XC CSD セットアップガイド

F5 ネットワークスジャパン合同会社

2024年03月12日

目次:

第1章	はじめに	1
1.1	XC Client-Side Defense(CSD) とは	1
1.2	XC Console での設定	2
1.3	Google Chrome を使った動作確認	7
1.4	XC Console での確認	10
1.5	運用監視方法....................................	13
1.6	<参考> CSD デモ動画	21

第1章

はじめに

このページでは、これらのオフィシャルなドキュメントの補足となる資料や、複数の機能を組合せてソリューションを実現する方法をご紹介いたします。

F5のオフィシャルなドキュメントはこちらにございます。

- AskF5: https://support.f5.com/csp/home
- F5 Cloud Docs: https://clouddocs.f5.com/
- F5 DevCentral (コミュニティ): https://devcentral.f5.com/
- F5 Distributed Cloud Tech Docs : https://docs.cloud.f5.com/docs/

本資料の画面表示や名称は資料作成時点の画面表示を利用しております。アップデート等より表示が若干異なる 場合がございます。

1.1 XC Client-Side Defense(CSD) とは

Client-Side Defense(以下、CSD) は、F5 Distributed Cloud Service(以下、XC) の1つとして提供可能な Web スキミ ング対策用セキュリティ SaaS 型サービスです。

クライアントのブラウザ上で動作する javascript の動作をリアルタイムに監視し、F5 が開発したシグナルに基づい て異常があった場合に管理者にアラートを上げ、データ流出のリスクを軽減することが可能となります。

CSD を使用すると、Web サイトにある「ユーザ名/パスワード」を入力するログイン画面や、クレジットカードの 情報を入力するページなどに情報奪取のための不正なコードを仕込んだり、javascript を改ざんして重要な情報を 抜き取ったりする挙動を検知し、不正とみなした接続先についてブロックすることが可能となります。

• 動作概要構成図





1.2 XC Console での設定

- 1. XC Console にアクセスし、以下の通り、 [Home] [Client-Side Defense] をクリックします。
- 2. [Dashboard]が表示されます。
- 3. 保護対象サイトの設定をします。

[Home] - [Client-Side Defense] - [Manage] – [Configuration]から、[Add Domain To Protect]をクリックします。

4. 対象サイトの [Root Domain]を追加し、 [Save and Exit]をクリックします。

Distribute Home	ed Cloud Console		Q Search			© Support ∨	(
Welc F5 Distrit managen	ome to the F5 I buted Cloud Console deliv nent services that can be	Distribu ers a set of used to solv	uted Cloud Console networking, security, and app e various use-cases.				
Comm	on services						
				Previe	ew	\$ 5 >	
Multi Conn Netwo clouds	-Cloud Network nect orking & security across s, edge and on-premises	>	Distributed Apps > Deploy apps in our global PoPs (REs) or your cloud/edge sites	Content Delivery Network Optimize asset delivery with content caching	>	DNS Management > Configure and manage primary or secondary DNS service	
E.			E	202		()	
Multi Conne edge Load	-Cloud App Connect act apps across clouds, and on-premises using Balancers	>	Web App & API Protection > Create a proxy and configure WAF, Bot, and API security services for your apps	DDoS & Transit Services Secure your infrastructure and apps against L3/L4 DDoS attacks	>	Bot Defense > Deploy bot mitigation for F5 BIG-IP and other 3rd party services	
0		ſ	Preview	Ø		R	
Appli Recog device applic	cation Traffic Insight gnize and monitor all clien es that access your ations	> t	Client-Side Defense > Monitor and mitigate fraudulent app requests at the client devices	Account Protection Reduce online fraud against web and mobile applications	>	Authentication Intelligence > Identify returning/known users and reduce authentication friction	

