SECURE PSU VoD Cisco XDR **製品統合ガイド** Firewall Threat Defense 編⁽)

2024年3月 シスコシステムズ合同会社 セキュリティ事業

CISCO



XDR - Firewall Threat Defense 構成と動作の仕組み



動作概要

- 1) FMC で管理している FTD デバイス がイベントを生成
- 2) FTD デバイスが、サポートされてい るイベントを Security Service Exchange (SSX) に送信
- 3) XDR が検出情報を SSX に照会し、
 XDR にイベントやインシデントとして表示

XDR - Firewall Threat Defense 本ガイドでの条件

- FMC 管理の FTD と XDR の連携方法を解説
 FDM 管理でも XDR との連携は可能だが本ガイドでは割愛
- FMC / FTD バージョン 7.2 以降で、FTD と XDR が直接連携する方法を解
 説

Syslog 経由であればバージョン 6.3 から、直接連携であればバージョン 6.4 から FTD と XDR との連携は可能だが、バージョン 7.2 以降の直接連携が最もシンプルでわかり やすいので、本ガイドはその方法の解説に注力

 FMC でレジストしている Smart Account の Virtual Account に管理者権限 が必要 評価期間中の FMC / FTD (Smart License 未登録) では連携設定不可



ISCO SECURE © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

XDR - Firewall Threat Defense 設定手順の流れ



設定手順

- 1) Security Services Exchange (SSX) にて Smart Account を紐付け
- 2) Firewall Management Center (FMC) にて XDR との連携設定
- 3) XDR 管理コンソールにて Secure Firewall (FTD) インテグレーション の確認
- 4) 動作確認

設定1) SSX で Smart Account の紐付け

SecureX End of Life. Cisco anneunced the end-of-life for Cisco SecureX on August 11, 2023. An improved experience for customers to manage their Cisco Security Cloud applications will be released to replace Se	1 Cisco Security Cloud にログイン https://sign-on.security.cisco.com
Image: Cloudlock Meraki Umbrella De Secure Access Secure Access Secure Workload Circo Cloudlock Ope Merali De Secure Access Secure Workload	② 使っているデータセンターの XDR をクリックして XDR 管理画面にログイン (本ガイドでは APJC)
CDO (APJC) Cisco Defense Orchestrator (APJC)	eraki China Cisco Vulnerability Management (IN)
SecureX Threat Response (APJC)	5

設定1) SSX で Smart Account の紐付け(続き)

