cyllium

LEAD YOUR BUSINESS PROTECTED

Asociácia priemyselných zväzov a dopravy – seminár KB

Kybernetická bezpečnosť
– seminár, 16.9.2024

00/

Skupina CYLLIUM

Kto sme a čo robíme

Skupina Cyllium

- poskytuje komplexné služby v oblasti informačnej a kybernetickej bezpečnosti na Slovensku i v zahraničí.
- vykonáva auditné, expertné a technologické služby pod vedením profesionálov s medzinárodnými skúsenosťami a certifikáciami.
- náš tím má dlhoročné skúsenosti v oblasti IT auditu, IT bezpečnosti, riadenia informačných a kybernetických rizík pre oblasti IT a OT a poradenstva v oblasti IT a kyberbezpečnosti.

Členmi skupiny sú spoločnosti:

- auditori.it, s. r. o.
- Cyllium SK, s. r. o.
- Cyllium IT, s. r. o.

LEAD
YOUR
BUSINESS
PROTECTED

Naše služby

> Auditné služby

- > Audit KB podľa ZoKB
- > Interný a externý audit alebo GAP analýza voči medzinárodným normám / štandardom (ISO, PCI-DSS, SWIFT, eIDAS, ENSTO-e) / ZoKB
- > Posúdenie IT prostredia pre účely štatutárneho auditu (ITGC)

> Expertné služby

- > Analýza bezpečnostnej architektúry v organizácii a aktívne overenie a testovanie bezpečnosti organizácie
- > Analýza rizík v organizácii, biznis dopadov, kritickosti procesov a aktív a ich väzby,
- > Návrh bezpečnostných opatrení v organizácii, vrátane analýzy možností technologických riešení a bezpečnostných nástrojov na trhu
- > Poskytovanie bezpečnostných rolí Riadenie projektu a plánovanie projektových prác
- > Školenie zamestnancov a dodávateľov

> Technologické služby

- > Návrh, realizácia, správa a prevádzka lokálnej, serverovej, virtualizačnej, cloudovej alebo hybridnej infraštruktúry
- > Návrh, realizácia, správa a prevádzka adresárových služieb a infraštruktúry verejných kľúčov
- > Migrácia a konsolidácia prevádzkových infraštruktúr
- > Bezpečnostná konfigurácia (Security hardening)
- > Zabezpečenie koncových staníc