If is dealer, service Clear-Side Defense Im Monitoring Definer Script List Network Form Fields Im Manage Configuration A Maris Autors Autors Autors Autors Autors Autors Autors Script List Network Romain Beams Image Configuration Autors	6	Home > Client-Side Defense > System Dashboard	n > Monitoring			© Su	pport 🤟
Skinet-Side Defense Katter Needed Found & Milligated Found & Allowed Total Found Total Found <thte< th=""><th>Select service ~</th><th></th><th></th><th></th><th>Select Location ~</th><th>🕒 Auto-Refresh: Off 🗸 🦪 Refresh:</th><th>Jpdated ju</th></thte<>	Select service ~				Select Location ~	🕒 Auto-Refresh: Off 🗸 🦪 Refresh:	Jpdated ju
Monitoring banboard Script List Network Form Fields B lems Correct Science Since implemented Since implemented Since implemented Since implemented Manage Configuration B lems Last Seen Demain Category LeastBoor Science LeastBoor Science Configuration Manage Configuration ganalities.com Action Needed 1/125/2023 03:45:25 Search Engines https://shop.apac-ent.f5demos.com/ Notifications Alerts Juudit Logs webfaset.com Action Needed 1/125/2023 03:45:25 Search Engines https://shop.apac-ent.f5demos.com/ Partice Information Action Needed 1/125/2023 03:45:25 Unknown https://shop.apac-ent.f5demos.com/ Partice Information Action Needed 1/125/2023 03:45:25 Unknown https://shop.apac-ent.f5demos.com/ Partice Information Action Needed 1/125/2023 03:45:25 Business and Economy https://shop.apac-ent.f5demos.com/ Partice Information Action Needed 1/125/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Ipageretid.online Action Needed 1/125/2023 03:45:25 Computer and Internet Info https://shop.apac-ent	lient-Side Defense	Action Needed	Found & Mitigsted	Found & Allowed	Total Found	Transactions Consumed	
Dashed Script List Image	Monitoring	8 Since Nov 25, 2023	0	0	Since Implemented	203 Since Implemented	
Network Form Fields Domain Status Last Seen Domain Category Leastone Found Manage Configuration gaanitics.com - Action Needed 11/25/2023 03:45:25 Phishing and Other Frauds https://shop.apac-ent.f5demos.com/ Notifications Aderts Audri Logs - Action Needed 11/25/2023 03:45:25 Search Engines https://shop.apac-ent.f5demos.com/ Service Info Aderts - Action Needed 11/25/2023 03:45:25 Unknown https://shop.apac-ent.f5demos.com/ Gaanitis.com - Action Needed 11/25/2023 03:45:25 Unknown https://shop.apac-ent.f5demos.com/ Service Info Aderts - Action Needed 11/25/2023 03:45:25 Unknown https://shop.apac-ent.f5demos.com/ gaanitis.com - Action Needed 11/25/2023 03:45:25 Business and Economy https://shop.apac-ent.f5demos.com/ pixupiges.tech - Action Needed 11/25/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ ipwereid.online - Action Needed 11/25/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ ipwereid.online - Action Needed 11/25/2023 03:45:25 Com	Script List	9 items				Q Search	
Marage Configuration galallitic.com Action Needed 1/125/2023 03:45:25 Phishing and Other Frauds https://shop.apac-ent.f5demos.com/ Notifications Alerts Audit Logs • • • • • • • • • • • • • • • • • • •	Form Fields	Domain	Status	Last Seen	Domain Category	Locations Found	Actions
Configuration gstatcs.com Action Needed 11/25/2023 03:45:25 Search Engines https://shop.apac-ent.f5demos.com/ Notifications Alarts Audit Logs • Action Needed 11/25/2023 03:45:25 Phishing and Other Frauds https://shop.apac-ent.f5demos.com/ Specie Info Sporte • Action Needed 11/25/2023 03:45:25 Unknown https://shop.apac-ent.f5demos.com/ Specie Info Sporte • Action Needed 11/25/2023 03:45:25 Business and Economy https://shop.apac-ent.f5demos.com/ Intervention • Action Needed 11/25/2023 03:45:25 Business and Economy https://shop.apac-ent.f5demos.com/ Intervention • Action Needed 11/25/2023 03:45:25 Computer and Internet Security https://shop.apac-ent.f5demos.com/ Intervention • Action Needed 11/25/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Intervention • Action Needed 11/25/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Intervention • Action Needed 11/25/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Intervention • Action Needed 11/25/2023 03:45:25 Computer and Internet Info https://shop.apac	Manage	ganalitics.com	Action Needed	11/25/2023 03:45:25	Phishing and Other Frauds	https://shop.apac-ent.f5demos.com/	•••
Notifications Aleris Audit Logs evelfaset.com Action Needed 1/25/2023 03:45:25 Phishing and Other Frauds https://shop.apac-ent.f5demos.com/ Service Info About - Action Needed 1/25/2023 03:45:25 Unknown https://shop.apac-ent.f5demos.com/ Jesse - Action Needed 1/25/2023 03:45:25 Business and Economy https://shop.apac-ent.f5demos.com/ Jesse - Action Needed 1/25/2023 03:45:25 Computer and Internet Security https://shop.apac-ent.f5demos.com/ Jesse - Action Needed 1/25/2023 03:45:25 Computer and Internet Security https://shop.apac-ent.f5demos.com/ Jesse - Action Needed 1/25/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Jesse - Action Needed 1/12/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Jesse - Action Needed 1/12/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Jesse - Action Needed 1/12/2023 18:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Jesse - Action Needed 1/01/2023 18:45:25 Computer and Inter	Configuration	gstatcs.com	Action Needed	11/25/2023 03:45:25	Search Engines	https://shop.apac-ent.f5demos.com/	•••
Airris Audit Logs Fourtm.online - Action Needed 11/25/023 03:45:25 Unknown https://shop.apac-ent.f5demos.com/ Service Info - Action Needed 11/25/023 03:45:25 Business and Economy https://shop.apac-ent.f5demos.com/ About - Action Needed 11/25/023 03:45:25 Business and Economy https://shop.apac-ent.f5demos.com/ About - Action Needed 11/25/023 03:45:25 Computer and Internet Security https://shop.apac-ent.f5demos.com/ Igwereid.online - Action Needed 11/25/023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Igwereid.online - Action Needed 11/25/023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Igwereid.online - Action Needed 11/12/023 18:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Igwereid.online - Action Needed 11/12/023 18:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/	Notifications	webfaset.com	Action Needed	11/25/2023 03:45:25	Phishing and Other Frauds	https://shop.apac-ent.f5demos.com/	•••
Service Info About ganalitis.com Action Needed 11/25/2023 03:45:25 Business and Economy https://shop.apac-ent.f5demos.com/ Implement - Action Needed 11/25/2023 03:45:25 Computer and Internet Security https://shop.apac-ent.f5demos.com/ Implement - Action Needed 11/25/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Implement - Action Needed 11/25/2023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Implement - Action Needed 11/1/2023 18:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Implement - Action Needed 11/1/2023 18:45:25 Computer and Internet Info https://stodi.apac-ent.f5demos.com/ Implement - Action Needed 11/01/2023 18:45:25 Computer and Internet Info https://stodi.apac-ent.f5demos.com/	Alerts Audit Logs	fountm.online	Action Needed	11/25/2023 03:45:25	Unknown	https://shop.apac-ent.f5demos.com/	•••
Incom phup/ges.tech Action Needed 11/25/023 03:45:25 Computer and Internet Security https://shop.apac-ent.f5demos.com/ Igwereid.online Action Needed 11/25/023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Igwereid.online Action Needed 11/25/023 03:45:25 Computer and Internet Info https://shop.apac-ent.f5demos.com/ Igwereid.online Added to Mitigated List 11/11/2023 18:45:25 Computer and Internet Info https://arcadia.apac-ent.f5demos.com/ Igwereid.online Action Needed 11/01/2023 18:45:25 Computer and Internet Info https://arcadia.apac-ent.f5demos.com/	Service Info	ganalitis.com	Action Needed	11/25/2023 03:45:25	Business and Economy	https://shop.apac-ent.f5demos.com/	•••
Image: Index in the second of the s		pixupjqes.tech	Action Needed	11/25/2023 03:45:25	Computer and Internet Security	https://shop.apac-ent.fSdemos.com/	•••
Icom • Added to Miligated List 11/11/2023 18:45:25 Computer and Internet Info https://arcadia.apac-ent.f5demos.com/ Icom • Action Needed 11/01/2023 11:01:15 Computer and Internet Info https://bot-demo.apac-ent.f5demos.com/		jqwereid.online	Action Needed	11/25/2023 03:45:25	Computer and Internet Info	https://shop.apac-ent.f5demos.com/	•••
com Action Needed 11/01/2023 11:01:15 Computer and Internet Info https://bot-demo.apac-ent/5demos.com/		.con	Added to Mitigated List	11/11/2023 18:45:25	Computer and Internet Info	https://arcadia.apac-ent.f5demos.com/	•••
			om Action Needed	11/01/2023 11:01:15	Computer and Internet Info	https://bot-demo.apac-ent.f5demos.com/	•••

