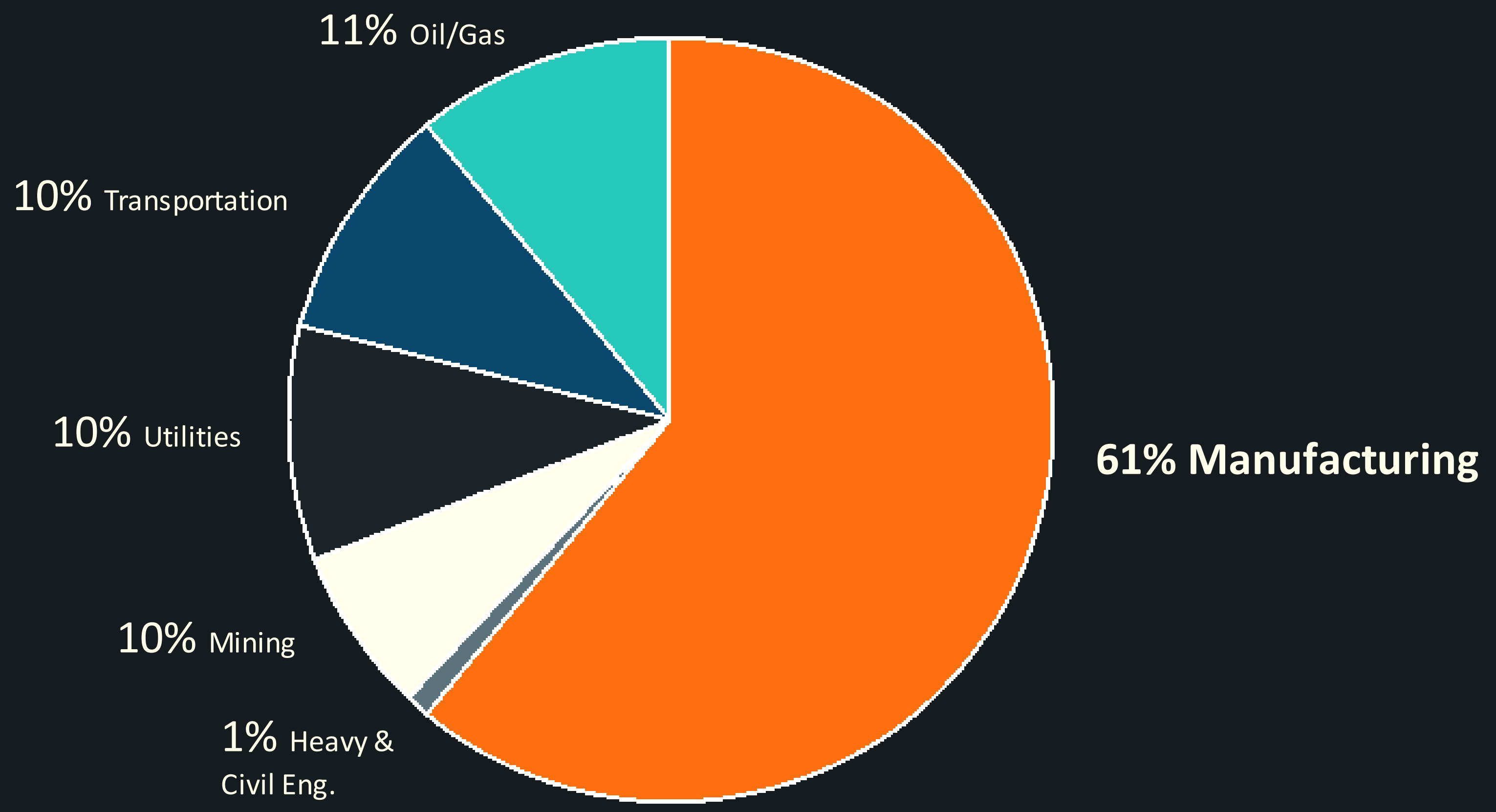
Greater Automation

Increases the risk of cascading failure, impact and safety incidents

Insecure-by-design

Operational systems lack cybersecurity, are often inherently vulnerable to compromise, and are the gooey centre of a "hard-shell" that is no longer a feasible way of working.

In 2021, out of 64 incidents reported, 22 were cyber-attacks with physical impact in the manufacturing industry - a 144% increase from 2020.



EXALENS®

Sources:
https://icsstrive.com
IBM X-Force

The Manufacturing Industry is heading into a ‘perfect storm’, where impact is Cyber-Physical

JAN

Production Shutdown

Palfinger

Westrock

FEB

Production Shutdown

Beneteau SA

MARCH

Production Shutdown

AmsteepFlash

APRIL

Production Disruption

Bakker Logistiek

MAY

Production Shutdown

Molson Coors

Siera Wireless

Production Disruption

Ardagh Group

SEP

Production Shutdown

Crystal Valley Cooperative

OCT

Production Shutdown

Schreiber Food

Ferrar

NOV

Production Shutdown

Damm Brewery

Madix

DEC

Production Shutdown

Amedia

Nortura

Source:
https://icsstrive.com

The Reality from the shop floor...

