

從風險範疇管理 厚植資安韌性基礎

趨勢 · 洞察 · 實踐



Bruce Lan

blan@paloaltonetworks.com

2024

Trend

Digital transformation and connectivity in OT environments bring great promise . . .



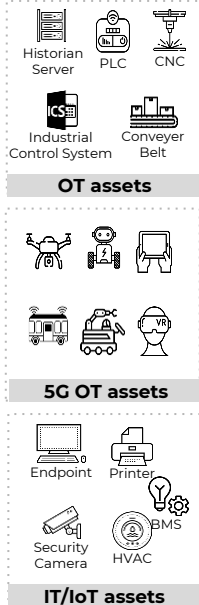
**IMPROVE OPERATIONAL
EFFICIENCY**



REDUCE COSTS



**ENHANCE WORKER
SAFETY**



... but they also bring great risk to operations.



Ukrainian Electric Grid Attack

Targeted power grid, resulting in blackouts



Saudi Arabian Oil Refinery Triton Attack

Targeted oil & gas, nuclear and manufacturing



Norsk Hydro Ransomware Attack

Affected aluminium production in 170 plants



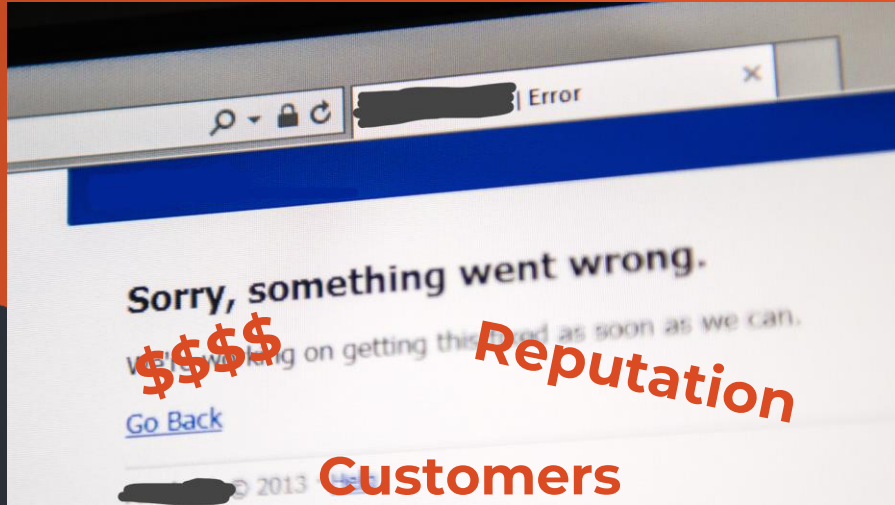
Colonial Pipeline Hack

Caused fuel and gasoline shortages

successful ransomware attacks on manufacturing sector FBI Internet Crime report

Enterprise cyber attack vs OT cyber attack

Enterprise



OT (ICS)



Insight



Modern OT security challenges ...



