Архітектура безпеки об’єктів енергетичної інфраструктури.

Як забезпечити захист та стійкість від кіберзагроз з урахуванням актуальних ризиків та нормативних вимог.

Володимир Ілібман
Cisco Security
CCSP, CISSP

cisco SECURE

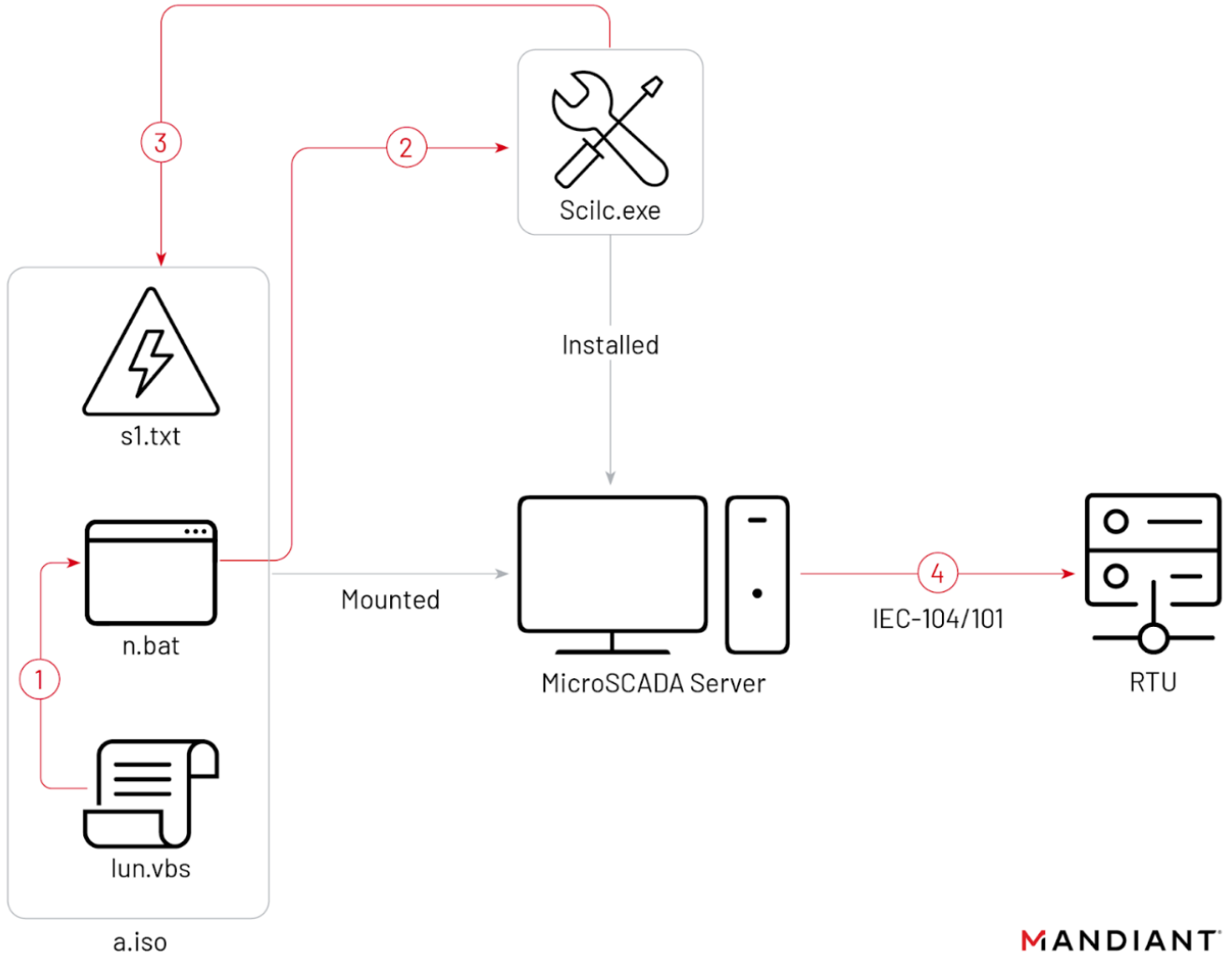
Модернізація енергосистеми та кібер ризики

- Кібератаки з боку рф
- Атаки з боку комерційних хакерських груп
- Цифровізація/Нові технології збільшують площу атаки
- Ризики з боку інсайдерів/ партнерів/контрактників
- Ризики невідповідності нормативним вимогам