$336k

Avg. cost of unplanned downtime per/hr

#1

Ranked industry for cyber crime

2 weeks

Of production was lost on average

Sources:
IBM, 2022. X-Force Threat Intelligence Index.
Deloitte and Mapi, 2016. Cyber Risk in Advanced Manufacturing.
Sophos, 2021, State of Ransomware Manufacturing Production
Exalens, 2021, Manufacturing Industry Survey on I4.0 & Cybersecurity

The first step to cybersecurity in the plant requires a cultural mindset and alignment from the organization and teams on strategies and measures.

Myth Busters

There's no way to 100% prevent cyberattacks, but you can protect yourself from their effects...

Company size / Sector
We are too small to be targeted, our data has no value to cyber criminals (cyber criminals are indiscriminate)

Airgaps
Our systems are air-gapped so we are secure from threats (there's no such thing if humans are involved)

Prevention Controls
We use a firewall, and antivirus software to lockdown systems (controls alone will not stop 100% of attacks)

Backups
We have backups of our critical data (do you, have you tested them?!)

Insurance
We have cyber insurance in case we are compromised (will they pay out after validating your cybersecurity measures?)

So how should you address cyber security in the plant? First reduce risk with the fundamentals

Asset Management

Identity & Access Management

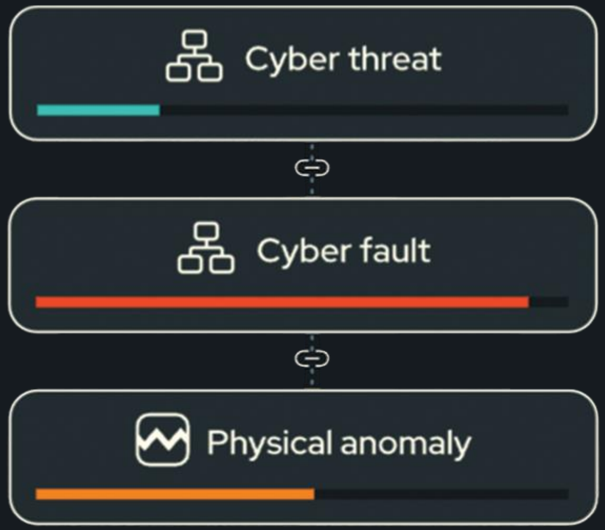
Data Security

Incident management

Sources:
https://www.ncsc.gov.uk/files/2021-10-steps-to-cyber-security-infographic.pdf

Resilience and preparedness is the key objective when it comes to cybersecurity in modern manufacturing environments, and this is where logging and monitoring is critical.

Like all things (safety included) there
is no way to prevent
100% of cyber risk



Cyber threat

Cyber fault

Physical anomaly

... but you can protect yourself from their effects

... and this relies on the ability to "see" and spot high risk activity

Cyber-Physical visibility is the “Missing Link” between IT & Production monitoring. Today, there is...

Lack of unified visibility across IT and Production systems

IT and Production teams cannot see or know when disruption is caused by attacks, faults, or equipment failures, and vice versa.

Slow incident response times & decision making between isolated IT & Production teams

… Cybersecurity is more than stopping attacks

Safety

Operational systems are secured and managed by appropriate controls that protect the production process and its human operators.