LEAD
YOUR
BUSINESS
PROTECTED

Naše certifikáty

Certified Internal Auditor

Certified Data Privacy Solutions Engineer

Certified Information Systems Auditor

Certified Information Security Manager

PRINCE2 Foundation

ISA/IEC 62443 Cybersecurity Fundamentals Specialist

ISA/IEC 62443 Cybersecurity Risk Assessment Specialist

ISA/IEC 62443 Cybersecurity Design Specialist

ISA/IEC 62443 Cybersecurity Maintenance Specialist

ISA/IEC 62443 Cybersecurity Expert

Certified Information Systems Security Professional

Microsoft Certified System Engineer

Certified Ethical Hacker

The Global Industrial Cyber Security Professional

LEAD
YOUR
BUSINESS
PROTECTED

Naše referencie

Centrálny depozitár cenných papierov SR

DFNKE
DETSKÁ FAKULTNÁ
NEMOCNICA KOŠICE

GGE

BURZA CENNÝCH PAPIEROV V BRATISLAVE

DIGI
SLOVAKIA

AGEL SK

MINISTERSTVO
ZDRAVOTNÍCTVA
SLOVENSKEJ REPUBLIKY

NÁRODNÝ
INŠPEKTORÁT
PRÁCE

ÚGKK SR

MARTIN

MINISTERSTVO
ZAHRANIČNÝCH VECÍ
A EURÓPSKYCH ZÁLEŽITOSTÍ
SLOVENSKEJ REPUBLIKY

SEPS
Slovenská
elektrizačná
prenosová
sústava

NÁRODNÉ LESNÍCKE CENTRUM
NATIONAL FOREST CENTRE

SLOVENSKÁ
BANKOVÁ
ASOCIÁCIA

MINISTERSTVO
FINANCIÍ
SLOVENSKEJ REPUBLIKY

SPRÁVA ŠTÁTNYCH
HMOTNÝCH REZERV
SLOVENSKEJ REPUBLIKY

STUPAVA

NAJVYŠŠÍ SÚD
SLOVENSKEJ REPUBLIKY

SLOVENSKÁ ZÁRUČNÁ
A ROZVOJOVÁ BANKA

tasr

NAJVYŠŠÍ
SPRÁVNY SÚD
SLOVENSKEJ REPUBLIKY

ŠTÁTNY VETERINÁRNY A POTRAVINOVÝ ÚSTAV

Webglob

websupport

LEAD
YOUR
BUSINESS
PROTECTED

O čom budeme diskutovať?

01 KB v priemysle

- Rozdiel oproti IT (IT vs. OT)
- Základné princípy KB v priemysle

02 Ako začať?

- Základné kroky ako začať s kybernetickou bezpečnosťou

03 Analýza rizík

- Cieľ
- Ako prebieha

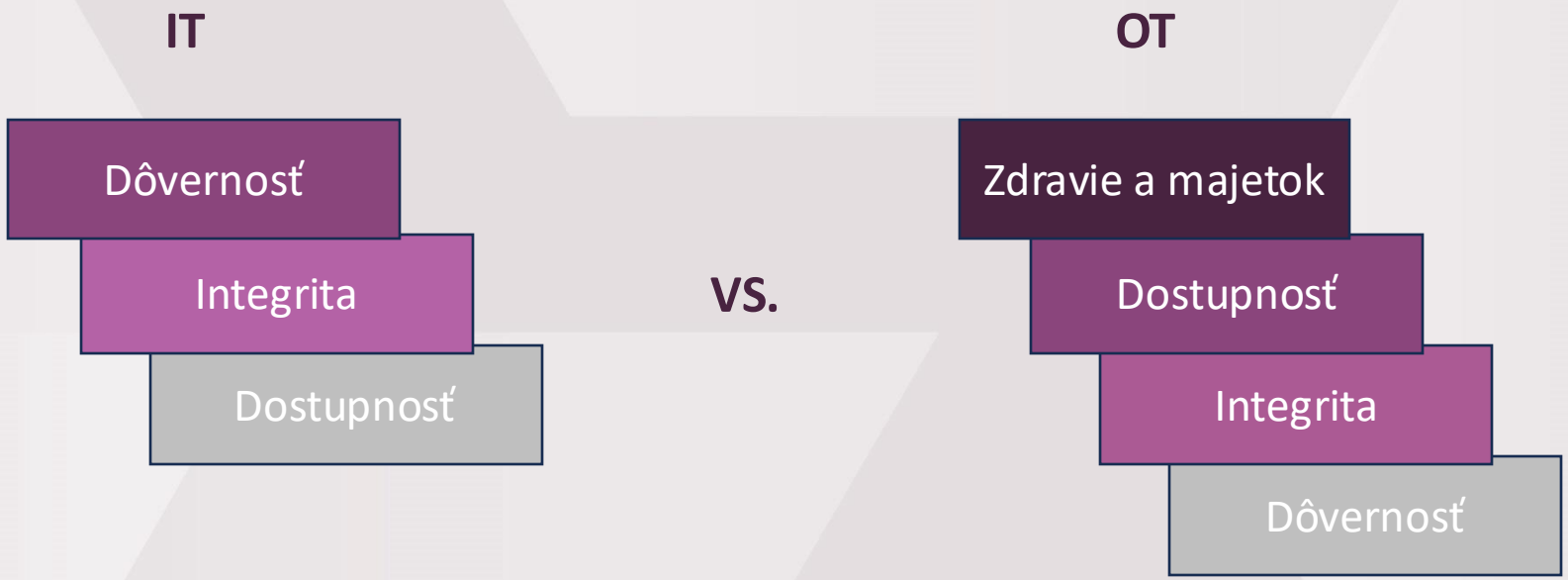
LEAD YOUR BUSINESS PROTECTED

01/ Kybernetická bezpečnosť v priemysle

Rozdiel oproti IT (IT vs. OT)

- OT = prevádzkové technológie (Operations Technology), sú systémy / zariadenia, ktoré interagujú s fyzickým prostredím (alebo riadia zariadenia, ktoré interagujú s fyzickým prostredím).