			Integrations					
allala yoo			Q. Search Capabilities V Aut	thorship Type 🗸				
cisco XDR			My Integrations				~	
≡		Administration ×	Cisco Third-Party Cisco Integrations					
Control Center	>	My Account 🗸	Cisco Defense Orchestrator	Cisco Duo	Cisco Threat Intelligence API	Cisco Vulnerability Management	Sec Cyber Vision	
Incidents		Notifications	se Cisco Managed	an Cisco Managed	te: Cisco Managed	se: Cisco Managed	se Cisco Managed	
-Q Investigate		Playbooks 1	Claco Defense Orchestrator sa o dou-based multi-device manager you can use to manage feculty post, changes across verices security products. Free Trial Get Started	Continuously verify user and device trust to protect access from everywhere with MFA, SSD, passwordtes, and more.	An open-source architecture and API for hosting and providing threat intelligence data to inform XOE westigations.	Clico Vulnerability Management (tormety Kanna VM) is a mich-based vulnerability management platform the hops security and IT teams determine which vulnerabilities por Free Trial Cet Started	Cyber Vision short description place holder. Get Started	
🕸 Intelligence	>	On-Premises Appliances				2		
Automate	>	API Clients Users	Cisco Managed Meraki provides clock-managed IT solutions, from networking appliance to endpoint management.	Orbital Cisco Managed Cisco Orbital is a service that uses Dropsery to provide you and your applications with detailed information about your brote.	((e)) SMA Web Cisco Managed The Cisco Content Society Management Applance (SMA) centratizes management and reporting functions across methics Cisco mail and web method panolesces	Cisco Managed Cain the visibility and continuous thread detaction needed to secure your public cloud, private network, and hybrid	Secure Email Appliance Cisco Managed The Cisco Secure Email Appliance (formerly Email Security Appliance) provides advanced threat protection capabilities for detect fork and remeded thereas feature report for	
Assets	>		Get Started	Get Started	Get Started	Free Trial + Enable	Free Trial Get Started	
ा त्र _{भेग} Client Management	>		Secure Email Threat Defense (Australia)	Secure Email Threat Defense (India)	Secure Email and Web Manager	Secure Endpoint	Secure Firewall	
20 Administration	>		tat Cisco Managed Cisco Secure Email Threat Defense (formerly Secure Email Cloud Malibox) provides the most comprehensive protection	tte Cisco Managed Cisco Secure Email Threat Defense (formerly Secure Email Cioud Malbox) provides the most comprehensive protection	ta: Cisco Managed Cisco Secure Email and Web Manager (formerty SMA Email) centralizes management and reporting functions across	tt: Cisco Managed Secure Endpoint (formerly AMP for Endpoints) prevents threats at the point of entry, by identifying and halting	tez Cisco Managed Secure Firewall (formerly Firepower) provides complete and unified management over firewalls, application control,	
			against damaging and costly threats that compromise your Free Trial + Enable	against damaging and costly threats that compromise your Free Trial + Enable	multiple Cisco email and web security appliances. Free Trial Get Started	advanced threats before they reach your endpoints. Free Trial + Enable	Intrusion prevention, URL filtering, and advanced malware Free Trial Get Started	

- 1 XDR 画面左メニューより Administration → Integration をクリック
- 2 Cisco Integrations から Secure Firewall の Get Started をクリック

CISCO SECURE © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



③ Go to Security Service Exchange をクリック 6

設定1) SSX で Smart Account の紐付け(続き)



Link	Smart/Virtual Accounts 💿	\times
	Select accounts to be linked to FTD-GUIDE-TEST-JP	
0	Your Smart or Virtual Account can be connected to one SecureX ten at a time. If you don't see it available here, check whether your team has already connected it to another SecureX tenant.	ant
	Smart/Virtual Accounts Cisco Demo Internal Customer Smart Account (dem GSSO Architecture (gsso-architecture.cisco.com) InternalTestDemoAccount69.cisco.com (internaltest InternalTestDemoAccount69.cisco.com (internaltest tatskoba-test sangWich (ciscointernal.cisco.com)	
	Cancel Link Smart/Virtual Accounts	s. A

Accounts Linked to	FTD-GUIDE-TEST-JP
inked 1 of 1 Account(s)	
Smart/Virtual Accounts A	Status
InternalTestDemoAcco / tatskoba- test	✓ Linked

- 1 Link More accounts をクリック
- ② FMC にてレジストしている Virtual Account (要管理者権限)を選択して Link Smart/Virtual Accounts をクリック
- ③ Smart/Virtual Account が SSX に紐付いたこと を確認して OK をクリック

s. All rights reserved. Cisco Public

補足) SSX でのイベントプロモート

		cisco Security Services Exchange	Devices Cloud Services Events Audit Log	
		Cloud Services for FTD-GUIDE-TEST	r-JP	
	Settings		Cisco SecureX threat response or Cisco XDR Cisco SecureX threat response or Cisco XDR enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.	•
	General Filter Intrusion Events Auto-Promote Events			
	✓ By Event Type		Eventing Eventing allows you to collect and view events in the cloud.	€) ⇔
	Intrusion Events			
	Impact Red (Poor)			
	Talos IP Reputation ()			
	All other lower impact events 0	カイドでは、Intrusion	Event を全て SSX 経由で XDR で解析す	「るため、
	Malware Events	SX σ Cloud Services \cdot	→ Eventing を有効にして Auto-Promote	e Events で
	All Security Intelligence Events	rusion Events 全てを	与効にしておくこと	
	IP Reputation			
	> By Custom IP Address (Intrusion Events Only)			
	> By Intrusion Rule Category			
	> By Custom Security Intelligence Object			
וןוי כוי	2	Discard Save		8