**You can't secure
what you can't see**



**Unseen vulnerabilities
create exponential risk**



**Threats are outpacing
the ability to stop them**



**You can't operate what is
too complex**

OT Security Challenged

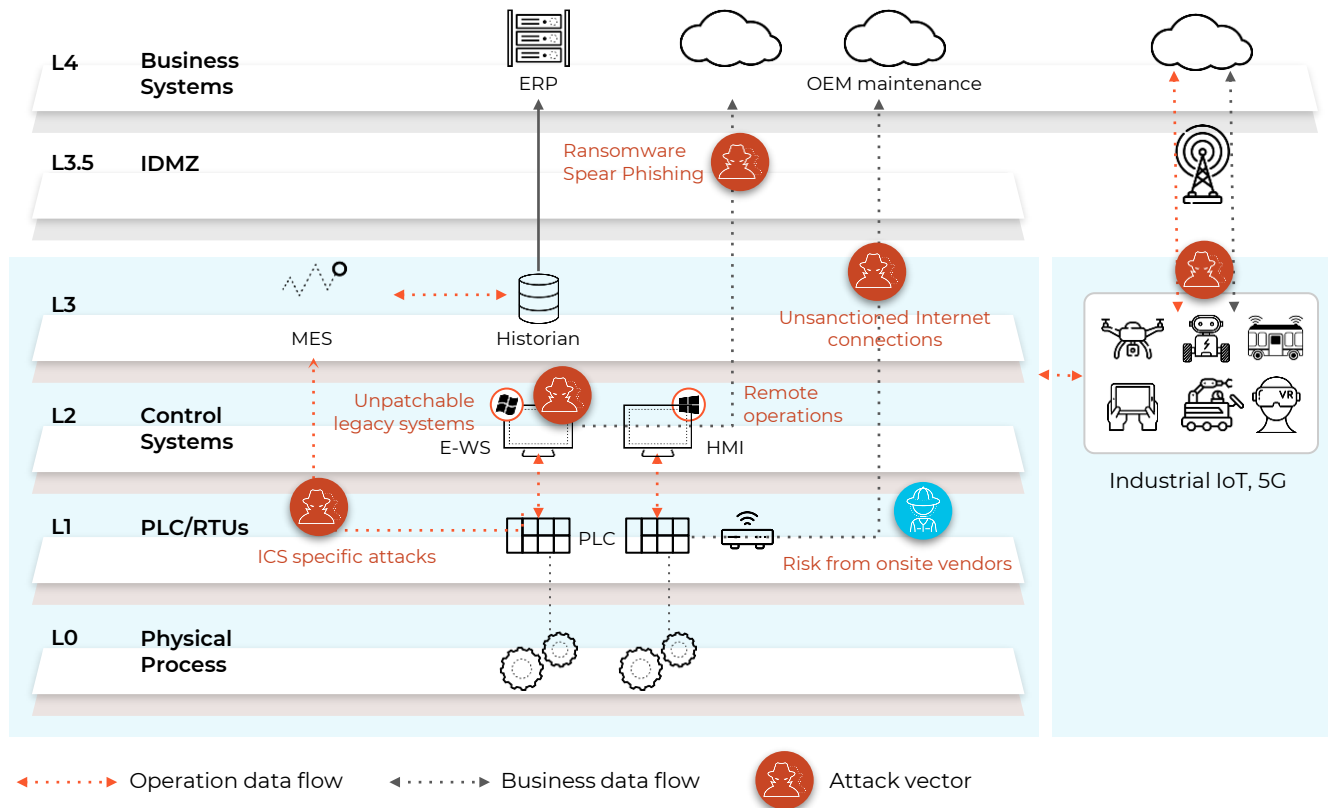
Legacy & vulnerable OT assets exposed to external threats, **lack effective segmentation & threat protection**

Lack of visibility into OT assets leads to security & compliance gaps

OT operation constraints challenge existing security tools and processes

New next generation 5G connected devices showing up for operational efficiency use cases, **lack of security strategy**

Lack governance & consistent security for OT networks, **hugely complex**



A Zero Trust OT Security Approach is More Critical Than Ever

to maximize operational uptime by reducing security breaches

1.

Least privilege access control

- Micro-segment
- Grant minimum access

2.

Continuous trust verification

- Asses OT assets security posture and behavior
- Asses app and user behavior

3.

Continuous security inspection

- Inspect all traffic, even for allowed connections
- Prevent all threats, including zero-day threats

**Founded on accurate visibility of assets, devices, apps and users across
OT Networks* | 5G Networks | Remote Operations**

* For ICS zones, applied as permissible under operating conditions, leveraging segmentation recommendations defined in IEC-62443