- Порушення роботи OT/IT підсистем
- Кібершпіонаж (в тому числі для дорозвідки кінетичних цілей)
- Репутаційні ризики
- Штрафи/відповідальність посадових осіб за невідповідність

Приклад: комбінована атака на об’єкт енергетичної критичної інфраструктури

- **Атака Sandworm**: Втручання в українську критичну інфраструктуру у жовтні 2022 року
- **Тактика**: Використання штатних інструментів, зокрема мови SCIL для MicroSCADA, які далі транслювалися в команди 101 та 104 протоколи для для розмикання автоматичних вимикачів і відключення електроенергії.
- **CADDYWIPER**: Додаткове знищення даних в IT середовищі 12 жовтня.
- **Гібрідні атаки**: Завершальна фаза кібератаки корелюється по часу з початком широкомаштабних ракетних ударів на критичну інфраструктуру.



MANDIANT

Nov, 9 2023 https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

Безпека технологічної мережі є пріоритетом

Відповідність вимогам та правилам

- Загальних вимог до кіберзахисту ОКІ, постанова № 518 КМУ
- Вимоги з кібербезпеки паливно-енергетичного сектору КІ від 15.12.2022
- Адаптація IEC 62443

Державні ініціативи

- MISP UA та MISP UA30 для обміну інформаціє
- Підключення до національних Security Operation Center

Приватні ініціативи

- Співпраця з приватними командами аналітики кіберзагроз (зокрема Cisco TALOS)

Технічні рішення

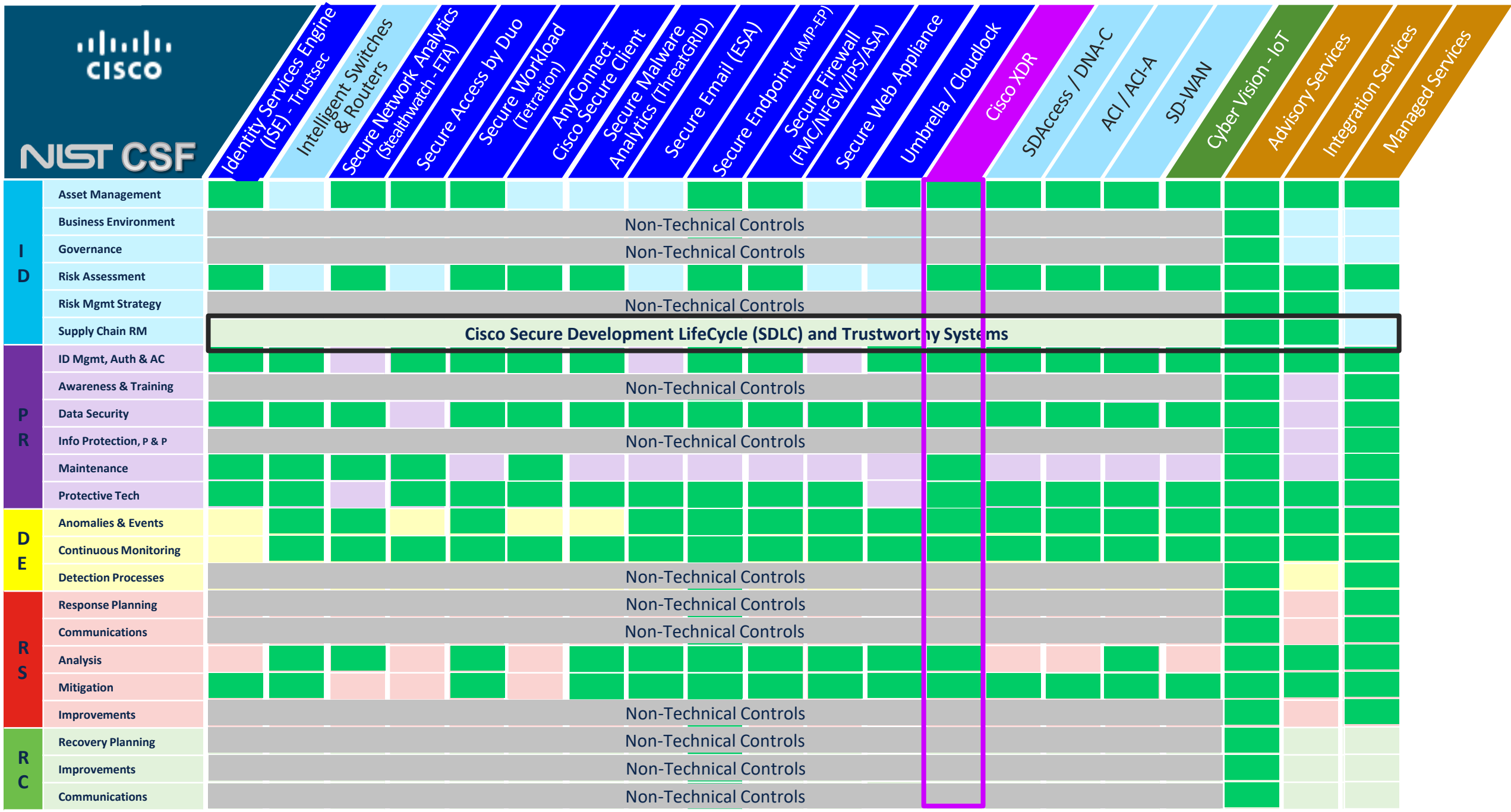
- Обладнання для промислових систем управління (ICS) з підвищеним рівнем безпеки
- Рішення з кібербезпеки для IT та OT
- Архітектура комплексного захисту