設定2) FMC にて XDR 連携を設定

Firewall Management Center	Overview Analysis Policies Devices Obje	ts Integration Deploy Q 🥥 🌣 🖗 admin ▼ """"" "	ECURE
SecureX Integration			
SecureX Setup		Cisco Cloud Support	
This feature allows Secure Firewall Man	agement Center to integrate with other SecureX services via SecureX ril	bon. Learn more C The Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings	
1 Cloud Region	This setting determines where events are sent to, if configured to se well as data generated by the Cisco Success Network and Cisco Su tools. Current Region ap-northeast-1 (APJ Region)	▲ Do you want to change the region? Changing your region without having either Smart Licensing or SecureX enabled will result in no change to region upon save.	
2 SecureX Enablement	After completing this configuration, the SecureX ribbon will show up each page. Learn more \underline{r}_{2}^{\ast}	Cancel Confirm	
	Enable SecureX 🗅	FMC の Integration → SecureX * をク	リック、SecureX
3 Event Configuration	 Send events to the cloud Intrusion events File and malware events Connection Events Security All 	Setup 画面の ① Cloud Region からXI は通常は APCJ であり本ガイドも AP て Confirm をクリック	DR の Region (日本で JC を利用) を選択し
(4) Orchestration	Enable SecureX orchestration to allow SecureX users to build autom that interact with various resources in the Secure Firewall Managem Learn more C	ted workflows nt Center.	

****** se*注) FMC での XDR 連携設定のメニューは、まだ SecureX という表記になっている 9

設定2) FMC にて XDR 連携を設定 (続き)

Firewall Management Center	Overview Analysis Policies Devices Objects Integration	Deploy Q 📀 🏠 🚱 admin 🛛 📩
SecureX Integration		
SecureX Setup		Cisco Cloud Support
This feature allows Secure Firewall Mana	agement Center to integrate with other SecureX services via SecureX ribbon. Learn more 🛙	The Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco.
(1) Cloud Region	This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.	The Management Center will establish and maintain this secure connection at all times, you can turn on this connection at any time by disabling Clace Success Network and Clace Support Clagnostics. Disabling these services will disconnect the Management Center from participating in these additional cloud service offerings.
	Current Region ap-northeast-1 (APJ Region)	> 🛃 Enable Clisca Success Network
		Enable Cisco Support Diagnostics
2 SecureX Enablement	After completing this configuration, the SecureX ribbon will show up at the bottom of each page. Learn more $\underline{\sigma}$	① Event Configuration より XDR (SSX) に送りたい
	Enable SecureX [1]	イベントを選択
3 Event Configuration	Send events to the cloud View your Close Cloud configuration View your Close Cloud configuration	2 Save をクリックして設定を反映させる
	Intrusion events view your Events in SecureX	
	Connection Events	
	G Security	
	 All () 	
(a) Orchestration	Enable SecureX orchestration to allow SecureX users to build automated workflows that interact with various resources in the Secure Firewall Management Center. Learn more Ξ	
	Enable SecureX Orchestration	
	Specify the Firewall Management Center user role you want to assign to the SecureX orchestration workflows. Assigned Role	
	Access Admin 🗸	
		2 Save

cisco SECURE © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

設定2) FMC にて XDR 連携を設定 (続き)