Reliability

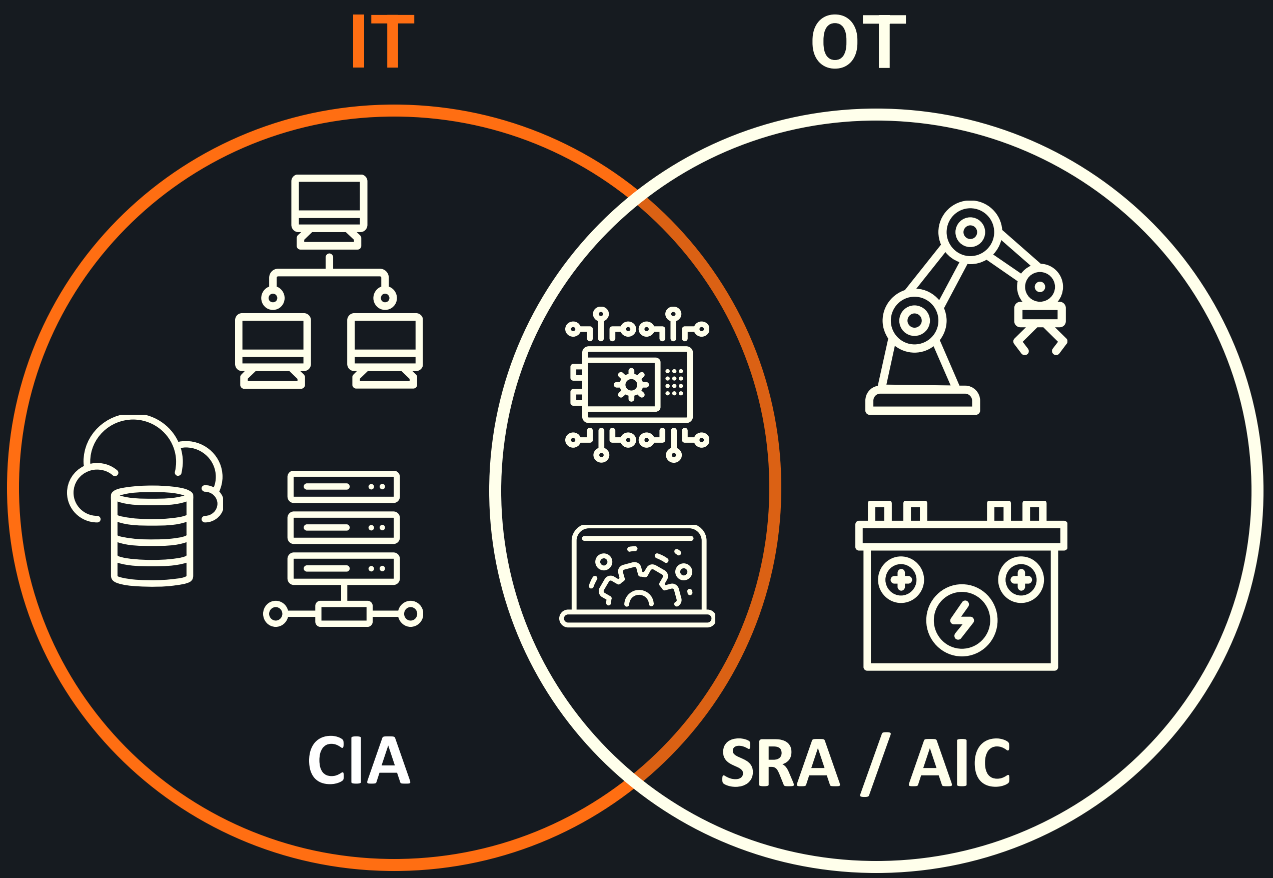
Systems function as intended, and produce consistent quality and output from start to finish of production process

Availability

Systems is highly available for dependent processes, and resilient to failures.

The Intersection of Connected Factories is Cyber-Physical, and it's growing...

Data and the Flow of Digital Information



Operation of physical processes and the machine used to carry them out

Cyber Attacks Vs Cyber Faults

Can you tell the difference?