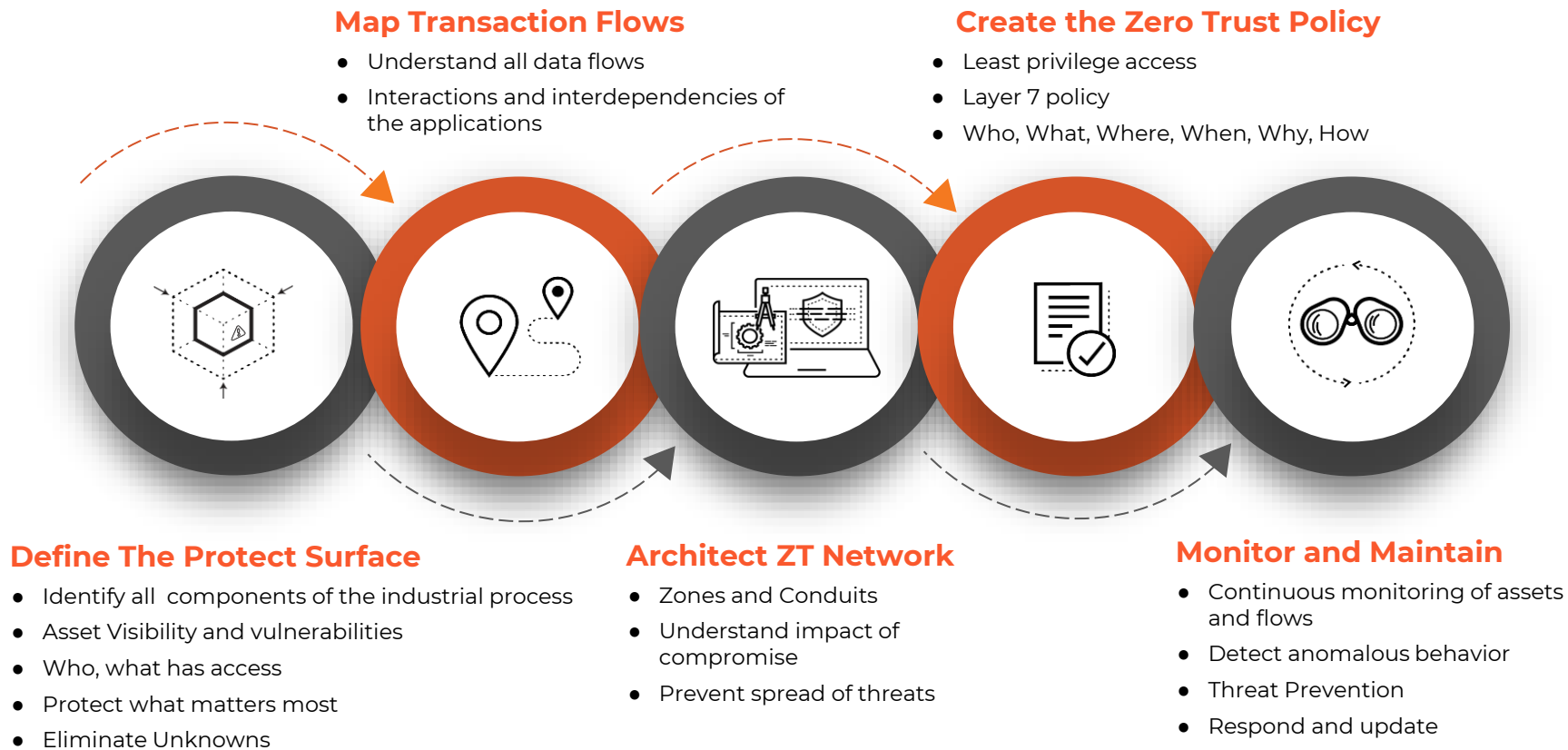
關鍵資產與服務

1. 誰是總統...

2. 總統在哪裡...