iniļi. Isco	Secu	rity Ser	vices Excl	hange Devices Cloud Services Ever	nts Audit Log					0 * Å	Tatsuya Kobayashi 🕚
Devic	es for	FTD-0	GUIDE-TES	ST-JP							
• 0 Rov	Q Dev	vice Name	/ ID								+ 0 Ľ
		*∕↓	#	Name 🔿	Туре	Version	Status	Cloud Connectivity	Description	Actions	
		>	1	cdo-cisco-tatskoba	Cisco Firewall Confi	7.4.1	Registered	2024-03-29 03:46:48	10.200.23.27 cdo-cisco-tatskoba		
		>	2	FMCTEST	Secure Firewall Man	7.2.6	🐼 Registered	2024-03-29 04:02:58 I	192.168.254.67 FMCTEST		J
C		>	3	FTDTEST	Cisco Firepower Thr	7.2.6	🚯 Registered	2024-03-29 04:02:59 I	192.168.254.57 FTDTEST (FMC managed)		
		>	4	Secure Event Connector - localhost.localdomain	Secure Event Conne	2023120819	🕄 Registered	2024-03-29 03:48:26	Secure Event Connector listening on TCP: 10125, UDP: 10025, N.		
Page	Size: 2	25 ~	Total Entries:	4							< < 1 > >

FMC 側での Cloud Region 指定が終わると、SSX の Devices の画面に、FMC と FTD デバイスの一覧が表示される

設定2) FMC にて XDR 連携を設定(続き)





FMC に戻って ② SecureX Enablement にある Enable SecureX というボタンをクリック

② ブラウザ内で新たなタブが起動、Continue to Cisco SSO をクリック、Cisco Security Cloud へのログインを行う

cisco SECURE © 2024 Cisco and/or its affiliate

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

設定2) FMC にて XDR 連携を設定 (続き)

		rview Analysis	Policies Devices Objects Integration		De
		egion ap-northeast	-1 (APJ Region) 🗸	Enable Cisco Support Diagnostics	
	uluilu cisco				
	Welcome to Cisco Defense Orchestrator	pleting this configuration	n, the SecureX ribbon will show up at the bottom of		
	To proceed with the registration of your FMC, please select a CDO tenant to register with the FMC and verify the code displayed below matches the user code from your FMC.	ureX setup is waiting for	Grant Application Access	:	×
-	Select Tenant O Create Tenant	SecureX C View Se	cure Please verify the code	e provided by SecureX.	
	Search Tenants	events to the cloud	- 3EB7	26CE	
	cisco-jp-fy24-hot-6	trusion events			
	cisco-jp-fy24-hot-7 cisco-jp-fy24-hot-8	le and malware events			
	cisco-jp-fy24-hot-9			Close	
- 1	cisco-tatskoba	コートの合致を確認			
		ecureX orchestration to	allow SecureX users to build automated workflows		
	Grant Application Access	act with various resource re 단	es in the Secure Firewall Management Center.		
	Compare the code below to the authorization code shown in the FMC tab. If the codes match, authorize the FMC to complete the registration.				
	3EB726CE	Cisco Security C	loud にログイン後	後、利用する (DDO のテナ
	The FMC will be registered with tenant cisco-tatskoba	2010 ントが表示される	る(複数のテナント	、があれば複数	が表示される
1	Authorize FMC	ので利田するテ-	ナントを選択)		
	2				
		💻 2 画面下部に表示 る	されたコードと、「	-MC の画面に表	示されてい
		るコードが合っ ⁻	ていることを確認	τ Authorize F	EMC をク
	cisco SECURE © 2024 Cisco and/or its affiliate				
		リッシン			

設定2) FMC にて XDR 連携を設定 (続き)

2	SecureX Enablement	After completing this configuration, the SecureX ribbon will show up at the bottom of each page. Learn more 🗅
	(A SecureX is enabled for APJ Region. You will need to save your configuration for this change to take effect.
		Enable SecureX 🗹
3	Event Configuration	Send events to the cloud View your Cisco Cloud configuration
		✓ Intrusion events View your Events in SecureX
		File and malware events
		Connection Events
		⊚ Security
		All
4	Orchestration	Enable SecureX orchestration to allow SecureX users to build automated workflows that interact with various resources in the Secure Firewall Management Center.
		Enable SecureX Orchestration
		2 Save
		ithorized FMC が終わると Region で XDR (表示は SecureX) が Enable になった旨の ッセージが表示される



設定2) FMC にて XDR 連携を設定(続き)

XDR へのレジストが終わり、 XDR が有効になった旨のメッ セージ (表示は SecureX) が表示 される

tools.