XC CSD セットアップガイド

6	Home > Client-Side Defense > System > Manage Configuration		🙋 💿 Support 🗸 🔘 🤟
Select service ~	Add Domain To Protect How to Inject JS (1) Sc	chedule a session 🛗	
Client-Side Defense Preview	40 items		Q Search
Monitoring	Root Domain	Time Added	Actions
Dashboard Script List	.cloud	10/28/2023 19:19:36	Test JS Injection
Network	.com	06/26/2023 13:56:07	Test JS Injection
A Manage		06/15/2023 15:14:48	Test JS Injection +
Configuration	org	03/13/2023 13:12:02	Test JS Injection ***
A Notifications	.net	01/24/2023 13:17:48	Test JS Injection ***
Alerts Audit Logs	.co.id	01/18/2023 13:55:43	Test JS Injection ***
For Documentati	JS	\subightarrow Reset All Fields	s Q Search ^ V X
New Domain to protect	Domain to protect • Root Domain ① f5se.com	×)	\sub Reset All Fields \land
Cancel and Ex	it		Save and Exit

• 参考) Root Domain は、eTDL(effective TLD) + 1の値でないと以下のようにエラーとなります。

For Documentati JS	
New Domain to protect Domain to protect	We found 1 error Field spec.protected_domain should be of Effective TLD plus one(acmecorp.com, acmecorp.co.xx), got www.f5se.co.jp in request. Show More
	Domain to protect Reset All Fields ∧ • Root Domain ① www.f5se.co.jp
Cancel and Exit	Save and Exit

5. 登録後、 [Configuration] に反映されていることを確認します。

6	Home > Client-Side Defense > System > Manage Configuration		🔎 🛛 🕲 Support 🗸 🔘 🗸
Client Side Defense	Add Domain To Protect How to Inject JS	Schedule a session 📋	Î
Client-Side Defense Preview	1 of 40 items		Q f5se × 🕸
Monitoring	Root Domain	Time Added	Actions
Dashboard Script List	f5se.com	02/08/2022 14:34:56	Test JS Injection

6. [How to Inject JS] をクリックすると、CSD JS が表示されます。

右の赤枠がスクリプトの内容となりますが、これを挿入する設定を行います。

6	Home > Client-Side Defense > System > Configuration	Manage			How to Inject JS	×
Select service v	Add Domain To Protect	How to Inject JS (3)	Schedule a session 📋		JS Tag Web App and API Protection	
Client-Side Defense					Learn more about enabling Client-Side Defense with a JS tag, 🖄	
	1 of 40 items				1. Locate the <head> tag on the webpages of the sites where you want Side Defense protection.</head>	Client-
Monitoring	Root Domain			Time Heled		
Dashboard	f5se.com			02/08/2022 14:34:56	 Copy the script tag below and paste it between the <head> and If there are other scripts or JS tags between the <head> and </head> tag</head> 	ad> tags. ags,
Script List					ensure that the CSD JS is the first one to load by placing it before any of	ther
Network						
Form Fields					<script src="https://us.gimp.zeronaugnt.com/imp_apg/js/volt-</th> <th></th>	
🤌 Manage						- 10
Configuration					3. Save your changes.	
A Notifications					4. Add Domain of the pages where you have injected JS to the list of pa	ges to
Alorte					protect. Once this step is complete, malicious third-party scripts for the	se pages
Alerta					will be detected and reported.	
Audit Logs						
③ Service Info About					 Use 'Test JS Injection' button on Configuration page to test if JS inject successful. 	tion was

- CSD JS の挿入方法は以下 2 パターンあります。
 - (1). XCのHTTPLBで設定する場合

CSD 保護が必要な対象 HTTP LB の設定にて、CSD 機能を有効化し、CSD JS を LB で挿入するように設定します。(サーバ側での設定変更不要)

[Home] - [Web App and API Protection] - [Manage] - [Load Balancers] - [HTTP Load Balancers] から対象の HTTP LB の右側 [Action] - [Manage Configuration] をクリックし、右上の [Edit Configuration] をクリックします。

左側タブの [Client-Side Defense] をクリックし、下図の [Client-Side Defense] を Disable から Enable に変更し、 [Edit Configuration] から [Insert JavaScript in All Pages] 選択し、 [Apply], [Save and Exit] をクリックします。

Documentation JSON		Q Search	~ ~ X	
adn HTTP Load Balancer http-lb-80	Client-Side Defense ①			
Metadata Domains and LB Type Origins	Client-Side Defense Policy ⊕ O Configure 1 Edit Configuration > P Reset Configuration			
			(
Documentation JSON			Q Search	~ ~ ×
orm Documentation JSON	JavaScript Insertion		Q. Search Show Advanced Fields	~ ~ ×
orm Documentation JSON ren ITTP Load Balancer http-lb-80	JavaScript Insertion • JavaScript Insertion ① Insert JavaScript in All Pages		Q Search Show Advanced Fields	~ ~ ×

(2). サーバ側で設定する場合

CSD 保護が必要なサイトの Web ページで<head> タグと </head> タグの間に先ほど XC Console

で確認した CSD JS をコピーし、挿入します。

<head> タグと </head> タグの間に他のスクリプトまたは JS タグがある場合は、CSD JS を他のスクリプトまたは JS タグの前に配置して、CSD JS が最初に読み込まれるように挿入してください。