Вимоги з кібербезпеки паливно-енергетичного сектору критичної інфраструктури

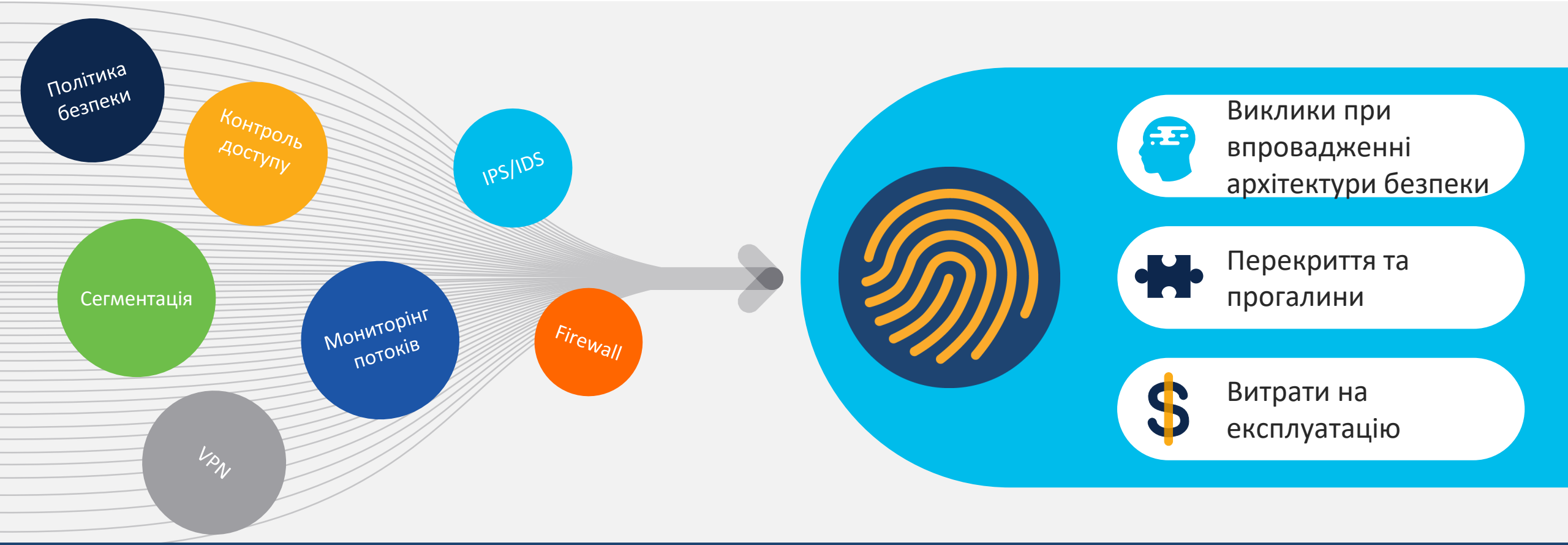
Наказ №417 Міністерства енергетики України від 15 грудня 2022 року