Root Cause

May appear similar, but is different

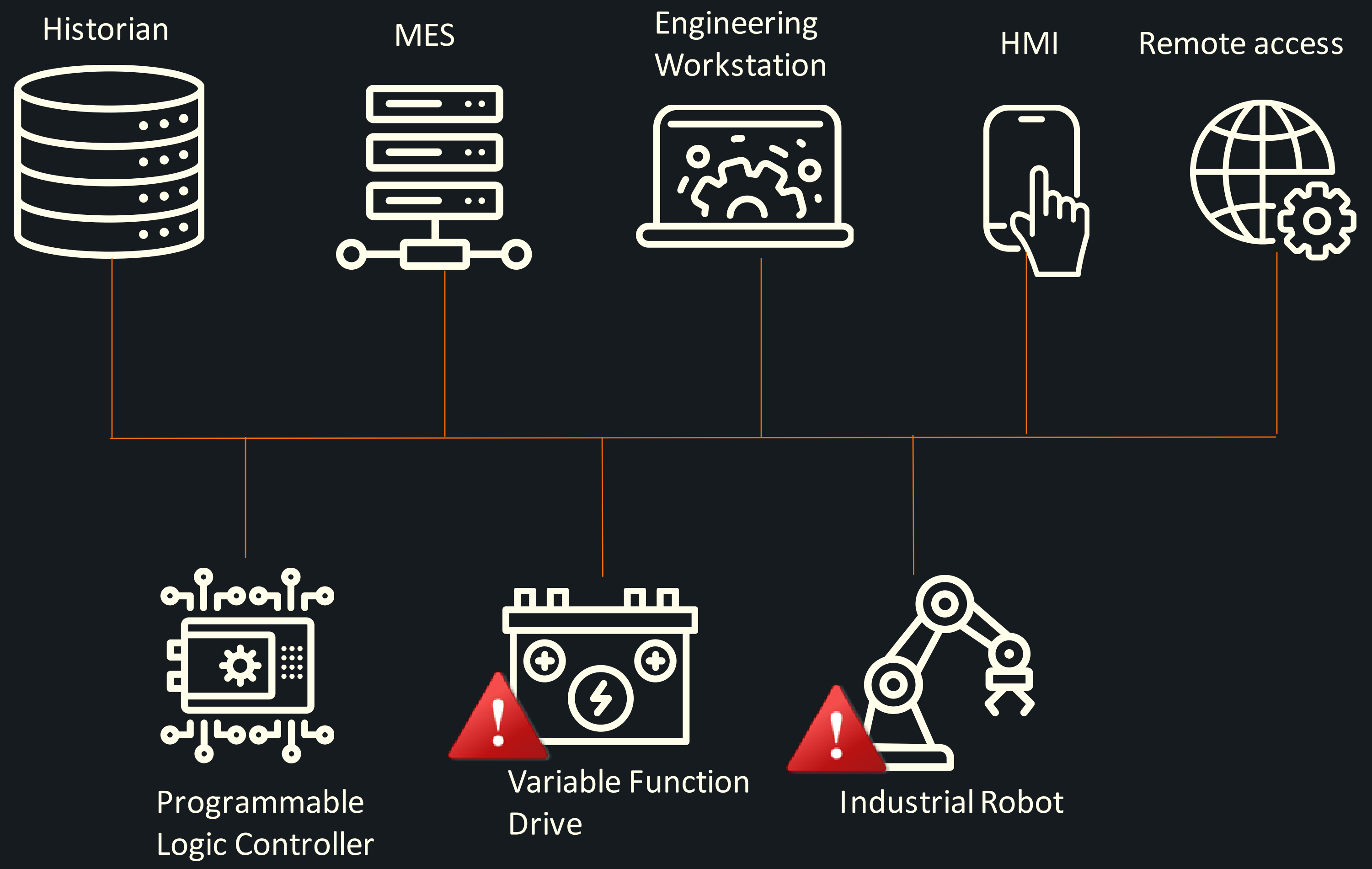
Impact

Can be the same on production operations.

Response

Should be tailored to the root cause...