注釈:

- JavaScript をすべてのページに挿入し、保護対象とすることを推奨(デフォルト値)しています。
- 理由は、データの取得とデータの流出が異なるページで起こりうる可能性があるためです。
- 例えば、悪質なスクリプトでは、フォームのあるページでフォームデータをキャプチャし、ローカルストレージや Cookie に保存することが可能です。その後、CSD が有効になっていないページで、スクリプトがこのデータを読み、悪意のあるドメインに送信するような攻撃もあるため、完全に保護するためには、全てのページで CSD を使用することを推奨しています。
- 7. 実際にパブリックにアクセスできるサイトへ CSD JS を挿入した場合は、[Test JS Injection] から CSD JS が 動作しているか確認できます。

G	Home > Client-Side Defense > System Configuration	m > Manage				e 6) Support 🗸 🔘 🗸
Select service ~	Add Domain To Protect	How to Inject JS	Schedule a session 📋				î
Client-Side Defense	1 of 40 items					Q f5se	×
Monitoring	Root Domain			Time Added	_		Actions
Dashboard Script List	f5se.com			02/08/2022 14:34:56		Test JS Injection	
Test JS Injection			×				
Learn more about how	to test the JS injection.	2					
Paste the URL of a page JS injection.	e that is within the doma	iin f5se.com belt w	and test the				
https://example.com							
Test JS Injection							

なお、後述の Google Chrome を利用したテストではクライアント側ブラウザで CSD JS を挿入しているため [Test JS Injection] はエラーとなります。

1.3 Google Chrome を使った動作確認

1. クライアント PC で Google Chrome ブラウザを起動します。右上から [シークレットモード] で起動させます。

☆ 🛛	👼 シークレット 🔋
新しいシークレット タブ	Ctrl+T
新しいシークレット ウィンドウ	Ctrl+Shift+N

2. 右上から [その他のツール] - [デベロッパー ツール]をクリックします。



3. [Sources] – [Overrides] - [+ Select folder for overrides]をクリックします。

Elements Console	Sources	Network	Performance	Memory	Application	Security	Lighthouse	>>
Page Overrides >>	: 🖸							Þ
+ Select folder for overrides								
				Ctrl + P	Open file			
			Ctrl +	- Shift + P	Run commar	ıd		

4. 任意のフォルダを作成し、[フォルダーの選択]をクリックします。

◎フォルダーの選択						×
← → ~ ↑ 🖡 > PC	» ドキュメント » CSD-JS	~	ð X	つ CSD-JSの検	索	
整理・ 新しいフォルダー					•	?
OneDrive - F5 Net	名前	^		更新日時		種類
S PC		検索条件に一致	改する項目は	ありません。		
🧼 ネットワーク						
Ý	<)
フォルシ	≠–: CSD-JS		_			
			フォル	ダーの選択	キャンセル	

5. 以下のようにフォルダが作成されていることを確認します。

Elements	Console	Sources	Network
Page Overrides >>	•	•	
Enable Local Override	s Ø		
CSD-JS]	

6. 対象 URL にアクセスし、[Network] タブをクリックします。対象の通信を選択し、右クリックで [Override content]を選択します。

Elemen	nts Console Sources	Network Pe	rformance
Ø	. 🗌 Preserve log 🛛 🗹 D	isable cache No f	hrottling
Filter	Invert 🛛	Hide data URLs	Hide ext
All Doc JS Fe	tch/XHR CSS Font Img	Media Manife	st WS
500 ms 1000	ms 1500 ms 2000 ms	2500 ms 3	000 ms
			" í `-
Name		Status	Type
arcadia.apac-	0	200	docum
common.js?n	Open in Sources panel	:00	script
🖸 common.js?si	Open in new tab	200	script
🙂 volt-f5_apac_	Clear browser cache	200	script
🗹 bootstrap.mii	Clear browser cookies	:00	stylesh
css?family=Re	Copy	▶ 200	stylesh
🛛 css?family=La		200	stylesh
font-awesom	Block request URL	200	stylesh
🗹 owl.carousel.c	Block request domain	:00	stylesh
owl.theme.cs	Sort By	► 200	stylesh
🛛 magnific-pop	Header Options	▶ 200	stylesh
Style.css		200	stylesh
47 requests	Override content	Finish: 6.0	3 s DOM
: Console	Show all overrides		
🗈 🖉 top	Save all as HAR with conte	nt	
	Save as		

7. [Sources] – [Overrides]に戻ると作成したフォルダ配下に対象サイトのトップページ、本書では[index.html]が表示されます。



8. CSD JS が最初に読み込まれるように、CSD JS と不審なドメインに対する JS スニペットを挿入します。

Elements Console Sources	A Network Performance Memory Application Security Lighthouse >>
Page Overrides >> :	index.html* ×
✓ Enable Local Overrides	html
	<html lang="en"></html>
* 🗋 C3D-13	<pre>kneadxcscript src= /common.jsrmatcher x/scriptxcscript src= /common</pre>
arcadia.apac-ent.f5demos.com	amoto chancot-"utf 8">
*index.html	<pre>(meta name="viewnort" content="width=device-width initial-scal())</pre>
	<pre><meta content="" name="description"/></pre>
8	<pre><meta content="" name="author"/> CSD JS </pre>
9	
10	<pre><script bootstrap.min.css"="" css="" rel="stylesneet" src="https://us.gimp.zeronaught.com/ imp apg /is/vol</pre></td></tr><tr><td>11</td><td><script>(function() { var s = document.createElement('script');</td></tr><tr><td>12</td><td></td></tr><tr><td>13</td><td><title>Arcadia Finance</title> 不審なドメインに対する 1</td></tr><tr><td>14</td><td></td></tr><tr><td>15</td><td><! Bootstrap></td></tr><tr><td>16</td><td><pre><link nref="></script></pre>