- Rozdiel medzi OT a IT je v prioritách. Pri IT je priorita dôvernosť a integrita dát. V OT je priorita **ochrana zdravia a majetku, dostupnosť a 24/7 funkčnosť procesov**.

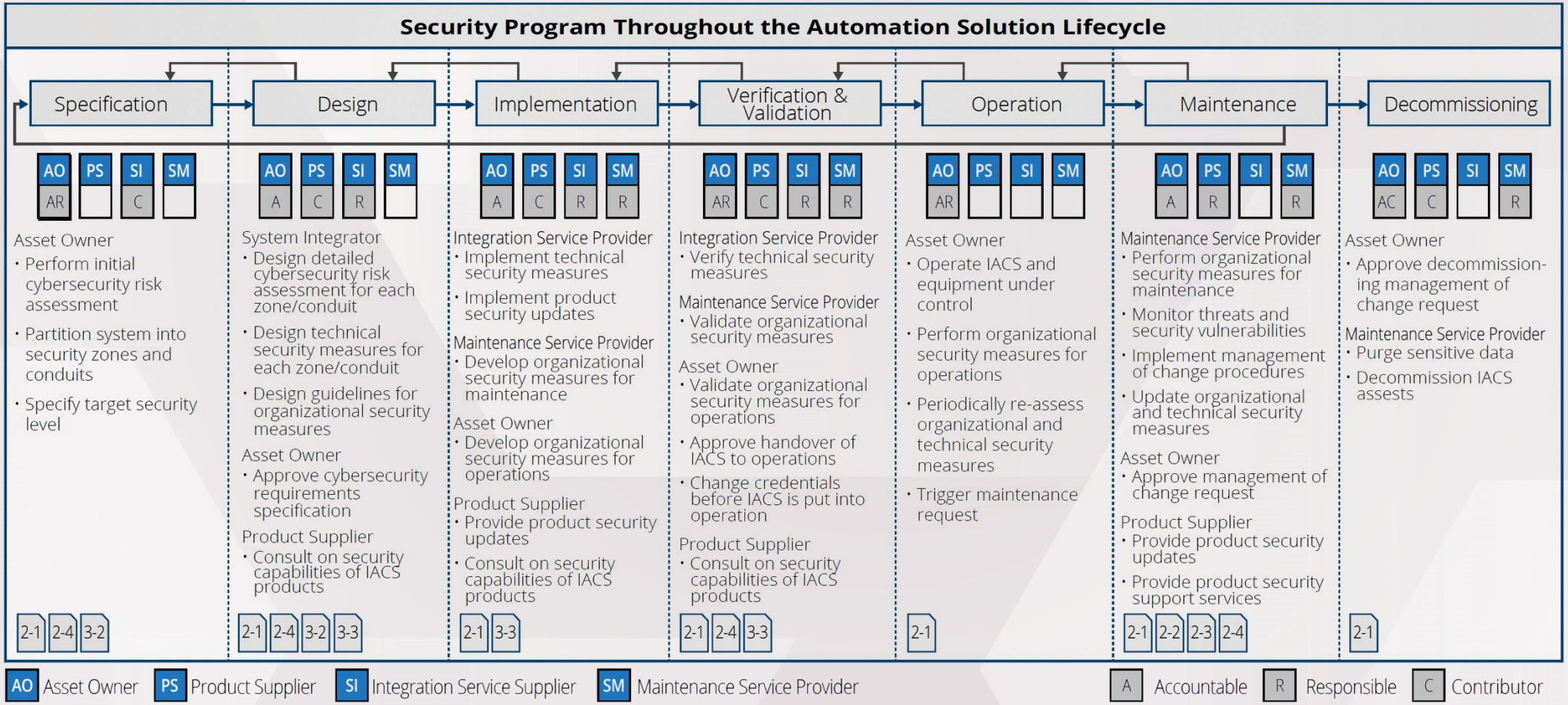


LEAD YOUR BUSINESS PROTECTED

Rozdiel oproti IT (IT vs. OT) II.