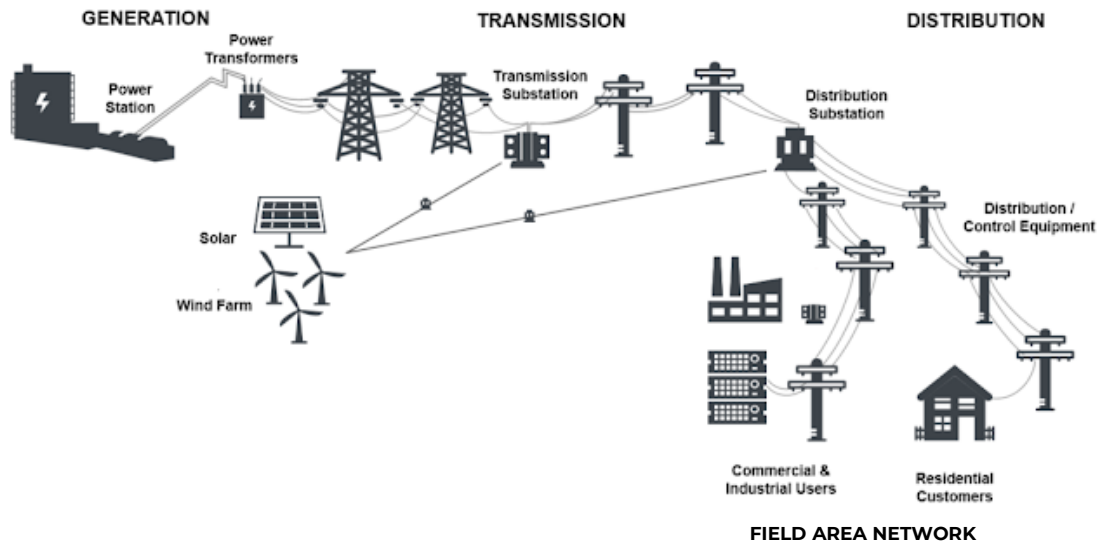
3. 誰可以接觸到總統...

