

## CloudOne Workload Security 註冊 VisionOne SOP

### 系統需求檢查

- 確保Workload Security Agent 版本至少v20.0.1559 或更高。
  - ≻ 檢查方式
    - Windows

至新增移除應用程式,檢視DSA版本。

• Linux

使用terminal執行指令: rpm -qa|grep ds\_agent



### Firewall 需開通 FQDN URLs & Port

- 請先檢查、開通Firewall相關網路配置,確保Workload Security Agent 能 對外Internet連線至下列TrendMicro CloudOne 及 Vision One 位置:
   下列註冊地區以Singapore 為例 (其它區域請參閱此):
  - \*.workload.sg-1.cloudone.trendmicro.com:443
  - gateway-control.workload.sg-1.cloudone.trendmicro.com:443
  - gateway.workload.sg-1.cloudone.trendmicro.com:443
  - \*.xdr.trendmicro.com:443
  - \*.xbc.trendmicro.com:443
  - \*.mgcp.trendmicro.com:443
  - \*.manage.trendmicro.com:443
  - ak5ih4ev105f2-ats.iot.us-east-1.amazonaws.com
  - ➤ azrb5zzyvrkw6-ats.iot.us-east-1.amazonaws.com



## Firewall 需開通 FQDN URLs & Port

若你的防火牆配置不支援\*.workload.<region>.cloudone.trendmicro.com格式,請個別允許訪運下列FQDN位置:

workload.sg-1.cloudone.trendmicro.com agents.workload.sg-1.cloudone.trendmicro.com •agents-001.workload.sg-1.cloudone.trendmicro.com •agents-002.workload.sg-1.cloudone.trendmicro.com •agents-003.workload.sg-1.cloudone.trendmicro.com •agents-004.workload.sg-1.cloudone.trendmicro.com •agents-005.workload.sg-1.cloudone.trendmicro.com •agents-006.workload.sg-1.cloudone.trendmicro.com •agents-007.workload.sg-1.cloudone.trendmicro.com •agents-008.workload.sg-1.cloudone.trendmicro.com •agents-009.workload.sg-1.cloudone.trendmicro.com agents-010.workload.sg-1.cloudone.trendmicro.com •gateway.workload.sg-1.cloudone.trendmicro.com •gateway-control.workload.sg-1.cloudone.trendmicro.com •xdr-resp-gw.workload.sg-1.cloudone.trendmicro.com dsmim.workload.sg-1.cloudone.trendmicro.com relay.workload.sg-1.cloudone.trendmicro.com agent-comm.workload.sg-1.cloudone.trendmicro.com

## Workload Security 註冊 Trend Micro Vision One (XDR)

• 登入 TrendMicro Vision One console (ADMINISTRATION → Product Connector)

$(\mathbf{A})$	ADMINISTRATION	sion One <sup>™</sup>	M Security	Dashboard		
	Single Sign-On					
[ÿ]]	User Accounts					
Х	User Roles					
₽≡	Product Connector	k Techniques			Got	о Арр
<b>_</b> •)			Critical	High	Medi	Total ↓
	Third-Party Integration	1.92)			450	450
	Alert Notifications	10.49)		20	50	70
ŗ	. P	cal(192.168			59	59
ഷ്ട്	Audit Logs	3.33)		39		39
<u></u>	Console Settings	3.108)			36	36
	License Information	2.80)	-	-	29	29



#### • 建立 Product Connector · 點擊Connect

V	Trend Micro V	ision One™   Product	Connector	O 2022-03-11 11:23 (UTC+08:00)	Ļ		NARRORS OF
	Connect					XD	PR Data Center: Sing
	Product	Connection status	Data center	Identifier 🛈	Desc	ription	Action
	Cloud One - Workload Security	<ul> <li>Connected 2022-03-11</li> <li>08:25:22</li> </ul>	United States	app.deepsecurity.trendmicro.com (870610754999)			Disconnect
₽E	Network Sensor	<ul> <li>Connected 2022-03-11</li> <li>11:23:02</li> </ul>		N/A			
£)							
ĽĴ							
ഷ്							
3							



#### • 產品名稱選擇 Select Product: Workload Security

Trend Micro Vi	sion One <sup>™</sup>   Product	Connector	
Connect			
Product	Connection status	Data center	Identifie
Cloud One - Workload Security	<ul> <li>Connected 2022-03-11</li> <li>08:25:22</li> </ul>	United States	app.deer (8706107
Network Sensor	<ul> <li>Connected 2022-03-11</li> <li>11:23:02</li> </ul>		N/A

Connect Product	×
* Product name:	
Cloud One - Workload Security	
Cloud App Security	
Cloud One - Workload Security	
Deep Discovery	
Network Security	
Deep Security Software	
TippingPoint Security Management System	
Trend Micro Web Security	



• 點擊Click Generate enrollment token並記錄保存token

#### **Connect Product**

#### \* Product name:

#### Deep Security Software

#### Enrollment token:

<u>Click to generate the enrollment token.</u> The token expires Automatically adds the product to the product list.