ACME Food and Drink



Historian

MES

Engineering Workstation

HMI

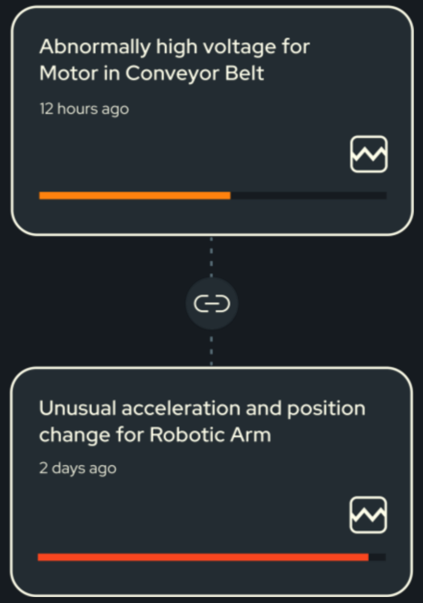
Remote access

Programmable Logic Controller

Variable Function Drive

Industrial Robot

Monitoring Alerts



Abnormally high voltage for Motor in Conveyor Belt

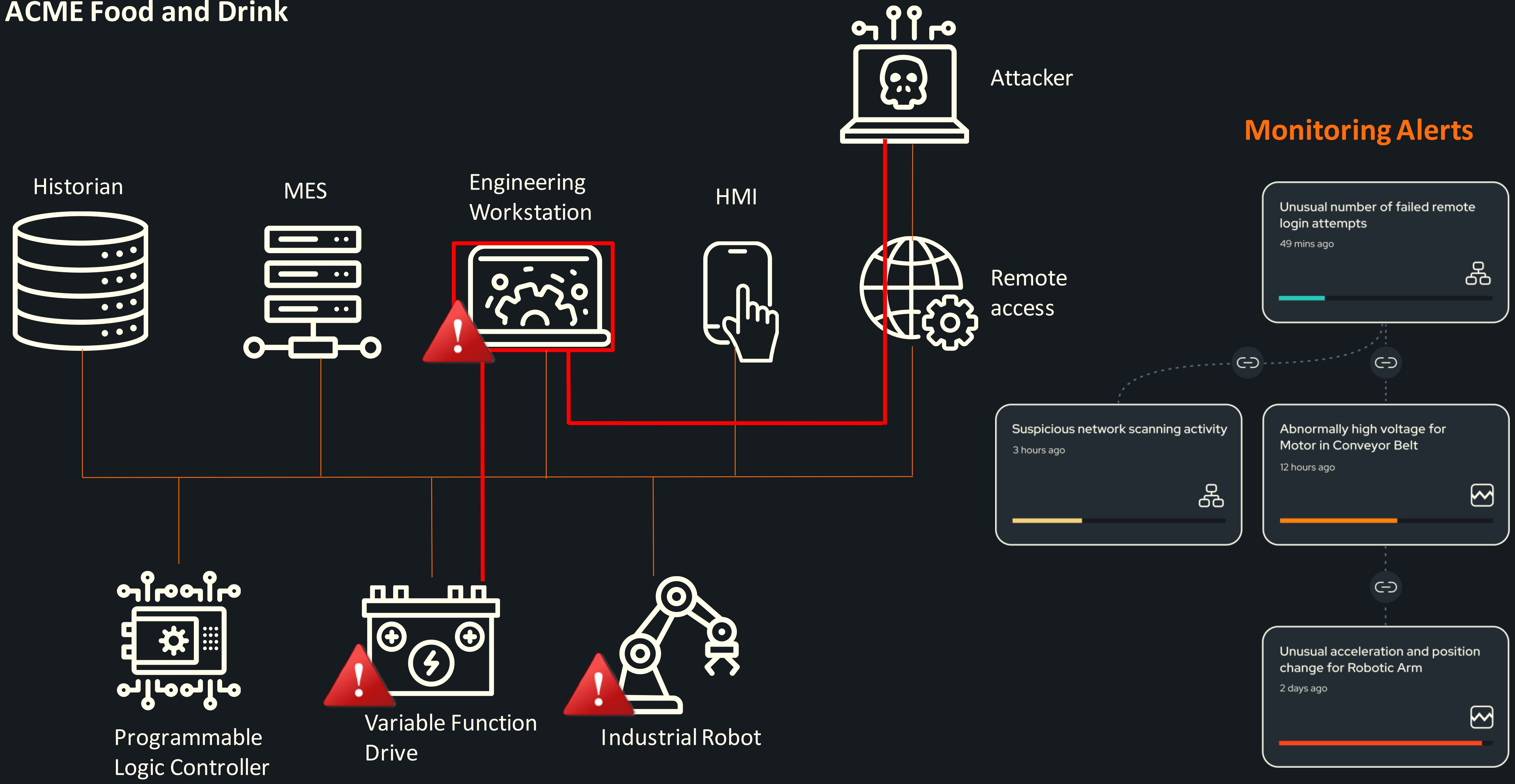
12 hours ago

Unusual acceleration and position change for Robotic Arm

2 days ago

EXALENS®

ACME Food and Drink



Monitoring Alerts

Unusual number of failed remote login attempts
49 mins ago

Suspicious network scanning activity
3 hours ago

Abnormally high voltage for Motor in Conveyor Belt
12 hours ago

Unusual acceleration and position change for Robotic Arm
2 days ago

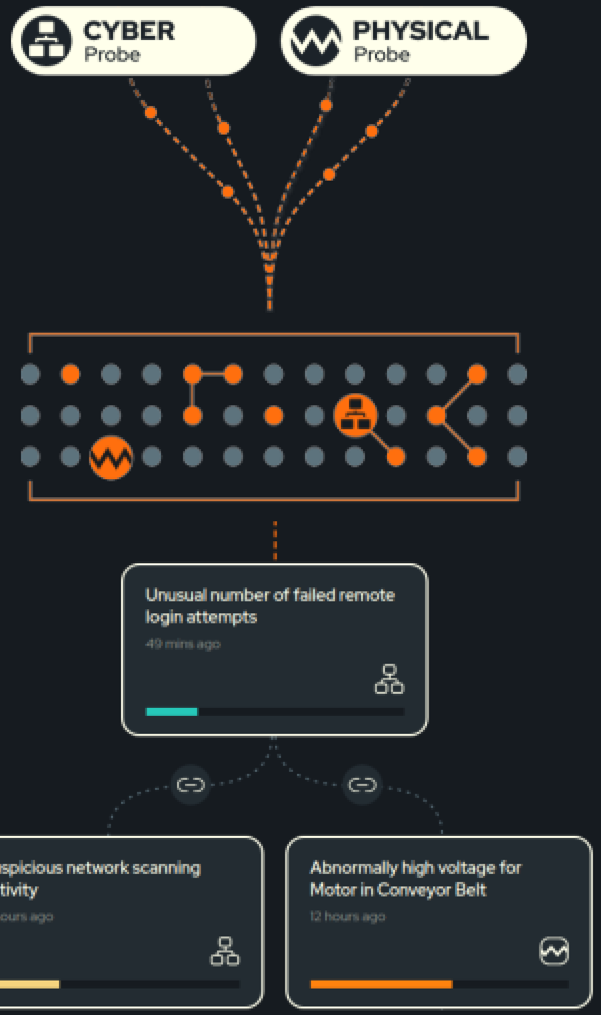
EXALENS®

So, if we are connecting IT and OT – why are we not combining how we monitor their behaviour and interactions?

