

راهنمای مقاومسازی سامانه امنیت نقاط پایانی بیتدیفندر

بر اساس توصیهنامه مـرکـز مـاهـر



مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانهای کشور (ماهر) توصیهنامهای برای امنسازی سامانههای فناوری اطلاعات در مقابل تهدیدات سایبری احتمالی همزمان با ۱۳ آبان ماه منتشر کرده که در آن طی ۱۰ بند مواردی جهت مقاومسازی سامانهها ارائه شده است.

شرکت مهندسی شبکه گستر همراستا با توصیهنامه فوق اقدام به انتشار راهنمای مقاومسازی محصولات خود مطابق با بندهای مورد اشاره مرکز ماهر کرده است.

در این راهنما نحوه بررسی تنظیمات سامانه امنیت نقاط پایانی بیتدیفندر در جهت اجرای توصیههای مرکز ماهر ارائه گردیده است.

بهروزرسانی سیستم عامل و نرمافزارها

امکان بهروزرسانی هسته سیستم عامل سرور و نسخه نرمافزاری محصولات سازمانی بیتدیفندر در کنسول مدیریتی GravityZone فراهم است. جهت بررسی نسخه، باید در کنسول مذکور به بخش Configuration | Update مراجعه کرده و هر دو سربرگ GravityZone Roles و Components را مورد بازبینی قرار داد.

Bitdefender ⁱ GravityZone					Weicome	e, SGC 🕓	?	2					
Application Inventory	GravityZone Roles Component	s											
Packages	Current Status												
Tasks	 Your console is up to date. 												
Policies	View changelog												
Assignment Rules	Enable automatic update	Enable automatic update											
Reports	Infrastructure												
Quarantine	(2) Refresh												
Accounts	Virtual appliance	IP	Roles	Current Version	Available version	Status							
User Activity	Q	Q	•	Q	Q			•					
Configuration	gzva	172.16.5.118	Database Server	6.3.7-7	N/A	Updated	(
Update	gzva	172.16.5.118	Update Server	6.3.7-7	N/A	Updated							
License	gzva	172.16.5.118	Communication Server	6.3.7-7	N/A	Updated							

شکل ۱: وضعیت بهروزرسانی اجزای ابزار مدیریتی GravityZone

Bitdefender GravityZone					Welcome, SG	c v (?	
Application Inventory	GravityZone Roles Components						
Packages	Settings Settings Check for updates		Product changelog				
Tasks	Product	Packa	ages				
Policies	BEST (Windows)						
Assignment Rules	BEST (Windows Legacy)	R	Actions (2) Refresh				
Reports	Endpoint Security for Mac		Version	State	Action Status	Published	
Quarantine	BEST (Linux)		q	•	•		
Accounts	Security Server (VMware, Nutanix)		6.6.5.82	Not downloaded	Downloading	N/A	
User Activity	Security Server (Microsoft Hyper-V)		6.6.3.61	Published	Published successfully	05 August 2018 -	Present
Configuration	Security Server (Citrix XenServer)						
Update	Security Server (ESXi standalone)						
License							
				First Page	of 1 → Last Page		2 items

شکل ۲: وضعیت بهروزرسانی نرمافزارهای قابل توزیع در سطح شبکه توسط ابزار مدیریتی GravityZone

بهمنظور جلوگیری از وجود هرگونه نقطه ضعف امنیتی بر روی سرور مدیریتی و همچنین بستههای نرمافزاری نصب شده بر روی دستگاههای تحت یوشش، نصب بهروزرسانیها در اولین فرصت ممکن توصیه میشود.

همچنین جهت بررسی وضعیت بهروزرسانی دستگاهها و ماشینهای تحت پوشش GravityZone میتوان از نماهای Endpoint Protection Status در بخش Dashboard ابزار مدیریتی استفاده کرد.

Bitdefender GravityZone	 Add Portlet 	Move Portlets			Welcome, SG	• •	?	P
Dashboard	3-10-14	3-10-14 3-10-14 3-10-14	8-10-14 8-10-14 8-10-14	2-10-14				
Network	2018	2018 2018 2018	2018	2018				
Application Inventory								
Packages					Scan infected targets			
Tasks				0 0 0		~	~	
Policies	Computers	s - Top 10 Detected M	alware	(* %) ×	Computers - Endpoint Protection Status	0	0	×
Assignment Rules					5 -			
Reports								
Quarantine								
Accounts		No client has been installed	or no relevant event has been re	corded yet.				
User Activity								
Configuration					0			
Update					Antimalware Update Status Online		Managed	
License								
	Page 1 of 5					Jump to	page:	1