Current Region

SecureX Integration

SecureX Setup

1 Cloud Region

2 SecureX Enablement



1111 ciso

設定2) FMC にて XDR 連携を設定(続き)

3 Event Configuration	✓ Send events to the cloud ● View your Cisco Cloud configuration ✓ Intrusion events View your Events in SecureX
	File and malware events
	Connection Events
	⊙ Security
	All ()
(4) Orchestration	Enable SecureX orchestration to allow SecureX users to build automated workflows that interact with various resources in the Secure Firewall Management Center. Learn more 더
	Enable SecureX Orchestration
× ::::	Save

Security Events を Cloud に送る設定になっていることを確認 (なっていなければ再度設定して Save) し、Deploy を実施

加也		Deploy Q 🥝 🌣 🝘 admin ▼ 🔤 🔥 SEC
	۹	Advanced Deploy Deploy
	FTDTEST	Ready for Deployment



cisco SECURE © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

設定3) XDR にて FMC & FTD の登録を確認

		Integrations						
cisco XDR		Q. Search Capabilities V Aut	Cisco	Integrations	から Secure F	irewall ${\cal O}$ Get		
		My Integrations	Ctorto			~		
_	Administration X	Cisco Third-Party	Starte	a をクリック				
-		Cisco Integrations						
Control Center >	My Account 🗸	Cisco Defense Orchestrator	R Cisco Duo	Cisco Threat Intelligence API	Cisco Vulnerability Management	کچ Cyber Vision		
Incidents	Notifications	tte Cisco Managed	the Cisco Managed	dat Cisco Managed	td: Cisco Managed	to: Cisco Managed		
P	Playbooks	Cisco Defense Orchestrator is a cloud-based multi-device manager you can use to manage security policy changes across various security products.	Continuously verify user and device trust to protect access from everywhere with MFA, SSO, passwordless, and more.	An open-source architecture and API for hosting and providing threat intelligence data to inform XDR investigations.	Cisco Vulnerability Management (formerly Kenna.VM) is a risk-based vulnerability management platform that helps Security and IT teams determine which vulnerabilities pos	Cyber Vision short description place holder.		
-Q Investigate	ntegrations	Free Trial Get Started	Get Started	Get Started	Free Trial Get Started	Get Started		
	Dn-Premises Appliances							
A	API Clients	🕞 Meraki	Orbital	SMA Web	Secure Cloud Analytics	Secure Email Appliance		
+ Automate >	leare	** Cisco Managed	Cisco Managed	the Cisco Managed	Cisco Managed	the Cisco Managed		
	72612	networking appliances to endpoint management.	and your applications with detailed information about your hosts.	centralizes management and reporting functions across multiple Cisco email and web security appliances.	secure your public cloud, private network, and hybrid environments.	Appliance) provides advanced threat protection capabilities to detect, block, and remediate threats faster, prevent dat		
Assets >		Get Started	Get Started	Get Started	Free Trial + Enable	Free Trial Get Started		
ः ब्रह्म Client Management		Secure Email Threat Defense (Australia)	Secure Email Threat Defense (India)	Secure Email and Web Manager	Secure Endpoint	Secure Firewall		
		ttt: Cisco Managed	ntt Cisco Managed	tat Cisco Managed	## Cisco Managed	tt Cisco Managed		
20 Administration >		Cisco Secure Email Threat Defense (formerly Secure Email Cloud Mailbox) provides the most comprehensive protection against damaging and costly threats that compromise your	Cisco Secure Email Threat Defense (formerly Secure Email Cloud Mailbox) provides the most comprehensive protection against damaging and costly threats that compromise your	Cisco Secure Email and Web Manager (formerly SMA Email) centralizes management and reporting functions across multiple Cisco email and web security appliances.	Secure Endpoint (formerly AMP for Endpoints) prevents threats at the point of entry, by identifying and halting advanced threats before they reach your endpoints.	Secure Firewall (formerly Firepower) provides complete and unified management over firewalls, application control, intrusion prevention, URL filtering, and advanced malware		
		Free Trial + Enable	Free Trial + Enable	Free Trial Get Started	Free Trial + Enable	Free Trial Get Started		
XDR 画面左メニューより Administration → Integration をクリック								
			FMCTEST	7.2.6 Registered	192.168.254.67 FMCTEST	192.168.254.67		
			FTDTEST	7.2.6 V Registered	192.168.254.57 FTDTEST (FMC managed)	192.168.254.57		
SFMC 😕 FI	∪ か登録されてし	いることを催認	Secure Event Connector - localhost.localdom	nain 202312081933 🕑 Registered	Secure Event Connector listening on TCP: 10125, UDP: 10025, N	NETFLOW: 10425 192.168.10.213		
					5_ r	berpage 1-3 of 3 ≪ < [1]/1 > ≫		
cisco SECURE @	© 2024 Cisco and/or its affiliates. All rig	ghts reserved. Cisco Public	Create Dashboard Create a dashboard of the tiles associated with	this integration, which can be shared by all members of your	organization.			
						+ Add		