EXALENS®

This is exactly where upcycling of production data becomes a key part of the solution

Empower IT and Production teams to respond effectively together



Unusual number of failed remote login attempts

49 mins ago

Suspicious network scanning activity

3 hours ago

Abnormally high voltage for Motor in Conveyor Belt

12 hours ago

Know when production is disrupted by cybersecurity related incidents

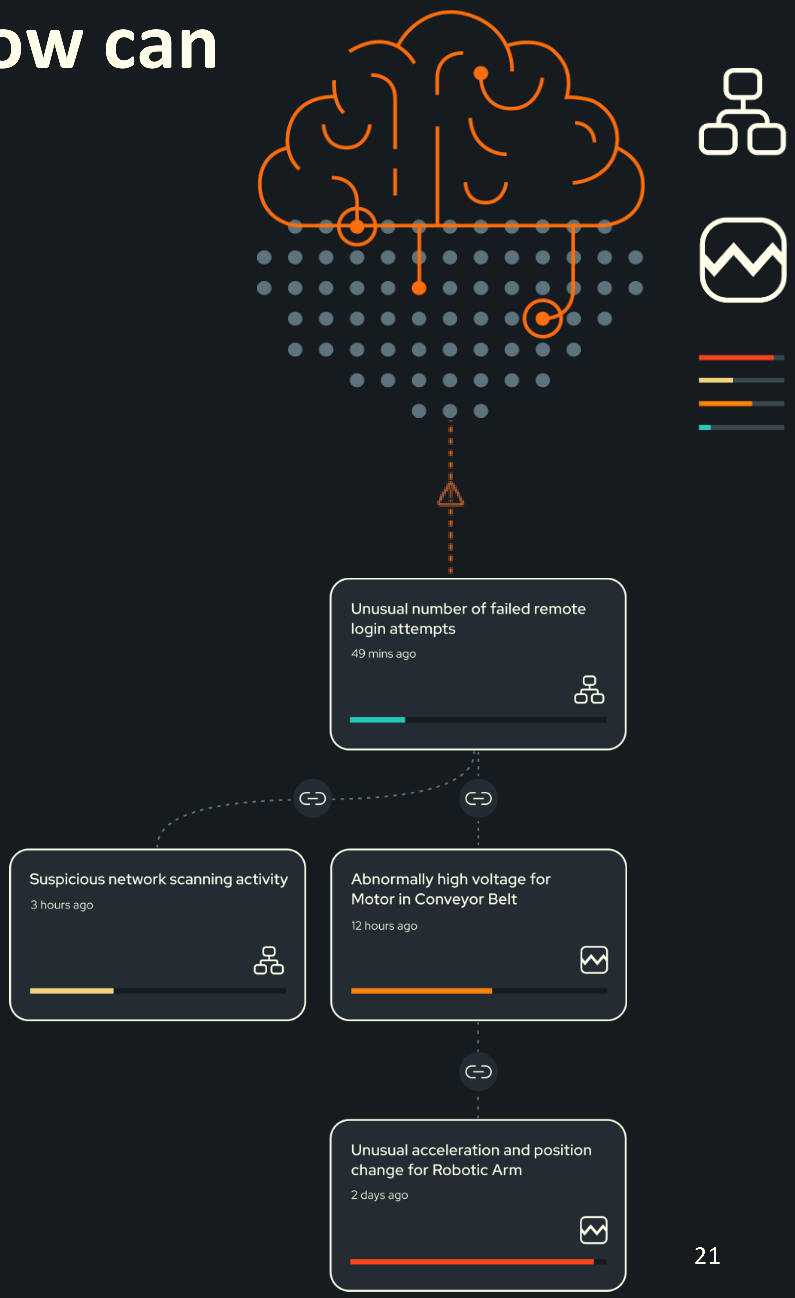
EXALENS®

So, where do "Virtual Analysts" come in and how can they help with resilience?

The next step forward for manufacturers building resilience to cyber attacks and faults requires scalable solutions that leverage Virtual Analyst technology with **Cyber-Physical AI**

- Automating the analysis of cyber and physical system activity to detect, correlate and classify incidents in seconds. Without needing to increase inhouse workforce.

- Reducing burden on existing teams, improving cyber-physical visibility, and speeding up response time to incidents, which increases resilience and reduces downtime.