شکل ۳: وضعیت بهروزرسانی ضدویروس دستگاهها و ماشینهای تحت پوشش GravityZone (فلش آبی رنگ)

Bitdefender GravityZone						Welco	ame, SGC \vee 🕜	٠
Dashboard	Update Status Report							
Network	Generated by:	admin						
Application Inventory	On:	03 October 2018	3, 10:43:28					
Packages	Recurrence:	Now				The second se		
Tasks	Targets:	Computers and	Virtual Machines			Opdated		
Policies								
Assignment Rules								
Reports								
Quarantine	🕃 Update							
Accounts	Endpoint Name		IP	Update status	Last update	Product Version	Signatures Version	
User Activity		Q	Q				Q	
Configuration	DESKTOP-INKGKER		172.16.5.207	Updated	03 October 2018, 10:24:05	6.6.5.82	7.77654 (11509752)	
Update	BIT-AC-CLIENT		172.16.5.252	Updated	03 October 2018, 09:15:21	6.6.5.82	7.77654 (11509752)	
License								
				First Page - Page 1 of 1 -	- Last Page 20 +			2 items

این جزییات در گزارش Update Status در بخش Reports نیز قابل مشاهده است.

شکل ۴: گزارش Update Status در بخش Reports

در صورت عدم دریافت بهروزرسانی توسط هر یک کامپیوترهای تحت پوشش این سامانه، پس از اطمینان از نکات زیر، موضوع از طریق شماره تلفن ۴۲۰۵۲ یا سامانه خدمات پس از فروش و پشتیبانی شرکت مهندسی شبکه گستر (MY) به نشانی https://my.shabakeh.net به گروه پشتیبانی شرکت مهندسی شبکه گستر اعلام شود:

- فراهم بودن ارتباط شبکهای مناسب بین سرور GravityZone و کامپیوتر مورد نظر
 - فراهم بودن حداقل فضای خالی بر روی دیسک سخت کامپیوتر مورد نظر

تهیه و نگهداری نسخه پشتیبان

با مراجعه به بخش Configuration | Backup در کنسول مدیریتی GravityZone میتوان از پایگاه داده و تنظیمات سرور نسخه پشتیبان تهیه نموده و یا انجام آن را زمانبندی کرد.

itdefender ravityZone							Welcome, SGC	~	?	
ashboard	Mail Server F	Proxy Miscellaneous	Backup	Active Directory	Virtualization Providers	Certificates				
ətwork	Find how	you can restore a DB B	ackup in case	of Failure at:						
Application Inventory	http://www	v.bitdefender.com/suppor	t/how-to-resto	re-a-gravityzone-data	base-backup-1358.html					
Packages	C. Dealars M	O - Wie O	Defect							
Tasks		ow 👦 Settings	8 Refresh							
olicies	Date		Scheduled		Status		Location			
Assignment Rules										
ports										
arantine										
counts										
User Activity										
onfiguration 🔙										
		CrovityZo	no ".			16.4				

شکل ۵: بخش Backup در ابزار مدیریتی GravityZone

همچنین با استفاده از راهنمای ساخت تصویر لحظهای از ماشین GravityZone در سامانه MY میتوان در بستر مجازیسازی اقدام به تهیه نسخه پشتیان کرد.

بهرهگیری از رمزنگاری مناسب در تبادل اطلاعات

ارتباطات میان دستگاهها و ماشینها با سرور GravityZone از طریق پودمان امن HTTPS برقرار میگردد.

اتخاذ راهحل برای دسترسی ایمن از راه دور برای مدیریت سرویسها و زیرساختها

اگر چه تلاش گردیده که حداکثر مقاومسازی ممکن بر روی ماشین(های) مجازی GravityZone اعمال شود اما کنترل دسترسی به آن از طریق استفاده از دیواره آتش توصیه میگردد. ضمن اینکه در بخش Policies | Firewall در کنسول مدیریتی GravityZone امکان اعمال قواعد متنوع دیواره آتش بر روی دستگاههای تحت پوشش فراهم میباشد.



شکل ۶: قواعد دیواره آتش در ابزار مدیریتی GravityZone

اتخاذ مکانیزم احراز هویت و رمز عبور قوی

توصیه میشود تمامی رمزهای عبور، پیچیده و حاوی بیش از ۱۰ نویسه ٔ باشند.