設定4) XDR にて FTD Dashboard を作成



設定4) XDR にて FTD Dashboard を作成(続き)

Customize Dashbo	ards	C* Refresh	Tiles ×	
My Dashboards ii: Overview	Overview Author: Cisco XDR			
	The Overview dashboard provides a high-level summary of the incidents, includir ATT&CK® tactics and techniques, an overview of unassigned incidents organized reported by sources, and a mean time summary of incidents within your organiza by default and it is read-only.	Customize Dashboa	ards Dashboard Name	C ^e Refresh Tiles ×
		ii Overview	MyFTD-Dashboard	
		HyFTD-Dashboard	Dashboard name is required	
			Automation © 0 selected	Add All 🗸 🗸
			Private Intelligence O selected	Add All 🗸
+ Create new dashboard			Secure Client 🕒 0 selected	Add All ~
Shared dashboards (Secure Firewall O selected	2 Add All ~
		+ Create new dashboard Shared dashboards (i)	SecureX Global Threat Intelligence O selected	Add All 🗸
		No Dashboards		
+ Create nev	w dashboard をクリック			
任意の Dash	board 名を追記し、			
Secure Firev	vall の Add All をクリック			
cisco SECUR	E © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public		Cancel	Save

設定4) XDR にて FTD Dashboard を作成(続き)

	Customize Dashboa	C' Refresh Tiles	×		
	My Dashboards	boards Dashboard Name			
	ii Overview	MyFTD-Dashboard			
	:: MyFTD-Dashboard	Dashboard name is required			
		Automation O selected	Add All	~	
		Private Intelligence 🕒 0 selected	Add All	×	
		Secure Client © 0 selected	Add All	~	
		Secure Firewall 🥑 9 selected	Remove All	~	
	+ Create new dashboard	SecureX Global Threat Intelligence • 0 selected	Add All	~	
	No Dashboards				
Secure	Firewall で 9 se	elected (今後の Version によ	って数は変更有り))	となったことを
確認して	Save をクリ	ック		-	
		Carcel	S	We	
cisco SECURE	© 2024 Cisco and/or its affiliate	es. All rights reserved. Cisco Public			1

設定4) XDR にて FTD Dashboard を作成(続き)