Unusual number of failed remote login attempts

49 mins ago

Suspicious network scanning activity

3 hours ago

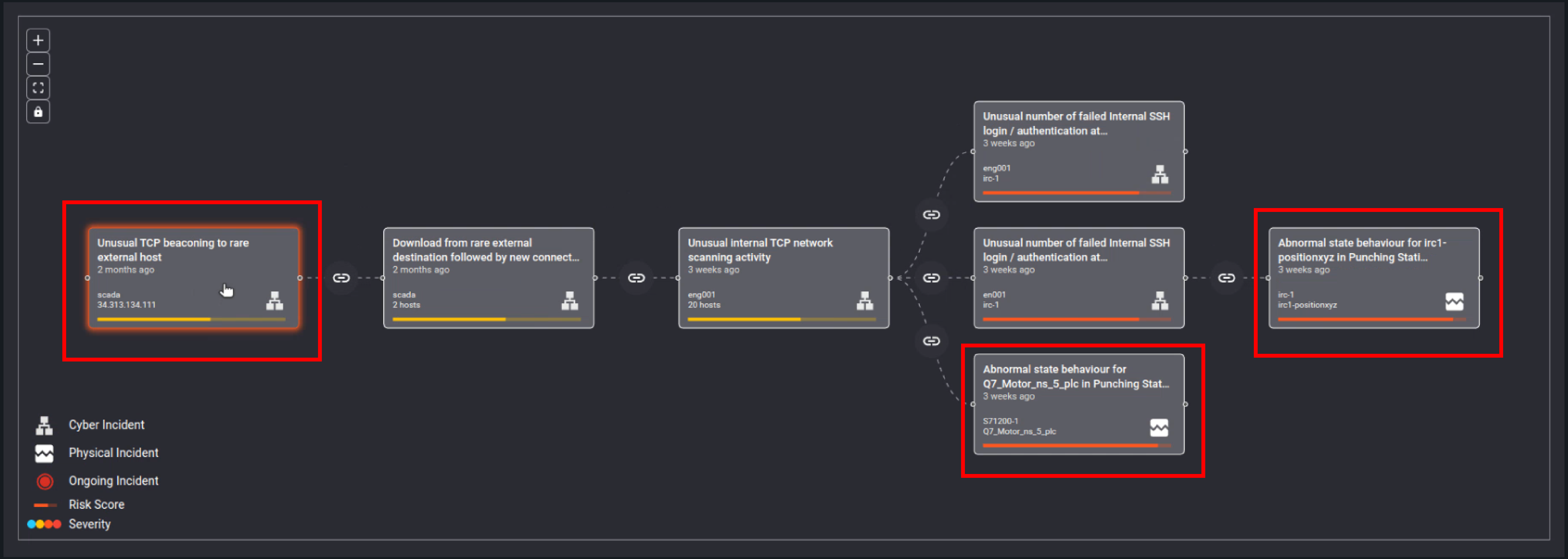
Abnormally high voltage for Motor in Conveyor Belt

12 hours ago

Unusual acceleration and position change for Robotic Arm

2 days ago

A Virtual Analyst automates the answers to: What, When, Where, How and Why. Helping to avoid impact, prevent downtime and optimise operations.



Unusual TCP beaconing to rare external host
2 months ago
scada
34.313.134.111

Download from rare external destination followed by new connect...
2 months ago
scada
2 hosts

Unusual internal TCP network scanning activity
3 weeks ago
eng001
20 hosts

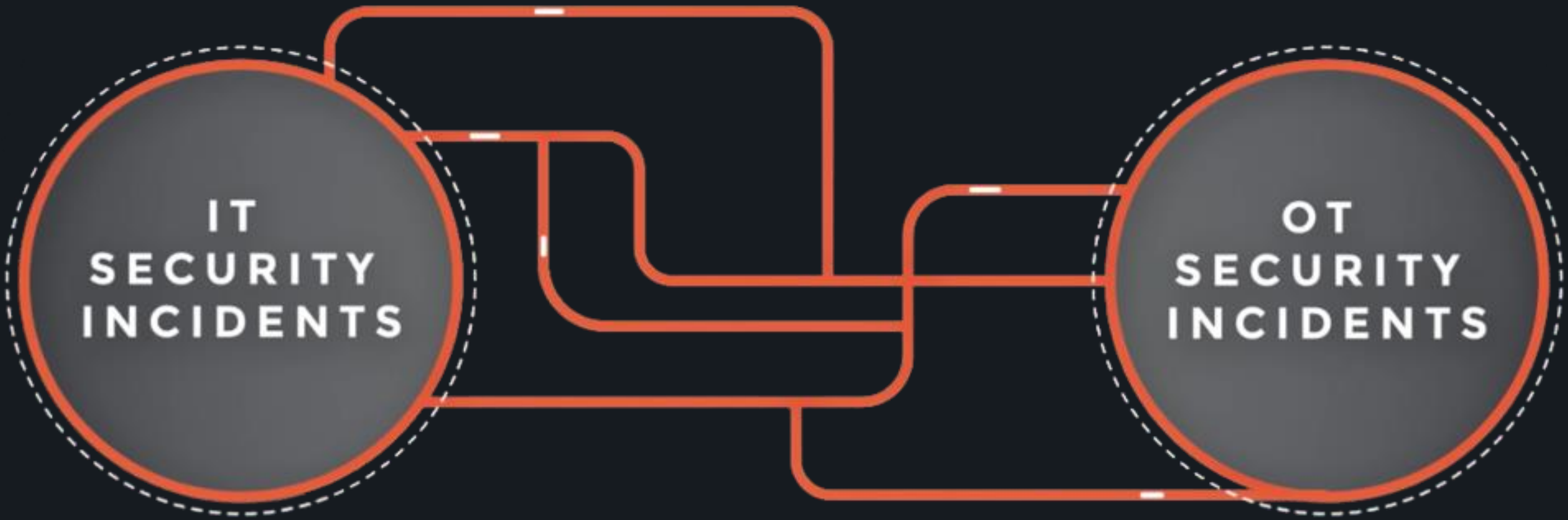
Unusual number of failed Internal SSH login / authentication at...
3 weeks ago
eng001
irc-1