سیستم عامل مورد استفاده در راهکار GravityZone دارای کاربری با سطح دسترسی root با نام bdadmin است که نحوه تغییر رمز عبور آن در راهنمای تغییر رمز عبور سیستم عامل و کنسول Bitdefender GravityZone بر روی سامانه MY قابل مطالعه است.

همچنین در کنسول مدیریتی GravityZone با کلیک بر روی نام کاربری و انتخاب گزینه My Account میتوان رمز عبور کاربر جاری را تغییر داد.

			Welcome, SGC 🛛 🗸					
			My Account	•				
			Credentials Manager					
			Help & Support					
			Feedback					
			Logout					
Bitdefender GravityZone					Welcome, SGC	~	?	
Dashboard	Account Details							
Network	Username:	admin						
Application Inventory	Account Type:	Custom						
Packages	Full name: *	SGC]				
Tasks	Email: *	support@shabak	eh.net	Ĩ				
	Error.							

با مراجعه به بخش Configuration | Miscellaneous و فعال کردن گزینه Enforce two-factor authentication for all accounts نیز میتوان قابلیت اصالتسنجی دو مرحلهای را برای کلیه نامهای کاربری دارای دسترسی به GravityZone فعال کرد.

Bitdefender GravityZone		Welcome, SGC	~	0	2
Dashboard	Mail Server Proxy Miscellaneous Backup Active Directory Virtualization Providers Certificates				
Network	Concurrent deployments:				
Application Inventory	Prefer basic deployment methods				
Packages	Instead of Integration-specific ones: 🕖 🦳				
Tasks	Two-factor Authentication				
Policies	Enforce two-factor authentication for all				
Assignment Rules	accounts: 🕥				
Reports	NTP Server Settings				
Quarantine	NTP Server Address: * 🕡 pool.ntp.org				
Accounts					
User Activity	Enable Syslog				
Configuration	TCP *				+
Update	Server Name / IP Protocol Port			A	ction
License					
Autor of the Landson					





GravityZone امکان تعریف هر تعداد راهبر با سطوح دسترسی متفاوت را فراهم میکند. توصیه میشود که به هر یک از این راهبران دسترسی مناسب – در حداقل سطح ممکن – تعریف شود. برای این منظور میتوان به بخش Accounts در کنسول مدیریتی GravityZone مراجعه کرد.

New Account	×	
Detuna		ī
Username: *		
Email: *		
Full Name: *		
Password: *		
Confirm password: *	Click here to retype the password	
	Note: The password must contain at least one digit, one upper case, one lower case	
	ana uno special citalacer.	
Settings and Privileges		
Timezone:	(GMT +03:30) Asia/Tehran *	
Language:	English *	1
Role:	Company Administrator *	
	Company Administrator	
Save Cano	Network Administrator	
Gard	Security Analyst	
	Custom	

شکل ۹: تعریف کاربر جدید در ابزار مدیریتی GravityZone

همچنین در صورت استفاده از دامنه ۳ امکان ورود به کنسول مدیریتی GravityZone با نام کاربری مبتنی بر دامنه فراهم میباشد.

جمعآوری، نگهداری و بررسی رخدادنماها

امکان گزارشگیری و رصد رخدادهای امنیتی صورت گرفته در سطح شبکه از طریق بخش Reports در ابزار مدیریتی GravityZone فراهم می باشد. خروجی این گزارشها را میتوان جهت مستندسازی در قالبهای PDF و Excel ذخیره نمود.

Details		
Type:	Antiphishing Activity *	
Name: *	Antiphishing Activity	
Settings	Blocked Applications Blocked Websites	
Now Scheduled	Data Protection Device Control Activity Endpoint Modules Status Endpoint Protection Status	
Reporting Interval:	Firewall Activity	
Show:	HyperDetect Activity Malware Activity	
Delivery:	Send by email to	
	Attach files: Summary as pôf Details as cov Archive files	
Select Target		

شکل ۱۰: انواع گزارشها در ابزار مدیریتی GravityZone

در مسير Accounts | User Activity نيز فعاليت راهبران GravityZone قابل رصد است.