5-Step journey for Zero Trust aligned with IEC-62443 standard



Best practice

Power Utilities - key use cases



Generation

- Secure power plants

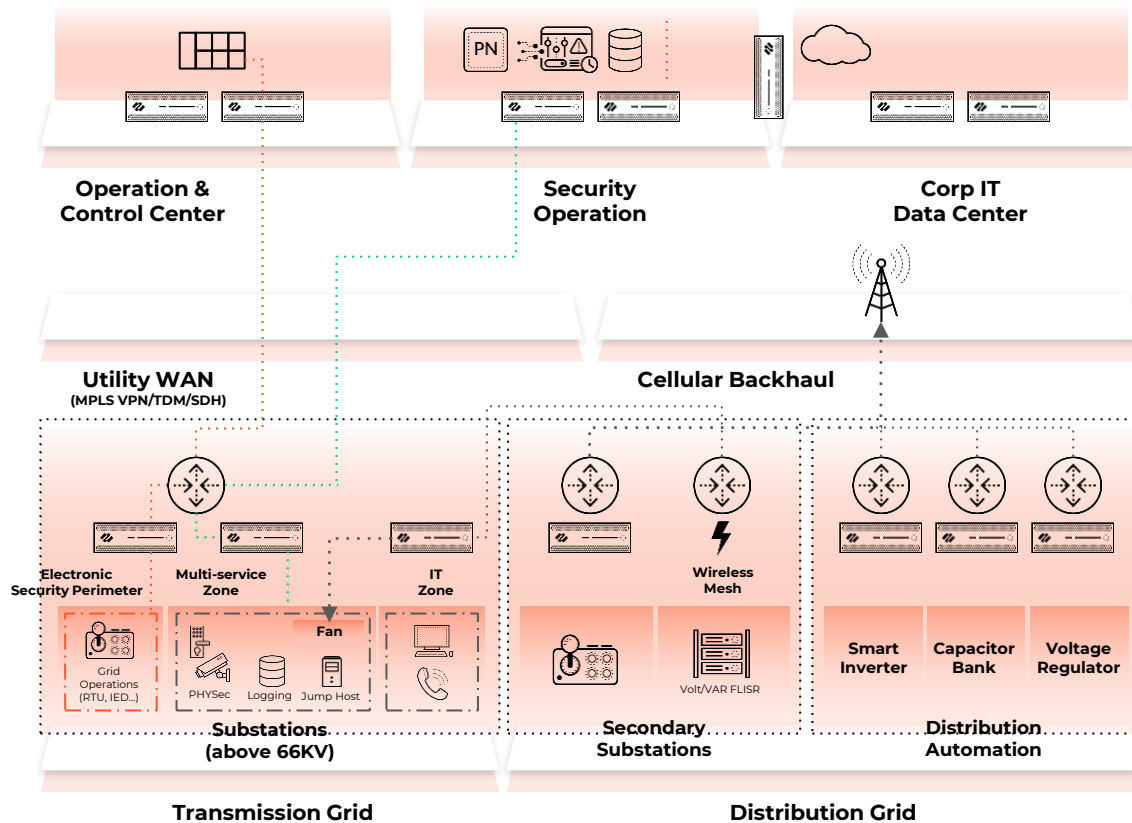
Distribution Grid

- Secure distribution substations

Transmission Grid

- Secure transmission substations

Power Utilities reference architecture



Zero Trust three use case - one platform

1

Secure OT Networks OT Assets

- Visibility into OT assets and risk factors with **Industrial OT Security**
- IT/OT (iDMZ) and OT segmentation
- Continuous security inspections

2

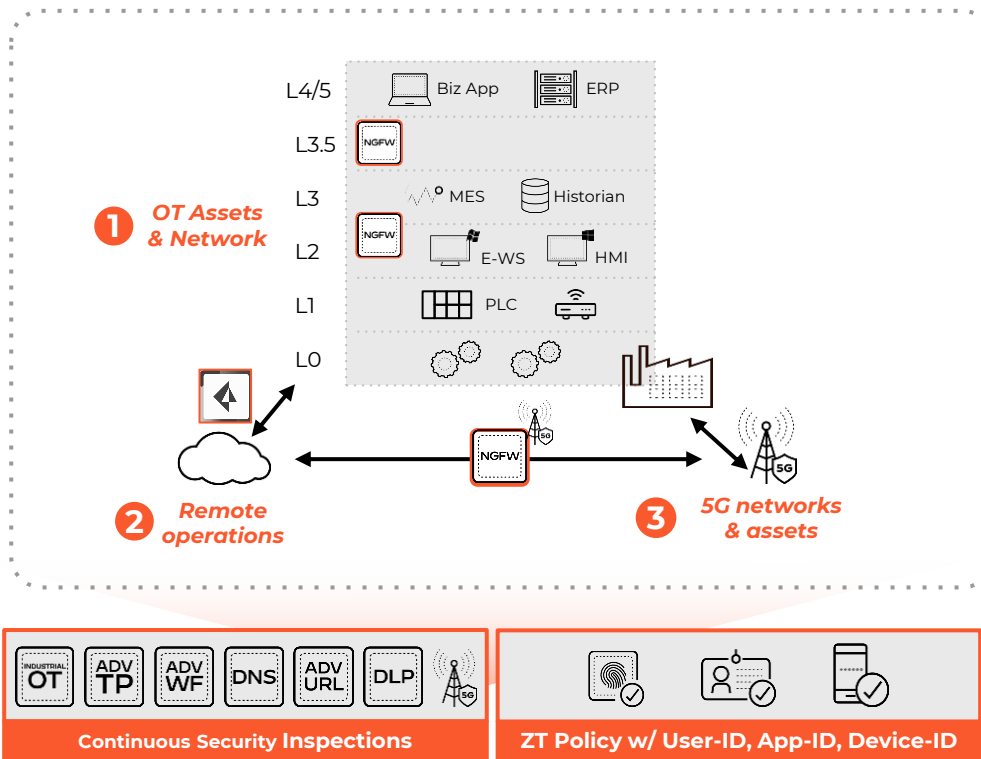
Secure Remote Operations

- Secure OT remote access (with ZTNA)
- Centralized SCADA operations (with SD-WAN)