Unusual number of failed Internal SSH login / authentication at...
3 weeks ago
en001
irc-1

Abnormal state behaviour for Q7_Motor_ns_5_plc in Punching Stat...
3 weeks ago
S71200-1
Q7_Motor_ns_5_plc

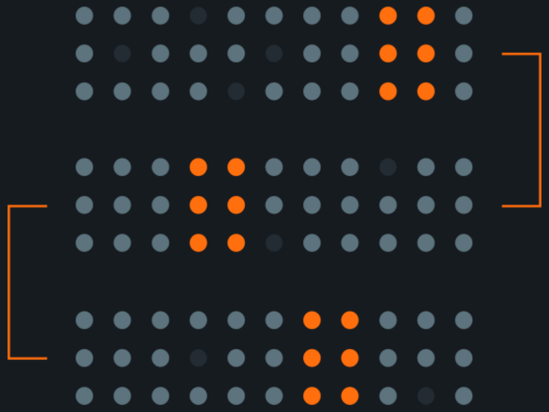
Abnormal state behaviour for irc1-positionxyz in Punching Stati...
3 weeks ago
irc-1
irc1-positionxyz

Empowering both IT and Production to swiftly pinpoint risks, speeding up response, saving precious time and money. Because it notifies both IT and Production teams with the information they need to efficiently and effectively respond.



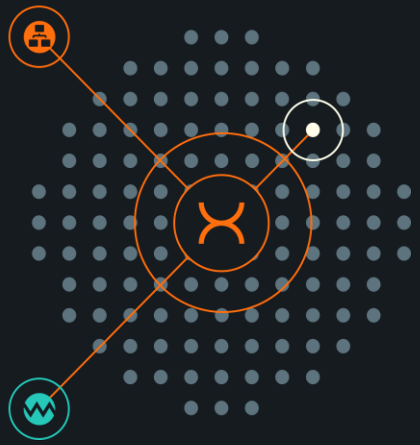
In the Connected Factory, Cybersecurity IS Safety

You **CANNOT** protect what you cannot see



You **NEED** to know the difference between threats and faults

You **MUST** have an incident response plan (think safety)



With greater connectivity and automation, cyber-physical system monitoring is an essential part of safety in manufacturing

Production Monitoring

It's the "CCTV" of cyber and physical system activity, and there to spot risk when things go wrong

Attacks vs faults

Can have the same impact on production operations, but how you respond is different

Cybersecurity IS Safety

In the connected-factor, risks to IT are risk to production process. Virtual analyst technology can help you spot and response in seconds to threats.

EXALENS®

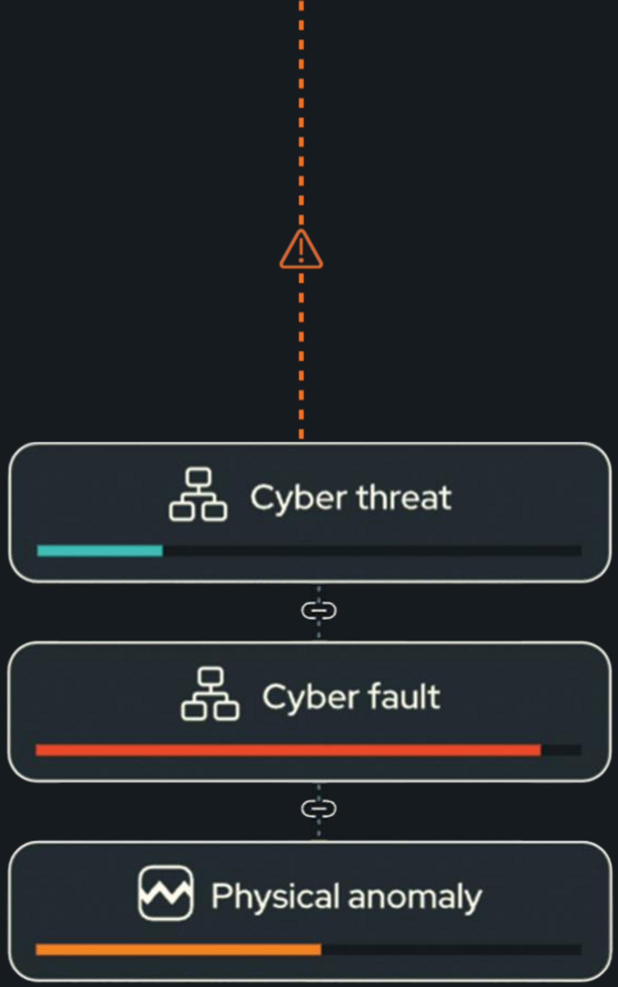
Thank you... Questions?

Gain Cyber-Physical Resilience

Phone: +44 (0) 20 8152 4467

Email: ryan.heartfield@exalens.com

Web: exalens.com



Cyber threat

Cyber fault

Physical anomaly