	Office IT systémy:	OT systémy (ICS/IACS):
Hlavné procesy:	spracovávanie informácií	riadenie technologických procesov
Charakteristika:	Dynamické systémy	Deterministické systémy
Životný cyklus:	4-6 rokov	**15-20 rokov**
Patch management:	2-3 x roky	1 x rok(1 x 2 roky)
Dostupnosť:	výpadky akceptované	**24/7**
Aktuálne zabezpečenie:	dobré	**nízke / žiadne**
Komunikačné protokoly:	TCP/IP	IEC80750, IEC61850
Koncové zariadenia:	server, PC/NTB, LAN	RTU, SCADA, PLC, DCS, EMS, …

Bezpečnosť je spoločná aktivita



LEAD YOUR BUSINESS PROTECTED

Incidenty v OT

2010
- Stuxnet

2013
- Kompromitácia priehrady v NY

2014
- Ovládnutie dávkovača liekov v nemocnici
- Ovládnutie dopravnej signalizácie v meste

2012
- Útok na vysokú pec v oceliarni (DE)
- Úspešné ovládnutie idúceho auta
- Útok na rozvodnú sieť v UA

2017
- Ransomware odstavil výrobu liekov (strata viac ako $1mld.)
- Ransomware odstavil riadenie lodnej premávky globálnej logistickej spoločnosti

2018
- TRISIS/TRITON: malware špeciálne vytvorených pre riadiace systémy

2019
- Globálny výrobca hliníka odstavil prevádzku kvôli ransowmare
- Výrobca leteckých dielov prerušil prevádzku na niekoľko dní