3

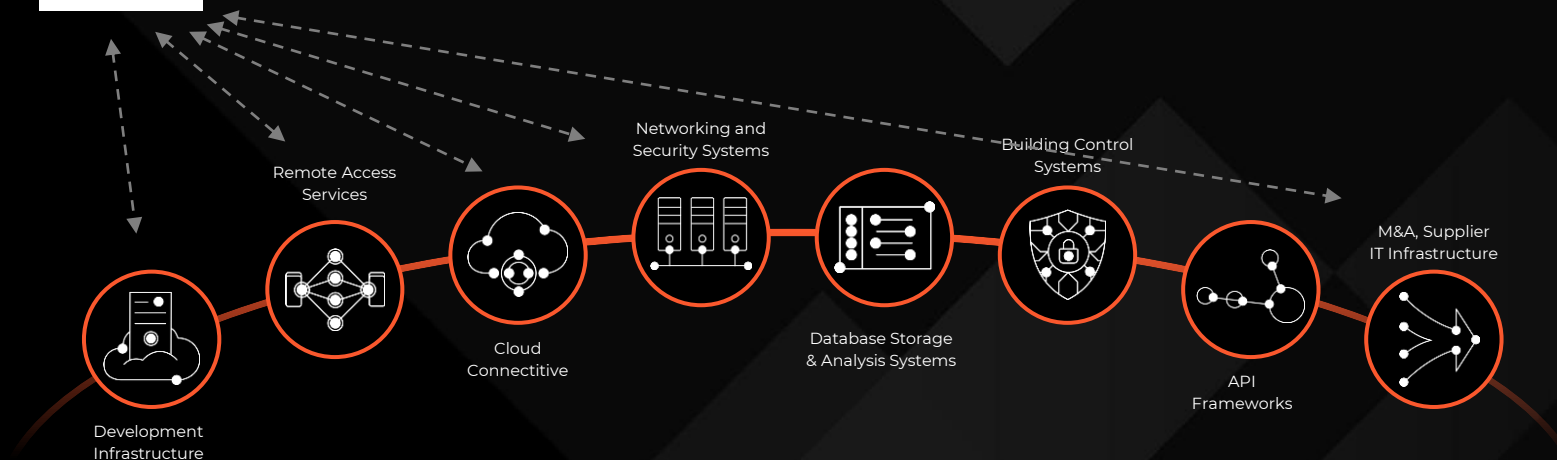
Secure 5G Assets & 5G Networks

- Mobile device (4G/LTE/5G) visibility
- Mobile identifier based security policy
- Advanced security inspections





Attack Surface = 攻擊者的機會之窗...

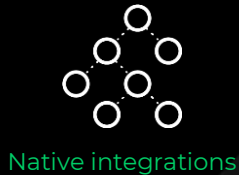


Our Attack Surface Management services are used by nearly 7,000 organizations to identify weaknesses in Internet-facing systems ...

Attack Surface Discovery

Complete

Vertically integrated scanning leads to 50x ports and 20x more banners per second than leading global scanners



Current

AI-driven discovery leads to +20% new assets discovered every month



Accurate

40% more assets discovered on average



【資安日報】2月2日，美國下令聯邦機構限時切斷Ivanti Connect Secure與內部網路環境之間的連線並著手清查

2月

2

資安日報

iThome CYBER INTELLIGENCE DAILY

聯邦機構應對曾與上述系統連線的所有裝置，持續進行威脅獵捕行動，並監控可能曝險的身分管理服務、設法將上述Ivanti系統與機構的其他資源隔離，並且繼續稽核曾存取的使用者帳號權限層級。

而對於上述Ivanti的系統，**CISA要求聯邦機構進行重設，回復至原廠初始設定**，並套用新版軟體或是導入緩解措施，最後，要將任何已連結或暴露的**憑證、金鑰、密碼進行撤銷與重新發布**的作業，才能讓這些系統上線。他們也要求聯邦機構必須在2月5日、3月1日，回報前述要求的處理狀態。



CORTEXXPANSE
BY PALO ALTO NETWORKS



Dashboards



Reports



Incident Response

Incidents

Alerts

Threat Response Center



Inventory



Settings



Tenant Navigator



Notifications (9)



Help



Bruce Lan

Public Television Ser...

Minimize menu



Incidents

Found 86 results



Export



Select the

Saved Filters **Custom**

Acclaim Systems USAHERDS, Apache NiFi, Atlassian Conflue...