	Категорія	Основні вимоги
ID	**Ідентифікація ризиків**	Розподіл обов'язків для запобігання кіберінцидентам, постійний перегляд тимчасово встановлених привілеїв щодо прав доступу
PR	**Кіберзахист**	Захист цілісності комунікаційної мережі за допомогою поділу і сегментації мережі
DE	**Виявлення кіберінцидентів**	Виявлення аномальної активності, потенційних кіберінцидентів
RS	**Реагування на кіберінциденти**	Заходи, спрямовані на зниження потенційного негативного впливу кіберінцидентів та кібератак
RC	**Відновлення поточного стану кібербезпеки**	Забезпечення спроможностей ОКІІ щодо стійкого надійного та безперервного надання життєво важливих послуг та функцій

NIST National Institute of Standards and Technology


NIST CSF
Identity Services Engine (ISE) - Trustsec
Intelligent Switches & Routers
Secure Network Analytics (Stealthwatch - ETA)
Secure Access by Duo
Secure Workload (Tetration)
AnyConnect Cisco Secure Client
Secure Malware Analytics (ThreatGRID)
Secure Email (ESA)
Secure Endpoint (AMP-EP)
Secure Firewall (FMC/NFGW/IPS/ASA)
Secure Web Appliance
Umbrella / Cloudlock
Cisco XDR
SDAccess / DNA-C
ACI / ACI-A
SD-WAN
Cyber Vision - IoT
Advisory Services
Integration Services
Managed Services
ID
Asset Management
Business Environment
Governance
Risk Assessment
Risk Mgmt Strategy
Supply Chain RM
PR
ID Mgmt, Auth & AC
Awareness & Training
Data Security
Info Protection, P & P
Maintenance
Protective Tech
DE
Anomalies & Events
Continuous Monitoring
Detection Processes
RS
Response Planning
Communications
Analysis
Mitigation
Improvements
RC
Recovery Planning
Improvements
Communications
Non-Technical Controls
Cisco Secure Development LifeCycle (SDLC) and Trustworthy Systems

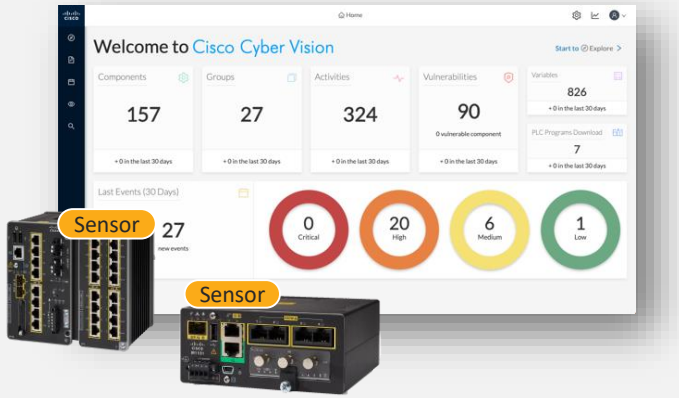
Виклики при впровадженні архітектури безпеки



Складніше, коли маєш справу з точковими продуктами або гетерогенними рішеннями

Фундаментальні компоненти архітектури безпеки Cisco для промислової мережі

Identify & Detect

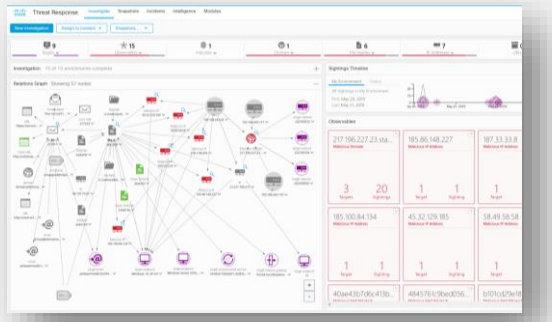


Використовуйте промислову мережу для ідентифікації активів і виявлення спроб втручання в роботу ICS за допомогою **Cyber Vision**

Protect

Запобігайте поширенню шкідливого ПЗ, з найкращими у своєму класі IPS/IDS з підтримкою промислових протоколів **ISA 3000** та EDR **Cisco Secure Endpoint**