<不審なドメインに対する JS スニペット サンプル> <script>(function() { var s = document.createElement('script'); var domains = [..., "ganalitis.com", "ganalitics.com", "gstatcs.com", "webfaset.com", "fountm.online", ..., "pixupjqes.tech", "jqwereid.online"]; for (var i = 0; i < domains.length; ++i) { s.src_ ...= 'https://' + domains[i]; } })();</script>

9. 最後に保存することで、 [*index.html]から [index.html]になります。



10. 対象サイトに数回アクセスを実施します。

Arcadia Finance × +					× -	a ×
← → C () arcadia.apac-ent.f5demos.com/index.html				₫ _E	☆ 🔲 ಿ ୬-୭	b≫F :
f y G+ ⊚ P Walcome to Arcodia Einance wakeita wa hawa avaartise in mananing	Elements Console Sources O Preserve log Disal	▲ Network Performance Memory ole cache No throttling ▼ つう 1	Application Security	Lighthouse >>>	٤ 🛦	8 : × ®
your finances!!!	Filter Invert His All Doc JS Fetch/XHR CSS Font Img	de data URLs 📄 Hide extension URLs Media Manifest WS Wasm Other	Blocked response cookie	es 🗌 Blocked requests	3rd-party requests	
	500 ms 1000 ms	1500 ms 2000	ms 2500 ms	3000 ms	3500 ms	
	Name	Status Type	Initiator	Size Time	Waterfall	
	common.js?matcher	200 document 200 script	Other index.html:2	31.3 kB 290 ms 516 B 11 ms		Â

次章で XC CSD で、検知できているかを確認します。

1.4 XC Console での確認

1. 対象アクセスから 5 分以上経過後に [Home] - [Client-Side Defense] - [Dashboard] で確認すると、不正な ドメインへのアクセスを検知していることが確認できます。

G	Home > Client-Side Defense > System > Mon Dashboard	itoring			🤨 🛛 🕲 Sup	xport ~ (0) ~
Select service ~				Select Location 🔗	🕒 Auto-Refresh: Off 🗸 🛛 💭 Refresh: Up	dated 2 min ago
Client-Side Defense Preview	Action Needed	Found & Mitigated	Found & Allowed	Total Found	Transactions Consumed	
Monitoring	Since Nov 27, 2023	0	U	Since Implemented	Since Implemented	
Dashboard Script List Network	9 items				Q. Search	
Form Fields	Domain	Status	Last Seen	Domain Category	Locations Found	Actions
A Manage	ganalitics.com	Action Needed	11/27/2023 17:15:25	Phishing and Other Frauds	2 Locations	
Configuration	pixupjqes.tech	Action Needed	11/27/2023 17:15:25	Computer and Internet Security	2 Locations	
A Notifications	jqwereid.online	Action Needed	11/27/2023 17:15:25	Computer and Internet Info	2 Locations	
Alerts Audit Logs	gstatcs.com	Action Needed	11/27/2023 17:15:25	Search Engines	2 Locations	
(i) Service Info	webfaset.com	Action Needed	11/27/2023 17:15:25	Phishing and Other Frauds	2 Locations	
About	fountm.online	Action Needed	11/27/2023 17:15:25	Unknown	2 Locations	
	ganalitis.com	Action Needed	11/27/2023 17:15:25	Business and Economy	2 Locations	de
	.com	Added to Mitigated List	11/11/2023 18:45:25	Computer and Internet Info	https://arcadia.apac-ent.f5demos.com/	
	.com	Action Needed	11/01/2023 11:01:15	Computer and Internet Info	https://bot-demo.apac-ent.f5demos.com/	

2. [Dashboard]では [Auto-Refresh]にて5分または15分でページの自動更新が可能です。

G	Home > Client-Side Defense > System Dashboard	n > Monitoring			Č	Support v 🔘 v
Select service				Select Location \vee	Auto-Refresh: Off	
Client-Side Defense Proview	Action Needed	Found & Mitigated	Found & Allowed	Total Found	Off Every 5 Min	onsumed
Monitoring	8 Since Nov 27, 2023	0	0	Since Implemented	Every 15 Min	rted

3. [Domain]をクリックすると、Risk Score など詳細情報が確認可能です。

AI/ML による Risk Score 判定が High Risk に分類されると、 [Status]が [Action Needed]表示となるため、意図するドメインへの通信の場合は [Add To Allow List]へ、意図しないドメインへの通信の場合は [Add To Mitigate List]へ追加します。

- 4. 意図するドメインへの通信許可の設定
 - (1). 対象 Domain を Allow List に追加します。

対象 Domain の一番右の [Actions] - [...] から [Add To Allow List] をクリックします。

(2). 警告を確認し、 [Add] を クリックで Allow List への登録は完了です。

6	Home > Client-Side Defense > Syste	em > Monitoring			ganalitics.com	ì	×
Client-Side Defense	Action Needed	Found & Mitigated	Found & Allowed	Sel Total Fc	Status Action Needed Risk Score ①	1	
Monitoring Dashboard Script List	8 Since Nov 25, 2023 9 items	0	0	9 Since In	100/100 Details First Seen	11/30/2022 18:30:08	
Network Form Fields	Domain ganalitics.com	Status Action Needed 	Last Seen 11/25/2023 03:45:25	Domain Category Phishing and Other Frau	Last Seen Action Taken Risk reasoning Young Domain Age	11/25/2023 03:45:25 ie	
Configuration	pixupjqes.tech	Action Needed	11/25/2023 03:45:25	Computer and Internet !	Protected Pages https://shop.apac-	-ent.f5demos.com/ 🖄	
Alerts Audit Logs	webfaset.com	Action Needed	11/25/2023 03:45:25	Phishing and Other Frau	Associated Script	ts ① -ent.f5demos.com/	
6	Home > Client-Side Defense > Syste Dashboard	em > Monitoring				٩	© Support → _
Select service Client-Side Defense				Sele	ect Location 🖂	\bigcirc Auto-Refresh: Off \lor \bigcirc 1	Refresh: Updated 4 min ago
Proview Mail Monitoring Dashboard	Action Needed 8 Since Nov 25, 2023	Found & Mitigated	Found & Allowed	Total FG 9 Since Ir	ound	Transactions Consu 203 Since Implemented	umed