2020
- Ransomware Ekans zasiahol niekoľko odvetví

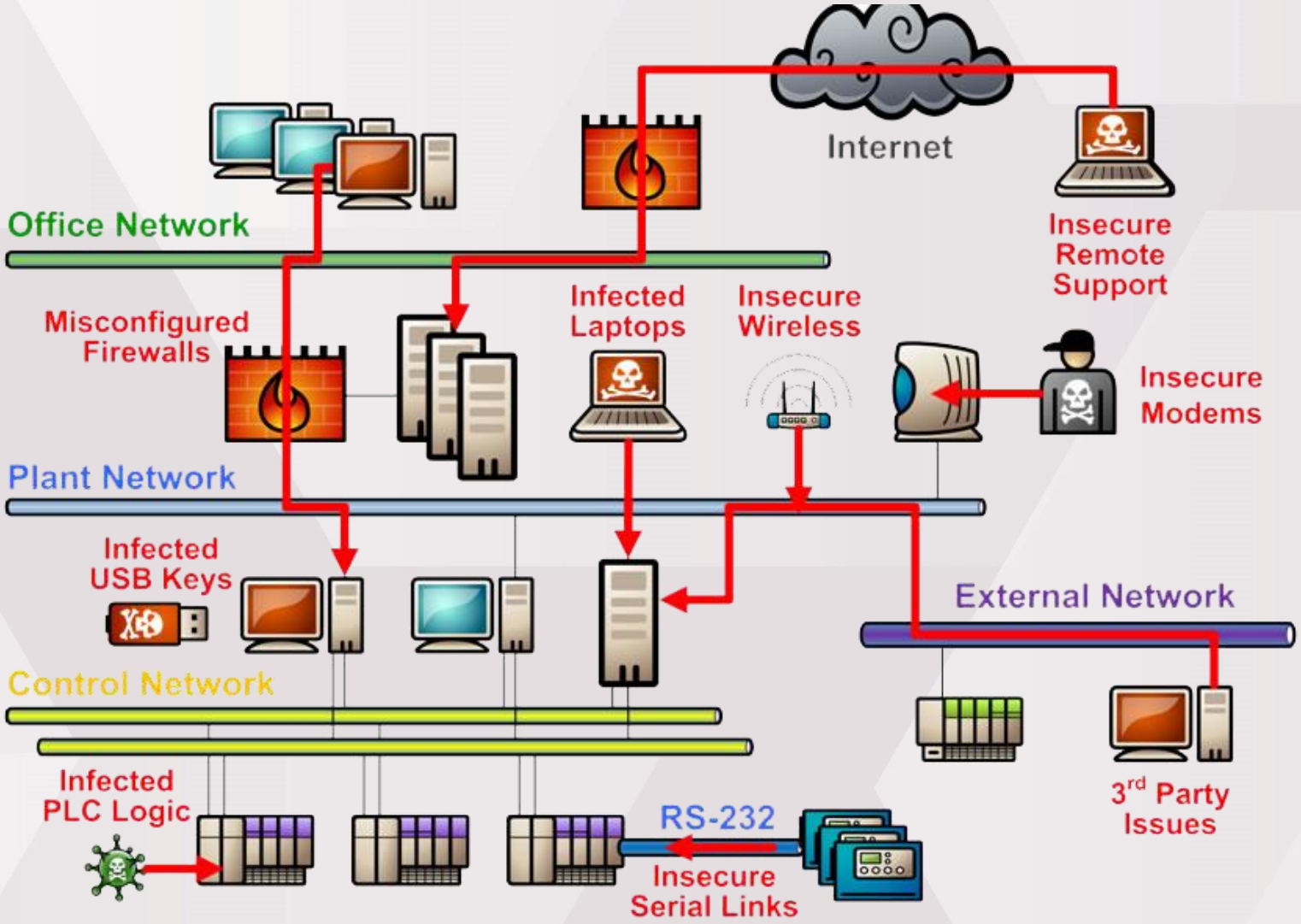
- Solarwinds Orion

2021
- Pokus o otrávenie pitnej vody

- Prerušenie distribúcie ropy v 1/3 USA

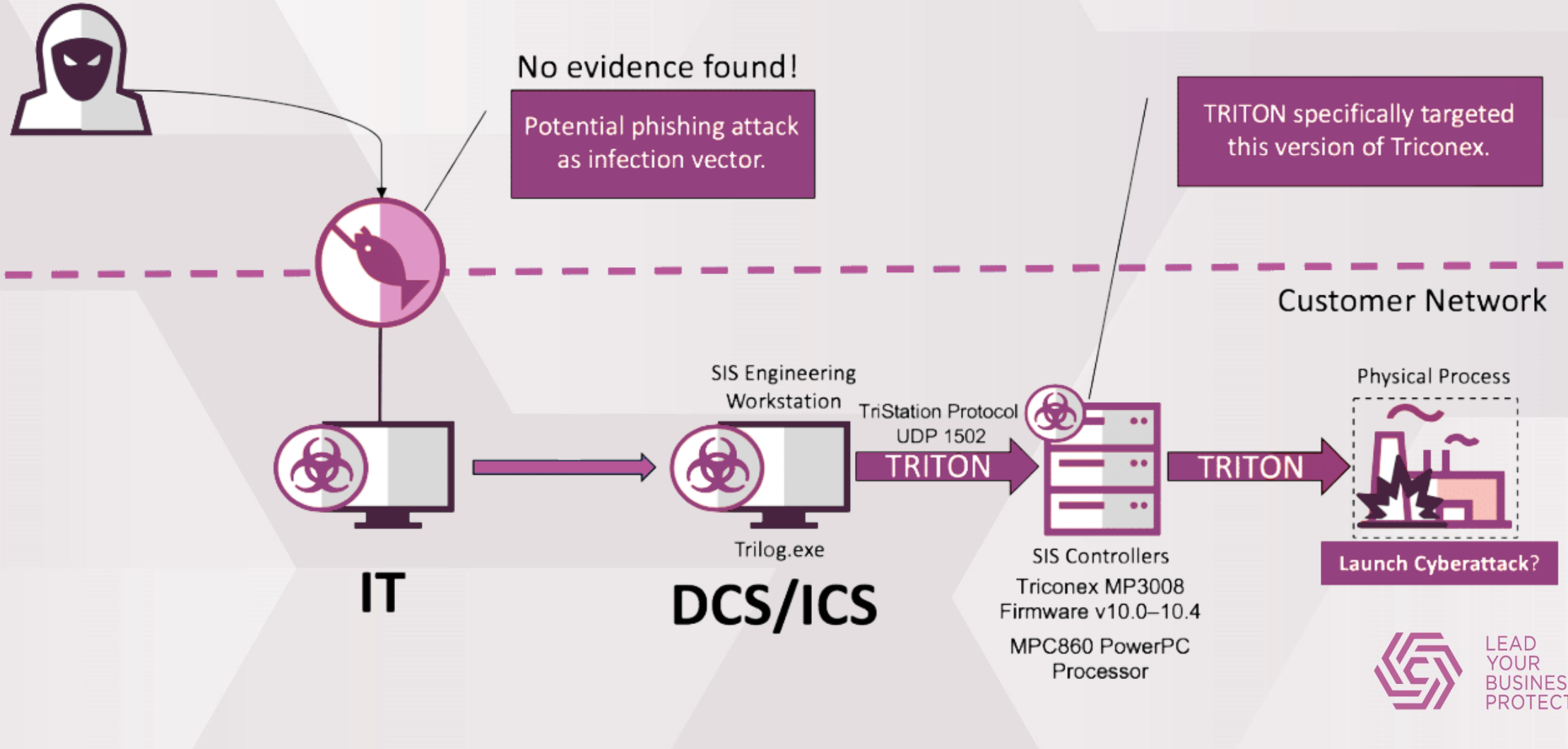
LEAD YOUR BUSINESS PROTECTED

Ako prebiehajú útoky I.



LEAD
YOUR
BUSINESS
PROTECTED

Ako prebiehajú útoky II. - TRITON



LEAD YOUR BUSINESS PROTECTED

02/ Ako začať?

Ako začať?

1.GAP Analýza:

Identifikácia rozdielov medzi súčasným stavom a požadovanými normami alebo cieľovým stavom kybernetickej bezpečnosti.

- Zber informácií o aktuálnom stave, porovnanie so štandardmi a identifikácia nedostatkov.

2.Analýza rizík:

Posúdenie potenciálnych hrozieb a zraniteľností, ktoré môžu ovplyvniť organizáciu.

- Identifikácia rizikových scenárov, hodnotenie pravdepodobnosti a dopadu, stanovenie úrovne rizika.

3.Príprava dokumentácie:

Vytvorenie alebo aktualizácia dokumentov

- Vypracovanie bezpečnostných politík, procedúr, plánov reakcie na incidenty, a ďalších relevantných dokumentov.

Definovanie rolí a zodpovedností

- Určenie kľúčových osôb a tímov, ich rolí, zodpovedností a autorít.

4.Technické opatrenia:

Implementácia technických riešení na ochranu informačných systémov.

- Zavedenie firewallov, antivírusových systémov, šifrovania, monitorovacích systémov, a iných bezpečnostných opatrení.

03/ Analýza rizík

Na čo slúži analýza rizík

- Ochrana obchodných cieľov spoločnosti
- Zvýšenie celkovej bezpečnosti podniku
- Súlad so zákonmi a medzinárodnými štandardmi
- Udržanie dobrej povesti na verejnosti

LEAD
YOUR
BUSINESS
PROTECTED

Zjednodušený proces analýzy rizík

LEAD YOUR BUSINESS PROTECTED

Výzvy pri analýze rizík v OT

- Moderné riadiace a bezpečnostné systémy sú zložité
- Je veľmi bežné, že sú integrované s IT
- Identifikácia kybernetických hrozieb a zraniteľností, ktoré môžu viesť k vysokým rizikovým dôsledkom, môže byť náročná
- Štúdie bezpečnosti procesov (napr. PHA, HAZOP, LOPA) zvyčajne nezohľadňujú udalosti iniciujúce kybernetickú bezpečnosť alebo účinnosť bezpečnostných opatrení kybernetickej bezpečnosti

cyllium

LEAD YOUR BUSINESS PROTECTED

Cyllium SK, s.r.o.
Bottova 2A
811 09 Bratislava
SLOVAKIA

IČO: 55278507

Cyllium IT, s.r.o.
Bottova 2A
811 09 Bratislava
SLOVAKIA

IČO: 56243855

auditori.it, s.r.o.
Bottova 2A
811 09 Bratislava
SLOVAKIA

IČO: 53566114

www.cyllium.eu