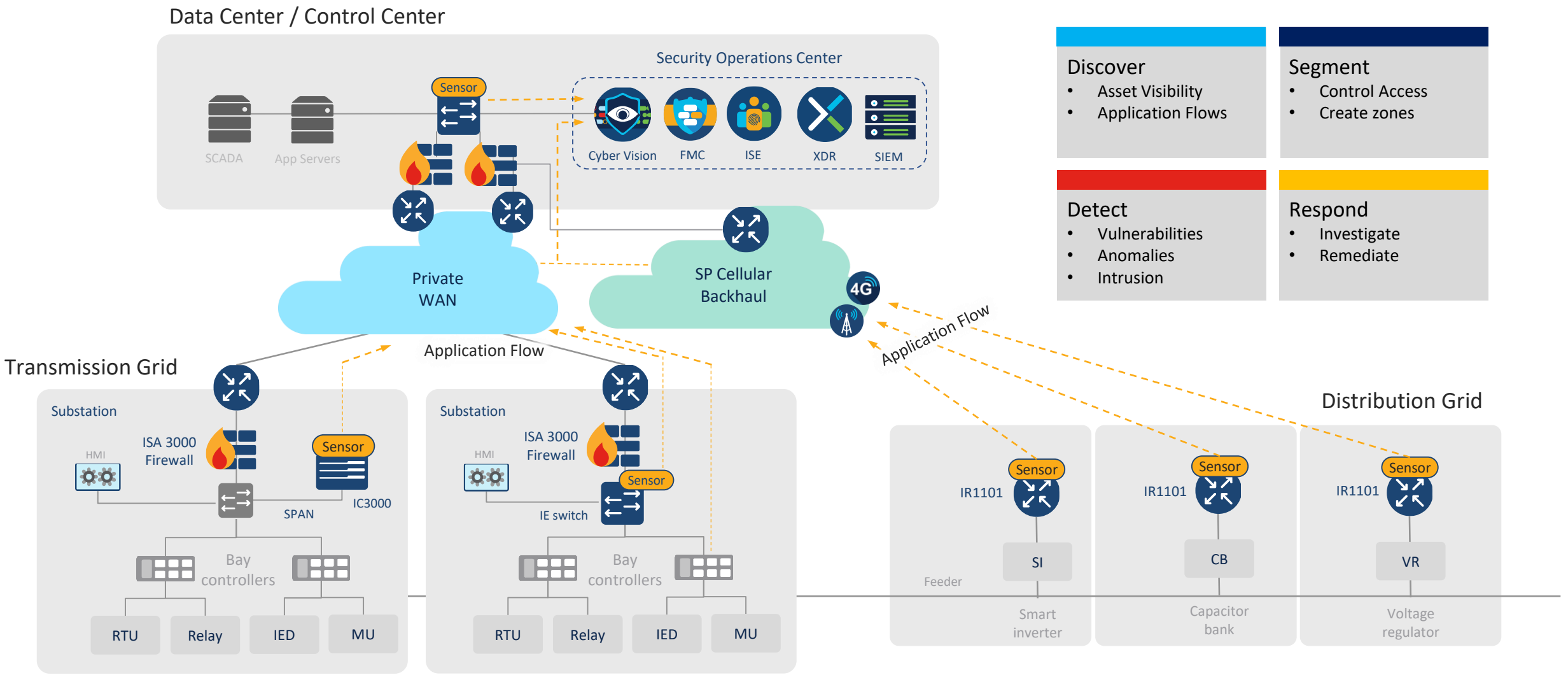
Respond



Дозвольте IT-SOC розслідувати промислові загрози завдяки інтеграції з Cyber Vision, Secure Endpoint та ISA3000 з **Cisco XDR**

Працює на основі аналітики загроз Cisco TALOS

Базова архітектура кібербезпеки в електроенергетиці



Discover
- Asset Visibility
- Application Flows

Segment
- Control Access
- Create zones

Detect
- Vulnerabilities
- Anomalies
- Intrusion

Respond
- Investigate
- Remediate

Cisco IoT

Усунення прогалин в кібербезпеці OT

Робочі процеси між OT та IT

Обмежена видимість активів OT

Потреба в сегментації

Захист від шкідливого ПЗ та атак

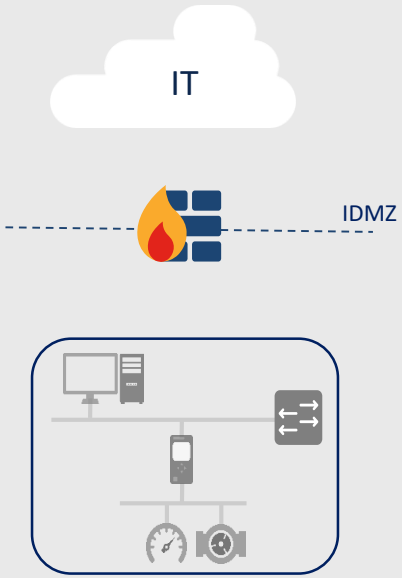
Many roadblocks towards success.
Industrial organizations need guidance.