FTD の Dashboard が作成されたことを確認



SECURE



Ę	Firewall Managem	nent Center c	Overview Analysis F	Policies Devices Obje	cts Integration				Deploy	Q 🔮 🌣 😰 admin 🔻	cisco SECURE
٩	Select										× Refresh
Ø)Showing 4 events (🖘 3 😌 1)	<u>+</u>							腸 2024-03-29 17:17:2 2	2 JST → 2024-03-29 17:17:48 JST	26s Resume
i	Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Application	Access Control Rule	Access Contr
	✓ 2024-03-29 17:17:24	😌 Intrusion	Block		192.168.150.74	192.168.10.72	58425 / top	21 (ftp) / tcp		CATCH-ALL	ACP-1
										Open in Pac	ket Tracer
	Event Type: 😍 Intrusion				Generator: Standard Text Rule				Ingress Interface: inside		
Time: 2024-03-29 17:17:24			Application Protocol: FTP				Egress Interface: outside				
Priority: medium			Application Protocol Category: remote file storage, network protocols/services				Ingress Virtual Router: Global				
Impact: Impact 2			Application Protocol Tag: file sharing/transfer			Egress Virtual Router: Global					
	Action: 😑 Block			Client Application: FTP client				Intrusion Policy: INTRUSION-1			
	Source IP: 192.168.150.74			Application Risk: Medium				Access Control Policy: ACP-1			
	Destination IP: 192.168.10.72				Business Relevance: Medium			Access Control Rule: CATCH-ALL			
Source Port / ICMP Type: 58425 / tcp			Ingress Security Zone: inzone			Network Analysis Policy: Balanced Security and Connectivity					
Destination Port / ICMP Code: 21 (ftp) / tcp				Egress Security Zone: outzone		Source Host Criticality: None					
Intrusion Message: PROTOCOL-FTP CWD ~root attempt (1:336:17)				Domain: Global			De	Destination Host Criticality: None			
		Classification: Potentially Ba	d Traffic		Device: FTD	TEST					

テスト用のイベントを発生させる。この例では、SID 336 の Intrusion Rule を Block に変更 (FTP サーバにログインして cd ~root を実施したら通信ブロック) し、実際にこの Rule にヒットするテ スト通信を発生させている

cisco SECURE © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

設定5) 動作確認(続き)

cisco XDR		⑦ ♀ A Tatsuya Kobayashi ∽ FTD-GUIDE-TEST	
=	Dashboards	C Full screen	
Control Center	Overview MyFTD-Dashboard		
Incidents			
-Q Investigate	Event Summary O Last Hour V ··· 2 ··· 2 ··· 2	Incident Promotion Reason ③ Last Hour V … 2 …	
☆ Intelligence >	📼 Total 대 👒 Intrusion 대 🖙 Malware 대 📼 Security Intelligence 대	Items	
↔ Automate >	3 3 0 0	User Promoted (0)	
Assets >		Security Intelligence Category: IP (0)	
Client Management		Security Intelligence Category: URL (0)	
		Intrusion Rules Category (3)	
Lo Administration		Malware Threat Score (0)	
	د م	2 ⁸	
	Intrusion Top Attackers	Talos IP Reputation O Last Hour 🗸 😷 😳	
	Secure Firewall	CISCO Security Services Exchange Devices Cloud Services Events Audit Log	🔘 🛠 🐥 🛛 Tatsuya Kobayashi 🗸
		Event Stream for FTD-GUIDE-TEST-JP	
	192.168.150.74 -	▼	
		AND OR Even Type InnusionElent X	Clear Save
		0 Rows Selected	Protocol Source IP Actions
		Utilinown Promoting 192.168.10.72 2207c9e9-b10a-4bb3-a593-2945e3e 2024-03-29 08:17:24 UTC 2024-03-29 08:17:28 UTC PROTOCOL-F	tcp 192.168.150.74 o
dealer annual		Utknown * Yes 192.168.10.72 630/93d3-9dba-475c-b11e-0db0/17b 2024-03-29 07:30:25 UTC 2024-03-29 07:30:29 UTC PROTOCOL-F	tcp 192.168.150.74 o 💿
		Utitinoum * Yes 192.168.10.72 630/93d3-9dba-475c-b11e-0db0/17b 2024-03-29 07-28:00 UTC 2024-03-29 07-28:03 UTC PROTOCOL-F	tcp 192.168.150.74 👁 💿
		Page Size: 25 V Total Entries: 3	

数分後、XDR の Dashboard にて Intrusion Event がカウントアップしていることを確認

cisco SECURE