+AND

Siemens

electric



Business units that end in (Only) contain assets assigned to that BU, but

Select All

Business Operations Applications (0)

Schneider Electric Harmony STU And STO Series HMI (0)

Schneider Electric Magelis XBT Touchscreen HMI (0)

IoT and Embedded Devices (21)

Schneider Electric Harmony GTO Series HMI (1)

Schneider Electric Harmony GTU Series HMI (0)

Schneider Electric Harmony STU And STO Series HMI (0)

Schneider Electric Magelis XBT Touchscreen HMI (0)

Operational Technology (2)

Schneider Electric Harmony GTO Series HMI (1)

Schneider Electric Harmony GTU Series HMI (0)

Schneider Electric Harmony STU And STO Series HMI (0)

Schneider Electric Magelis XBT Touchscreen HMI (0)



Business units that end in (Only) contain assets assigned to that BU, but not

Select All

Business Operations Applications (0)

Siemens Polarion Application Lifecycle Management (0)

IoT and Embedded Devices (21)

Siemens Desigo (1)

Siemens SIDrive IQ (0)

Siemens SIMATIC (0)

Siemens SIMOTICS (0)

Operational Technology (2)

Siemens Desigo (1)

Siemens Polarion Application Lifecycle Management (0)

Siemens SIMATIC (0)

Software Potentially Impacted by CISA Known Exploited Vulnera

Siemens SIMATIC (0)

在漏洞遭到利用前自動掌握並進行防治

完整的風險範疇探索

*See and monitor all assets
exposed to the internet*

零日漏洞的即時可視性

*Quickly know & react to
discovered threats and
vulnerabilities*

優先處理組織關鍵風險

*Proactively manage risk to focus
on highest impact areas*

專家劇本優化維運品質

*Reduce risk with actionable
context and automation*

無縫接軌管理工作

*Safe and easy to deploy in any
organization*

1,018

ASSETS UNDER MANAGEMENT

56.6%

All IP Addresses
(576)

21.9%

Services
(223)

6%

Certificate
(61)

0%

Cloud Resources
(0)

15.5%

Domain
(158)

Total External Assets – Filter Applied



- 158 | Domain
- 61 | Certificate
- 15 | Owned Responsive IP



Domains

Found 92 out of 158 results

Saved Filters

Custom



Last Updated: Apr 17th 2024 21:31

Recalculate

Externally Detected Providers not Contains On Prem

Business Units = Public Television Service Foundation V2, Unassigned

NAME	IPV4 ADDRESSES	DOMAIN RE...	ACTIVE SERVICE
		TWNIC	HttpServer
		TWNIC	HttpServer
		TWNIC	HttpServer
		TWNIC	HttpServer
		TWNIC	HttpServer
		TWNIC	HttpServer

20min

Inventory D

On

Risk Details

Higher Confidence Inferred CVEs



High

EXPLOIT MATURITY
WeaponizedEXPLOITED IN WILD
Yes

The following top CVEs contribute to this risk score. They were inferred based on matching CVE records with the observed software names and versions.

CVE ID	VULNERABILITY TEST RESULT	CVSS	EPSS SCORE	EXPLOITED IN WILD
CVE-2022-21661	Inferred	7.5 High	93.54%	No
CVE-2012-1023	Inferred	7.5 High	97.36%	Yes



Export

Select the format

302
RISK SCORE

'Insecure PHP (5.3.3) at about.p.org.tw:443'

Incident ID: ID-3

First Observed: Feb 05 2024

Time Open: 1 month

Tags: No

Overview

Alerts

Assets

Service/Website

Risk

Timeline

Service

Http Headers

Name
Date
Server
X-Powered-By
Location
Vary
X-Frame-Options
Content-Length
Content-Type

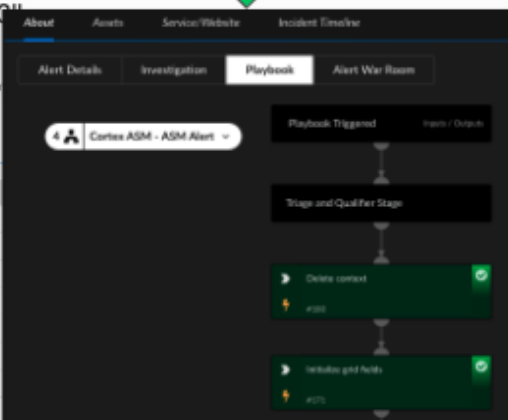


Cortex Copilot

Would you like to
do the remediation
by recommend
playbook ?