	8	0	0	9	203	
Monitoring	Since Nov 25, 2023			Since Implemented	Since Implemented	
Dashboard						
Script List	9 items				Q. Search	-
Network	Bassala	0 to the	1	Denvelo Osterene	Leasting Friend	A
Form Fields	Domain	Status	Last Seen	Domain Category	Locations Found	Actions
Manage	ganalitics.com	Action Needed	11/25/2023 03:45:25	Phishing and Other Frauds	https://shop.apac-ent.f5demos.com/	
Configuration	pixupjqes.tech	Action Needed	11/25/2023 03:45:25	Computer and Internet Security	https://shop.apac-ent.f5	w List
Notifications	fountm.online	Action Needed	11/25/2023 03:45:25	Unknown	https://shop.apac-ent.f5demos.com/	

Add To Allow List	
Are you sure you want to add this d	omain to the allow list? Cancel

- (3). [Monitoring] [Network] [Allow List]から登録内容を確認可能です。
- 5. 意図しないドメインへの通信遮断の設定
 - (1). 対象 Domain を Mitigate List に追加します。

対象 Domain の一番右の [Actions] - [...] から [Add To Mitigate List] をクリックします。

- (2). 警告を確認し、 [Add] をクリックで Mitigate List への登録は完了です。
- (3). [Monitoring] [Network] [Mitigate List]から登録内容を確認可能です。

G	Honte > Client-Side Defense > System > Monitoring Network		🧶 🔘 s	Support v 🔘 v
Select service Client-Side Defense (Proviso)	All Domains Mitigate List Allow List			Î
hal Monitoring	1 item		Q Search	*
Dashboard	Domain	Time Added		Actions
Network	ganalitis.com	11/27/2023 17:02:05		
Form Fields				

G	Home > Client-Side Defense > System Dashboard	iem > Monitoring			🧶 🛛 💿 Support 🗸 🔘 🗸
Select service ~				Select Location 👒	\bigcirc Auto-Refresh: Off \checkmark \bigcirc Refresh: Updated 4 min ago
Client-Side Defense Preview	Action Needed	Found & Mitigsted	Found & Allowed	Total Found	Transactions Consumed
Monitoring	8 Since Nov 25, 2023	0	U	Since Implemented	203 Since Implemented
Script List	9 items				Q Search \$
Form Fields	Domain	Status	Last Seen	Domain Category	Locations Found Actions
Anage	ganalitics.com	 Action Needed 	11/25/2023 03:45:25	Phishing and Other Frauds	https://shop.apac-ent.f5demos.com/
Configuration	pixupjqes.tech	Action Needed	11/25/2023 03:45:25	Computer and Internet Security	https://shop.apac-ent.f5
	fountm.online	Action Needed	11/25/2023 03:45:25	Unknown	https://shop.apac-ent.f5demos.com/ ***

Add To Mitigate List
Are you sure you want to add this domain to the mitigate list?
Cancel

ſ	Home > Client-Side Defense > System > Monitoring Network		🕐 💿 Support 🗸 🔘
Select service V	All Domains Mitigate List Allow List		
Client-Side Defense Preview	③ Add Domain		
had Monitoring	5 items		Q Search
Dashboard	Domain	Time Added	Actions
Network		07/18/2023 15:22:58	
Form Fields		04/13/2023 16:27:28	***
🖉 Manage		03/23/2023 13:55:06	***
Configuration		05/26/2022 11:16:21	•••
O Notifications		03/17/2022 16:18:42	•••

1.5 運用監視方法

監視時は検出スクリプト一覧から脅威内容を確認し、スクリプトが意図しないドメインヘアクセスしていないか確 認することと、意図しない Form Field の読み取りがないかを確認します。

検出スクリプト一覧

[Home] - [Client-Side Defense] - [Monitoring] - [Script List]から保護対象にて検出したスクリプトの一 覧を表示可能です。各スクリプトをクリックすることで詳細確認が可能です。

Status の状態の説明は下表のとおりです。

NA - No Action Needed	該当スクリプトでは不審な点を未検出		
Resolved - No Action	該当スクリプトでいくつかの不審な動作を検出したが、ユーザがすでにアクショ		
Needed	ンを実行済		
AN - Action Needed	注意が必要なスクリプトで不審な動作を検出		

検出したスクリプトがどのドメインへ通信を行っているか、どの Form Field の値を読み取ろうとしているかの 振る舞いが確認可能です。

意図する通信、意図しない通信のハンドリング

前章 [4. XC Console での確認] の 4 項,5 項 をご参照ください。

Form Field の読み取りを抑止

(1). [Home] - [Client-Side Defense] - [Monitoring] - [Form Fields]から特定のスクリプトによって読み
 取られる全フォームフィールドを確認することが可能です。

(2). 特定の Form Field に対して、その Field を読み取ろうとする Script があった際に、Risk Score を "High Risk "としてマークし、機微データへのアクセスリスクを管理することが可能です。

該当 Field の [Actions]から [Mark as Sensitive]を選択し、適用することで、当該 Field を機微データ として取り扱うことが可能です。

(3). Form Field を読み取るスクリプトに対する Mitigation Action として、意図する Form Field の読み取りの場合は [Allow Read]へ、意図しない Form Field の読み取りの場合は [Block Read]へ追加することが可能です。

[Home] - [Client-Side Defense] - [Monitoring] - [Script List]から[Form Fields Read]に数値が記録 されているスクリプトを確認し、[Form Fields Read]の数字を選択します。

(4). 該当 Script が読み取っている Form Filed の一覧が表示され、それぞれの Risk Level を確認可能です。

前述の [Mark as Sensitive] にて該当 Field を機微データとして登録しておくと、この Field を読み取ろうとする Script は "High Risk" として記録されます。