Cisco IoT

Система безпеки OT Security Framework

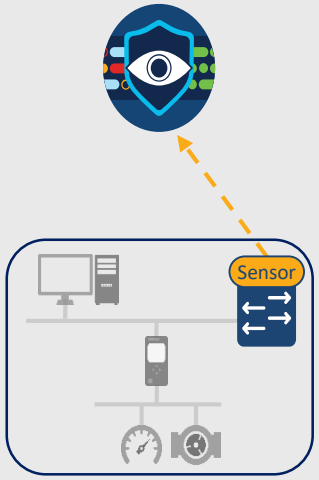
1 Створіть фундамент безпеки

Визначте межу IT/OT за допомогою Cisco Secure Firewall



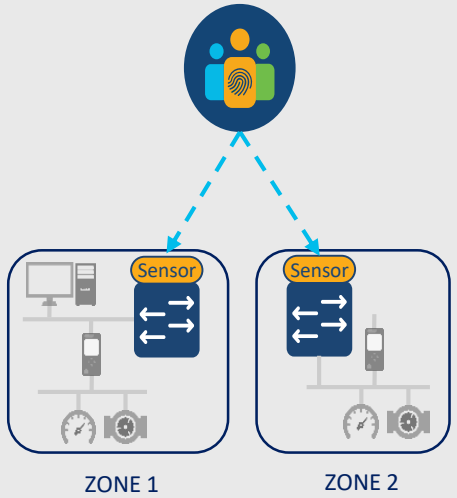
2 Покращуйте видимість і оцінки пристрою

Мережа як сенсор з Cisco Cyber Vision



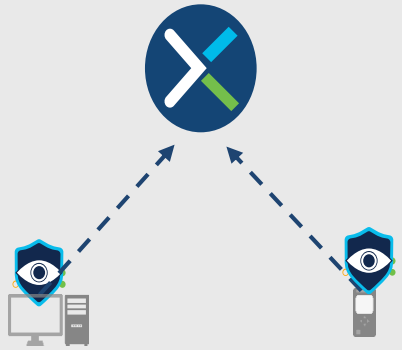
3 Сегментуйте мережу на менші зони довіри

Мережа як захисник з Cisco ISE



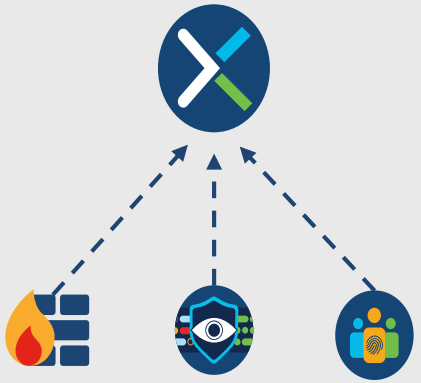
4 Посильте захист критичних станцій та серверів

Захищайте станції операторів та сервери з Cisco Secure Endpoint



4 Розробіть план реагування на інциденти

Досліджуйте загрози та реагуйте за допомогою Cisco XDR та Cisco Talos



Cisco IoT

Cisco Secure Endpoint в дії на прикладі пілоту для енергетики України

- Customers
- Users
- Organization Settings
- API Credentials
- Audit Log
- Service Agreement

energo | Tier: All | Time Period: 30 days

Generate API Keys

Name	Provisioning Status	Connectors	Compromised	TG Submissions	Global Threat Alerts Events	Payment State
[redacted]	completed	1479	0%	75	0	Not For Resale
	completed	1655	2.2%	229	0	Not For Resale
	completed	753	3.1%	273	0	Not For Resale
	completed	691	3.3%	3	0	Not For Resale
	completed	225	8.4%	0	0	Not For Resale
	completed	287	8.4%	55	0	Not For Resale
	completed	135	9.6%	14	0	Not For Resale
	completed	80	12.5%	23	0	Not For Resale
	completed	231	0%	0	0	Not For Resale
	completed	34	8.8%	0	0	Not For Resale
	completed	0	0%	0	0	Not For Resale
Totals (Filtered)	-	**5570**	-	**672**	**0**	-

1 – 11 of 11 total records

1 of 1

Export to CSV

TALOS

Cisco Security Research

Найбільша приватна дослідницька група з досліджень кібербезпеки у світі

Cisco IoT


cisco SECURE