Bitdefender GravityZone	Computers and Virtual Machines \mathbb{Q}					Welcome, SGC 🗸 🤤	ə 🧳
Dashboard	User	Action	•	Target			Search
Network	Role	Area	•	Created	•		
Application Inventory							
Packages	User	Role	Action	Area	Target	Created	
Taeke	admin	Custom	Created	Tasks	BIT-AC-CLIENT	14 October 2018, 13:02:33	
Idana	admin	Custom	Created	Reports	Update Status Report	14 October 2018, 13:00:53	
Policies	admin	Custom	Published	Endpoint Kit	6.6.5.82	14 October 2018, 12:57:18	
Assignment Rules	admin	Custom	Login	System	admin	14 October 2018, 11:59:30	
Reports	admin	Custom	Login	System	admin	14 October 2018, 11:24:32	
Quarantine	admin	Custom	Login(failed)	System	admin	14 October 2018, 11:24:24	
Accounts	admin	Custom	Login	System	admin	14 October 2018, 11:19:51	
User Activity			st Page - Page	1 of 10	Page 20 *		200 item
Configuration					roge 10		
Update	Details						
License	Summary admin created a new task Update Tasł	< 2018-10-14.					

شکل ۱۱: سوابق فعالیت راهبران در کنسول مدیریتی GravityZone

جلوگیری از نشت اطلاعات سازمانی

امکان کنترل و جلوگیری از دسترسی به درگاههای وب غیرمجاز بر اساس سیاستهای سازمان - نظیر شبکههای اجتماعی - و یا اجرای نرمافزارهای خاص از طریق قابلیتهای Content Control و یا Application Control فراهم میباشد.

برای مثال، میتوان دسترسی کاربران موجود در سطح شبکه را به یک یا چند نشانی وب خاص محدود کرد و یا تنها اجازه استفاده از نرمافزارهای مورد تایید سازمان را بر روی ایستگاههای کاری موجود در شبکه صادر نمود.

shboard	(*) Add 🧭 Edit 🗇 Remove	۲	Add to policy 🛞 As	sign updater 🕐 1	Dismiss updater 🕘 Delet	le 🕜 Refresh				
work	- 🖮 Applications and groups		Name	Assign updater	Product name	Product versi	Publisher/Au	Discovered on	Found on	Policies
Application Inventory	a 🗰 All annications		1	Q Q	Q	ρ	Q	•	•	•
ackages			C:\Program Files\C	mmz 0.0.0.0		0.0.0.0		26 September 2018, 15:07:58	1	0
sks	Ungrouped processes		C:\Program Files\W	indox 0.0.0.0		0.0.0.0		26 September 2018, 15:07:58	1	0
es			C:\Program Files\W	indox 1.1707.26019.0	View 3D Preview Resource	1.1707.26019.0	Microsoft Corpo	26 September 2018, 15:07:58	1	o
ignment Rules			C:\Program Files\W	indox 1.1707.26019.0	View 3D	1.1707.26019.0	Microsoft Corpo	26 September 2018, 15:07:58	1	0
rts			C:\Program Files\W	indox 16.0.8366.5761	Microsoft OneNote	16.0.8366.0	Microsoft Corpo	26 September 2018, 15:07:58	1	0
untine			C:\Program Files\W	indox 16.0.8366.5761	Microsoft OneNote Share C	16.0.8366.0	Microsoft Corpo	26 September 2018, 15:07:58	1	0
nte.			C:\Program Files\W	indox 11.18.596.0	SkypeApp	11.18.596.0	Microsoft	26 September 2018, 15:07:58	1	0
e Antivitu			C:\Program Files\W	indox 11.18.596.0	Microsoft® Skype	11.18.596.0	Microsoft Corpo	26 September 2018, 15:07:58	1	0
(Saura)		1	C:\Program Files\W	indox 117.6.1707.7010		117.6.1707.7010	Microsoft Corpo	26 September 2018, 15:07:58	1	0
juration			C:\Program Files\W	indox 0.0.0.0		0.0.0.0		26 September 2018, 15:07:58	1	0
ate			C:\Users\SGC\AppE	ata\1 0.0.0.0		0.0.0.0		26 September 2018, 15:07:58	1	0
inse			C:\Users\SGC\AppE	ata\1 0.0.0.0		0.0.0.0		26 September 2018, 15:07:58	1	0
			C:\Users\SGC\Down	load: 0.0.0.0		0.0.0.0		26 September 2018, 15:07:58	1	0
			C:\Windows\Infuse	BApp: 0.0.0.0		0.0.0.0		26 September 2018, 15:07:58	1	0
			C:\Windows\Infuse	App: 1.1707.26019.0	View 3D Preview Resource	1.1707.26019.0	Microsoft Corpo	26 September 2018, 15:07:58	1	D
			C:\Windows\Infuse	App: 1.1707.26019.0	View 3D	1.1707.26019.0	Microsoft Corpo	26 September 2018, 15:07:58	1	0
			C:\Windows\Infuse	App: 16.0.8326.1000	Microsoft Application Error	16.0.8326.0	Microsoft Corpo	26 September 2018, 15:07:58	1	0
			C:\Windows\Infuse	App: 16.0.8326.1000	Watson Subscriber for SEN	16.0.8326.0	Microsoft Corpo	26 September 2018, 15:07:58	1	0