G	Home > Client-Side Defense > System > Monitor Script List	ing					2	O Support	~ @ ~
Select service ~						🕒 Auto-Re	fresh: Off 🗸 🕒 Li	ast 7 days 🗸 📿	Refresh
Client-Side Defense Preview	6 items								8
Monitoring	Add Filter Script Name	Status	Risk Level	Last Seen	Locations Found	Network Interactions	Form Fields Read	New Behaviors	
Dashboard Script List Network		AN - Action Needed	High Risk	11/28/2023 14:15:36		Z	0	7	
Form Fields		AN - Action Needed	High Risk	11/27/2023 17:00:28		Z	0	7	
Manage Configuration		AN - Action Needed	High Risk	11/25/2023 03:45:25		Z	0	0	
O Notifications		NA - No Action Needed	Low Risk	11/28/2023 15:28:34	2 Locations	0	1	0	
Alerts Audit Logs		NA - No Action leeded	Low Risk	11/24/2023 16:24:56	3 Locations	0	1	0	
Service Info About		N - No Action Net Ved	Low Risk	11/23/2023 15:17:51	4 Locations	0	1	0	



G	Home > Client-Side Defense > System > Monitoring Form Fields				۹	() Support v () v
Select service				🕒 Auto-Refresh: Off 👒	I Last 7 days ∨	resh: Updated just now
Preview	2 items				Q Search	\$
Monitoring	Form Field	Last Read Time	Associated Scripts	Locations Found	Analysis	Actions
Dashboard Script List	input	11/28/2023 16:10:55	2 Scripts	6 Locations	Not Sensitive (by system)	
Network Form Fields	_w_simile	11/24/2023 16:24:56		3 Locations	Not Sensitive (by system)	

A	Home > Client-Side Defense > System	m > Monitoring				1 Support v (O)
	Form Fields					0
Select service V				④ Auto-Refresh: C	Off \sim 🕒 Last 7 days \sim	\bigcirc Refresh: Updated 36 min ago
Client-Side Defense Preview	2 items					Q Search 🔯
Monitoring	Form Field	Last Read Ti	ime Associated Scripts	Locations Found	Analysis	Actions
Dashboard Script List	input	11/28/2023	3 16:10:55 2 Scripts	6 Locations	Not Sensitive (by s	ystem)
Network Form Fields	_w_simile	11/24/2023	3 16:24:56	3 Locations	Not Sensitive (by s	Mark as Sensitive
Are you sure t Sensitive?	hat you want to marl	k the form field inpu Cancel	ut as			
Are you sure t Sensitive?	hat you want to mari	k the form field input	ut as			🖉 @ Support ~ 🔘
Are you sure t Sensitive?	hat you want to mar hat you want to mar	k the form field input	ut as		⊙ Auto-Refresh: Off ∽	ر العد 7 days ب المعالي Refresh المعالي معالي المعالي معالي المعالي معالي معالي معالي معالي معالي معالي معالي معالي معالي معالي معالي معالي معالي معالي معالي معالي معا
Are you sure t Sensitive?	hat you want to mark	k the form field input	ut as		⊙ Auto-Refresh: Off ∨	کو کې
Are you sure t Sensitive?	hat you want to mari	k the form field inpu Cancel	ut as		⊙ Auto-Refresh: Off ~	Image: Support → Image
Are you sure t Sensitive?	hat you want to mari	k the form field input Cancel	ut as pply RiskLevel Last Seen	Locations Found	Auto-Refresh: Off ~ Auto-Refresh: Off ~ Auto-Refresh: Off ~	Image: Support Image: Support Image: Support Image: Support <
Are you sure t Sensitive?	hat you want to mari	k the form field input Cancel (A Monitoring Monitoring Status AN - Action Needed	It as pply	Locations Found Network in	© Auto-Refresh: Off ~ Iteractions Form Fields Read	Image: Support Image: Support Image: Support Image: Support <
Are you sure to Sensitive?	hat you want to mark	k the form field input Cancel A Montoring Montoring AN - Action Needed AN - Action Needed	Risk Level Last Seen High Risk 12/21/202 High Risk 12/21/202	Locations Found Metwork in Documentary Statements of Statem Statements of Statements	Auto-Refresh: Off ~ teractions Form Fields Read Z Z	Image: Support Image: Support Image: Support Image: Support <

これらの Script による該当 Field の読み取り可否を確認の上、Mitigation Action として [Allow Read] もしくは [Block Read]を設定可能です。

Alert の通知設定

CSD で発生したアラート通知の設定として、 [Alert Receivers]ではどこに対し Alert Log を飛ばすかを設 定し、 [Alert Policies]では何の Alert Log を飛ばすか (ここでは CSD Alert Log)を設定し、最後にそれら の設定内容を [Active Alert Policies]として有効化することで、CSD アラート通知を設定可能です。

(1). Alert Receivers の設定

Home] - [Audit Logs & Alerts] - [Alerts Management] - [Alert Receivers] にて、[Add Alert Receiver] を選択します。

Receiver は下記から選択することが可能です。(2023/12 時点)

Slack · PagerDuty · OpsGenie · Email · SMS · Webhook

設定入力後、[Save and Exit]をクリックします。 [Alert Receiver]の設定が追加されます。

(2). Alert Policies の設定

ſ

Home > Client-Side Defense > System > Monitoring Script:	g → <u>Script List</u>	~		🧐 💿 Support 🗸 🔘 🗸
Overview Network Form Fields		\odot Auto-Refresh: Off \sim	ⓒ Last 7 days < 🖉 Refresh	⊘ Allow Read ⊘ Block Read
7 items				Q Search \$
Form Field	Risk Level	Last Read Time	Read Sowed/Blocked	
password	📕 🔸 High Risk	12/21/2023 20:21:16		
userName	📕 🔸 High Risk	12/21/2023 20:21:16	1.1	
password:nth-child(1)	📕 🔸 High Risk	12/21/2023 20:15:16	-	
username:nth-child(1)	📕 🔸 High Risk	12/21/2023 20:15:1	-	
email	📕 🔸 High Risk	12/21/2011 20:06:06		
password_confirmation	📕 🔸 High Risk	2/21/2023 20:06:06	-	
btn.btn-primary.btn-block.btn-lg	Low Risk	12/21/2023 20:06:06		
Allow script				
Are you sure you want to allow scri	ipt to read all form fields? Cancel			