Description:

#### х **Connect Product** \* Product name: Cloud One - Workload Security () The product has been added to the product list. Copy and paste the enrollment token to the connecting product's web console to complete configuration. Enrollment token: eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJjaWQiOiJkYTNhOD ດ Expiration date: 2022-03-12 11:28:04 Description:

Х

 登入 Workload Security主控台,至 Administration > System Settings > 頁籤 Trend Micro Vision One(XDR) > 點擊Registration Button

ť	🥏 Trend Micro Cloud One <sup>™</sup> > Workload Security ~ Help ~													
							Workload Securi	ty Account Details   W	orkload Secu	ırity User Pro	perties   🥐 Help	🛇 Support 🗸   🗖	Search docu	mentation
D	ashl	board Actions	Alerts	Events & R	eports	Computers	Policies	Administration						
[	₽	System Settings		Syst	em Sett	tings								
	Ľ	Scheduled Tasks												
	Ľ	Event-Based Tasks		Agents	Alerts	Contexts	Event Forwardir	ng System Events	Security	Updates	Smart Feedback	Trend Micro Visio	n One (XDR)	Managed Detec
>	્	User Management		Registra	ation									
~	¢,	Updates		Enrollme	nt status: I	Registered								
	~	Security		Regist	er enrollm	ent token								
		Rules		Security	y Events	Forwarding								
		Patterns		Forv	vard securi	ty events to Tr	end Micro Vision (	One						
	~	Software												
		Agent Versio	on Control											
		- Local												
		🦻 Relay Manageme	ent											



• 輸入貼上Vision One上取得的Token並點擊Register button.





• 顯示Trend Micro Vision One 註冊成功

0	⑦ Trend Micro Cloud One <sup>™</sup> > Workload Security ~									
						Workload Secur	ity Account Details   W	orkload Secu	rity User Pro	perties   🥐 Help
Das	shboard	Actions	Alerts	Events & Reports	Computers	Policies	Administration			
*	🕻 System	n Settings		System Set	ttings					
	Schedu	lled Tasks								
	Event-E	ased Tasks		Agents Alerts	Contexts	Event Forwardi	ng System Events	Security	Updates	Smart Feedback
> 4	💧 User M	anagement		Registration –						
~ (	ື Dpdate	S		Enrollment status	Registered					
	🗸 🔒 Se	curity		Register enrolln	nent token					
		I Rules		Security Events	Forwarding					



## ・ 啟用[安全事件轉發] 勾選Security Events Forwarding > Save

7 Trend Micro Cloud One <sup>™</sup> > Workload Sec	curity ~ Help ~ Help ~
	Workload Security Account Details   Workload Security User Properties   ?) Help   🕥 Support 🗸   🝳 Search documentation
Dashboard Actions Alerts Events & Reports	Computers Policies Administration
🔅 System Settings System Se	ettings
Scheduled Tasks	
Event-Based Tasks	s Contexts Event Forwarding System Events Security Updates Smart Feedback Trend Micro Vision One (XDR) Managed Detec
> 🔹 User Management Registration -	
V TUpdates	Incent teken
✓ Security	
Rules Security Event	ts Forwarding
Patterns	curity events to Trend Micro Vision One
✓ ⊚ Software	
Agent Version Control	
Local	Also Security Events forwarding check box will be enabled and ticked.
Relay Management	
	Security Events Forwarding
轉發將曾包含以下	模組事件:
•Anti-Malware	
•Web Reputation	At this point Deep Security Manager is enrolled with Vision One for Detection modules events (IPS, IM, LI, WRS, AM
<ul> <li>Integrity Monito</li> </ul>	ring
<ul> <li>Log Inspection</li> </ul>	
•Intrusion Preven	tion
<ul> <li>ACTIVITY IVIONITORI</li> </ul>	



# 啟用 [Activity Monitoring] 至Policies > Activity Monitoring > General > On > Save ※Agent 版本必須至少 v20.0.0-1681或更高版本才能支援。

Policy: ActivitySensor								
Proverview	General							
🐼 Anti-Malware	Activity Monitoring							
Web Reputation	Activity Monitoring State: On  On							
Activity Monitoring	Default (Off)							
Intrusion Prevention	On							
Integrity Monitoring	ΟΠ							
Q Log Inspection	啟用後將會將以下事件轉發至Vison One(XDR):							
Application Control	<ul> <li>Process activity</li> <li>File activity</li> </ul>							
Interface Types	<ul> <li>Network activity</li> </ul>							
Settings	<ul> <li>Connection activity</li> <li>Domain query activity</li> </ul>							
X <sup>♣</sup> Overrides	<ul> <li>Registry activity (Windows only)</li> </ul>							
	User account activity (Windows only)							



C