Bitdefender GravityZone	Computers and Virtual Ma	chines	14/							Welcome, SGC	19	0	٠
Dashboard	General	+	Veb Access Control	Se	Settings								
Dashboard Network Application inventory Packages Taska Policies Assignment Rules Reports Cuarrantine Accounts User Activity Configuration Update License	 General Antimalware Sandbox Analyzer Firewall Context Control Traffic Web Control Data Protection Application Control Device Control Nelay Exchange Protection 	· · · ·	Web Access Control Block Glock Glock Access Control Access Access Control Protection against fraud Protection against phish	Se Allow - Vieb access is all This option allows all brow Ex	Bettings Illowed owser access to web	pages, excluding	ng the pages define	d in Exceptions.					
🗞 Tools			Save Cancel										

شکل ۱۳: بخش Web در تنظیمات Web

ترمیم آسیبپذیریها

محصول Bitdefender Patch Management امکان بهروزرسانی و نصب اصلاحیههای مربوط به سیستم عامل و نرمافزارهای نصب شده در سطح سازمان را فراهم میکند. این محصول فایلهای بهروزرسانی و اصلاحیهها را بر روی دستگاه یا دستگاههای تعیین شده دریافت و بهصورت متمرکز آنها را بر روی ماشینها و دستگاههای تحت پوشش توزیع میکند.

Bitdefender GravityZone								Welco	me, Company	× ?	٠
Dashboard	Search products ×	0	Ignore patches		0	Refresh					ø II
Network	S Display all patches		Patch Name	КВ	CVE	Bull	Patch s	Categ *	Installed /	Missing / In	Affecte
Patch Inventory	= 7-7in		Q	ρ	ρ	ρ	•	•			Q
Packages			Windows6.1-Windows7	Q31	1 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
Tasks	+ AIMP Devi eam		Windows6.1-Windows7	Q31	1 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
Policies	+ 🖶 AOL Inc		Windows6.1-Windows7	Q31	1 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
Assignment Rules	+ 🖶 AT&T		Windows6.1-Windows7	Q31	1 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
Reports	+ 🖶 Acro Software		Windows6.1-Windows7	Q31	1 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
Quarantine	+ 🖶 Adobe		Windows6.1-Windows7	Q31	1 CV	MS1	Critical	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
Accounts	+ 🖶 Apache Software Foundation		Windows6.1-Windows7	Q31	1 CV	MS1	Critical	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
User Activity	+ 🖶 Apple		Windows6.1-Windows7	Q31	2 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
Configuration	+ 🖶 Arduino LLC		Windows6.1-Windows7	Q31	1 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
Update	+ 🖶 Atlassian	•	Windows6.1-Windows7	Q31	1 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
License	+ 🖶 Audacity		Windows6.1-Windows7	Q31	1 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
	+ 🖶 Autodesk		Windows6.1-Windows7	Q31	1 CV	MS1	Critical	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc
			Windows6.1-Windows7	Q31	1 CV	MS1	Critical	Security	1 EP / 0 EP	0 EP / 0 EP	5 Produc
	+ 💼 Bandicam Company		Windows6.1-Windows7	Q31	2 CV	MS1	Important	Security	0 EP / 0 EP	1 EP / 0 EP	5 Produc

شکل ۱۴: انباره اصلاحیههای امنیتی



شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تاسیس شد. این شرکت یکی از باسابقه ترین شرکتهای فعال در حوزه امنیت فناوری اطلاعات است. با بیش از ۲۵ سال تجربه موفق در عرضه محصولات و خدمات امنیت شبکه، شرکت شبکه گستر افتخار خدماتدهی به هزاران شرکت و سازمان در بخشهای مختلف کشور را دارد و مجری بزرگترین پروژههای نصب و نگهداری نرمافزارهای ضدبدافزار و سختافزارهای دیـواره آتش در کشور بوده است.



تهران خیابان شهید دستگردی (ظـفـر) شماره ۲۷۳ تلفن / دورنگار ۴۲۰۵۲ – ۲۱۰ www.shabakeh.net info@shabakeh.net