6	Home > Audit Logs & Alerts > Alerts Management Alert Receivers			Sup	port v 🔘 v
Select service	Add Alert Receiver				🗯 Refresh
Audit Logs & Alerts	14 items			Q Search	\$
Alerts	Name	Namespace	Туре	Details	Actions
Audit Logs		system	🖂 Email		
🤌 Alerts Management	> D	system	🖾 Email		
Active Alert Policies	›	system	🖂 Email		
Alert Receivers		shared	🖂 Email		

Form Documentation JSON		Q Search A V X
New Alert receiver	Metadata 0 •Name 0	
Metadata Receiver	Labels ①	
	Add Label	
	Description ()	
	* Receiver ①	
	∩"¢ Slack ^	
	Slack Default Send alert notifications to Slack	
	PagerDuty Send alert notifications to PagerDuty	
	OpsGenie Send alert notifications to OpsGenie	
	Email Send alert notifications as Email	
	SMS Send alert notifications as SMS	
	Webhook Send alert notifications to Webhook	
Cancel and Exit		Save and Exit

[Home] - [Audit Logs & Alerts] - [Alerts Management] - [Alert Policies] にて、[Add Alert Policy] を選択します。

ſ	Home > Audit Logs & Alerts > Alerts Management Alert Policies		◎ Support 、 ○ 、
Select service V	Add Alert Policy		<i>G</i> Refresh
Audit Logs & Alerts			
A Notifications	7 items		Q Search
Alerts	Name	Namespace	Actions
Audit Logs		system	
🤌 Alerts Management		shared	
Active Alert Policies		system	***
Alert Policies		shared	

Alert Policy 設定では、先ほど設定した Alert Receiver の設定を紐づけ、Policy Rules から [Security-CSD]を選択します。

Form Documentation JSON		
New Alert policy Metadata Alert Receiver Configuration Policy Rules	Metadata	
	Alert Receiver Configuration	
	Order *Alert Receivers ① Ⅲ 1 1 ☐ ☐	Actions
	O Add	tem
	Policy Rules	
Cancel and Exit		Save and Exit
* Policy Rules ⊕	There are no items added yet. Start by adding first item.	

以下の通り、[Security Alerts]と[Groups]を選択します。 + Security Alerts : Matching Group + Groups : Security-CSD

Route		-	$\stackrel{>}{\sim}$ Reset All Fields	Show Advanced Fields 🔵 🔿
Select Alerts (1)		•		
¬ [*] Matching Group	<i>₽</i> ° ∨			
Groups ③				
Security-CSD	C × ~			
* Action ①	~			

[Show Advanced Fields]をクリックすることで、通知間隔を調整可能です。

設定入力後、[Save and Exit]をクリックすることで、[Alert Policy]の設定が追加されます。

(3). Active Alert の設定

Home] - [Audit Logs & Alerts] - [Alerts Management] - [Active Alert Policies] にて、[Select Active Alert Policies] をクリックします。

[Add Item]をクリックします。

先ほど作成した Alert Policy を選択し、[Save and Exit]をクリックします。

ſ

Route	Show Advanced Fields 💽 🔨
Select Alerts 🚯	
ිරී Matching Group ∨	
Groups ()	
Security-CSD × v	
* Action ①	
\Im Send \checkmark	
Dolicy Pule Notification Parameters ()	
M Not configure >	
Notification Parameters Notify Interval For a Alert 4h ×	^
Notification Grouping	hightarrow Reset All Fields Show Advanced Fields 🥥 $hightarrow$
* Group Notifications By 🚯	
T\$ F5XC Defined Group C · ∨	
Wait to Notify ①	
30s ×	
Notify Interval for a Group	
1m ×	

Form Documentation JSON		$\stackrel{>}{_\sim}$ Reset All Fields	Q Search x]
New Alert policy Metadata Alert Receiver Configuration Policy Rules	Metadata © **ame © Labele © Add Label Description ©			
	Alert Receiver Configuration	⊖ Reset All F	Fields Show Advanced Fields 🔿 🔨	
	Order *Alert Receivers ①		Actions	
	Image:		***	
	Policy Rules O Configured Edit Configuration P Reset Configuration			
Cancel and Exit			Save and Exit	ה

XC CSD セットアップガイド

6	Home > Audit Logs & Alerts > Alerts Mar Active Alert Policies	nagement	③ Support 、 ②、
Select service V	Select Active Alert Policies		💭 Refresh
Audit Logs & Alerts	0 items		Q, Search 🕸
Alerts	Name	Namespace	Tenant
Audit Logs		No dat	ata found
Alerts Management Active Alert Policies Alert Policies			
Alert Receivers			

Now	Order Alert Policies ()	Actions
Alert Policies	There are no items added yet. Start by adding first item.	
	O Add Item	

New	Order Alert Policies ①	Actions
Select Active Alert Policies	1 1 V	•••
	Add Item	
Cancel and Exit		Save and Exit

Active Alert Policy として追加されます (Namespace は "system" として作成されます)

G	Home > Audit Logs & Alerts > Alerts Management Active Alert Policies			Support v
Select service ~	⊙ Select Active Alert Policies			💭 Refresh
Audit Logs & Alerts	2 items		Q Search	1
Alerts	Name	Namespace	Tenant	
Audit Logs		system		
🤌 Alerts Management		shared		
Active Alert Policies Alert Policies Alert Receivers				

以上の設定により、CSD アラートが発生した際に、指定した Receiver に対してアラート通知を飛ばす ことが可能です。

これで、XC CSD のセットアップガイドは終了となります。

1.6 <参考> CSD デモ動画

F5 XC CSD のデモを公開しています。

注釈: 本資料の画面表示や名称は資料作成時点の画面表示を利用しております。アップデート等より表示が若干異 なる場合がございます。