30Min -> 3Min

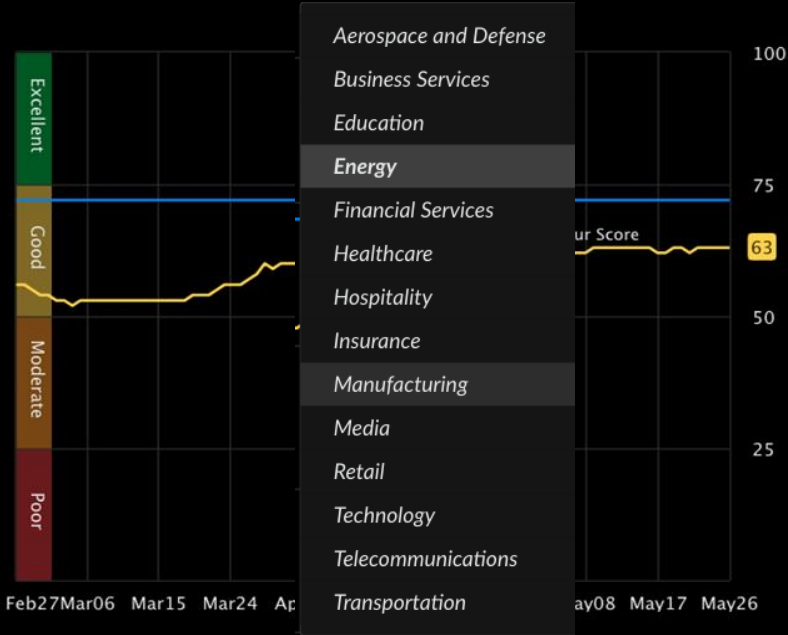
10min



Security Rating Trend Over Last 90 Days

Comparison Industry

Energy ▾

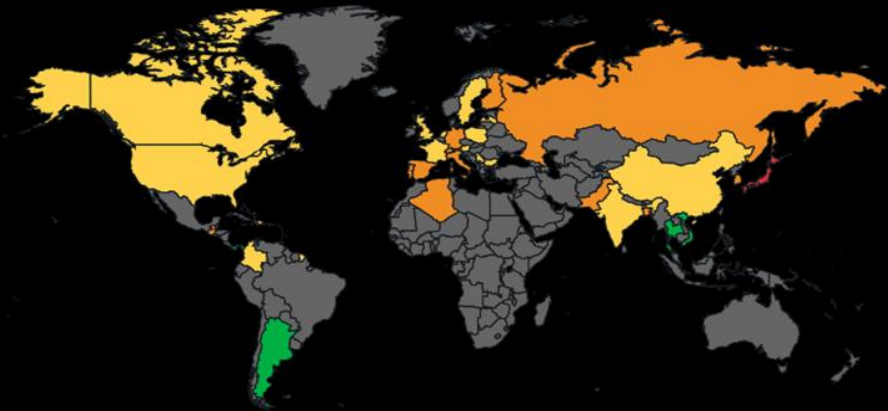


Overall Score 63 of 100 + 7 over last 90 days

Security Rating by Geo-IP Location

+

-



Cortex Xpanse is trusted by large and complex organizations

5 of the Fortune Top 10



Deployed across
every US DoD
Internet asset
(10% of the entire global Internet)



Protects all 6 branches
of the US Military
+ 45 DoD agencies



Protects all
federal civilian
agencies, 50
states, and over
3000 counties



Secures every
US nuclear
weapons lab



Secures every US
embassy and
consulate
worldwide



Thank You!



Bruce Lan

blan@paloaltonetworks.com