

قائمة المحتويات

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة Secure Ware Analytics

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة

مقدمة



ىرخأ تامدخ

[تاديدهتلا ةكبش ل ةبولطملا ذفانملاو IP نيوانع](#)

زاهجال رادصا ىلا اذانتسا ىرخألا تامدخلل ذفانمو ةيفاضا IP نيوانع دنتسملا اذه نمضتي

[تاديدهتلا ةكبش ةزهجأ تيبتت قلدا](#): ةيقررتلاو تيبتتلا ةلدا قئاثو ىلا عوجرلا ىجري

رارق

زاهجال ىلا ةيماحلا رادجل ليماحتلل ةيماحلا رادج دعاوق

ال اهنأ ىلع NSLOOKUP ربع ايلحم ديكأتلا عاجرلا. رشننلا تقوي ف ةحيحص IP نيوانع تناك*
ةحيحص لازت

Secure Ware Analytics زاهج

لوؤسملا ةهجاو

ردصملا	ةهجولا	لوكونوربلا	ذفنملا	هاجتلا	عارجالا	تاظحالم
يأ	ةهجاو لوؤسملا	TCP	22	يف	حامس	(SSH) نمآلا لقنلا لوكونورب
يأ	ةهجاو لوؤسملا	TCP	80/443	يف	حامس	ةهجاو ةهجاو ىلا لوصولاب حامسلا (GUI) ةيوسرلا مدختسملا لوؤسملا
ةهجاو لوؤسملا	مداخل IP NFS	TCP	2049	جراخ	حامس	مادختسالا احوتم نوكي نأ بجي* ةزيما واطايتحالا خسنلا ةزيما NFS ل "عيمجتلا"

ةفيظن ةهجاو

ردصملا	ةهجولا	لوكونوربلا	ذفنملا	هاجتلا	عارجالا	تاظحالم
--------	--------	------------	--------	--------	---------	---------

يأ	ة فيظن ةهجاو	TCP	80/443	يف	حامس	ةهجاو ىلا لوصولاب حامسلا ة فيظن GUI
يأ	ة فيظن ةهجاو	TCP	8443	يف	حامس	احوتفم نوكي نأ بجي* ةزيم ىلع Admin مادختسال Clean.
يأ	ة فيظن ةهجاو	TCP	9443	يف	حامس	احوتفم نوكي نأ بجي* Glovebox ةزيم مادختسال ةنيعل
ةهجاو ة فيظن	ديربلا ليحرت مداخ مت يذلا ينورتكلإلا هنيوكت	TCP	25	جراخ	ولات	DE ةهجاو زاهجلا مدختسي SMTP تالاصتإ ءدبل clean مت يذلا ديربلا مداخ هنيوكت
ةهجاو ة فيظن	DNS مداخ نيوكت مت فيظن	TCP/UDP	53	جراخ	حامس	يف طقف بولطم، يرايتخإ* فيظن DNS نيوكت ةلاح
ةهجاو ة فيظن	مت يذلا Syslog مداخ هنيوكت	TCP/UDP	514	جراخ	حامس	مداخلاب لاصلتالاب حامسلا لئاسر ريقلتل نيعل ةكبش تامالعو syslog تاديدهتلا
ةهجاو ة فيظن	LDAP مداخ	TCP/UDP	389/636	جراخ	حامس	يف طقف بولطم، يرايتخإ* لوكتورب نيوكت ةلاح LDAP.

ةرذق ةهجاو

ةرذقلا ةهجاو الجرخ

ردصملا	ةهجولا	لوكتوربلا	ذفنملا	ءارجلا	ةطالحم
ةهجاو ةرذق	تنرتنإلا	يأ	يأ	حامس	جذامنلا نم ةرداصل رورملا ةكرحب حامسلا لالخ نم يرايتخإ لكشب اهليكوكت متي يتلاو

جئاتن ىلع لوصحلل Cisco. تانايب زكارم قراضل حماربلل حامسل مزلي، ققيقد اهب صاخل مكحتلاو رماوالا مداخبل لاصتالاب همي مصت مت لوكتوربو ذفنم يا مادختساب (همادختسال)					
--	--	--	--	--	--

قفلات قحوا لاخدا مت

ردصملا	قحولا	لوكتوربل	ذفنملا	ءارجالا	قطحالم
يا	ردقلا تنرتنلا يا	يا	ركنن	قراوالا تالاصتالا قفاك ضفر	
ردصملا	قحولا	لوكتوربل	ذفنملا	ءارجالا	قطحالم
قحوا قردق	تنرتنلا	TCP	22	حامس	قطلل معدلاو شي دحتلا تامدخ صيخارثلاو
قحوا قردق	تنرتنلا	TCP/UDP	53	حامس	رداصل DNS ب حامسلا
قحوا قردق	تنرتنلا	UDP	123	حامس	رداصل NTP ب حامسلا
قحوا قردق	تنرتنلا	TCP	19791	حامس	تاليحت معدب لاصتالاب حامسلا قنمالا قراضل حماربل
قحوا قردق	Cisco Umbrella	TCP	443	حامس	نم ءارثاو فاشتكا تامدخب لاصتالا قجراخ قح
قحوا قردق	يلامجا تاسوريفلا	TCP	443	حامس	نم ءارثاو فاشتكا تامدخب لاصتالا قجراخ قح
قحوا قردق	قباحس مويئاتيتلا	TCP	443	حامس	نم ءارثاو فاشتكا تامدخب لاصتالا قجراخ قح

ردصملا	ةهجولا	لوكوتوربلا	ذفنملا	هاجتا	فيملا مسا	ليصافتلا
ةهجاو ةرذق	63.97.201.96 63.162.55.96	TCP	19791	جراخ	rash.threatgrid.com	نع زاهج / معد عضو دعب
ةهجاو ةرذق	63.97.201.97 63.162.55.97	TCP	22	جراخ	appliance-updates.threatgrid.com	ليمحتل مدختسي معدلا صيخشت يئاقلتلا  ةطحالم بلطتي رادصا جمانربلا 1.2+
ةهجاو ةرذق	63.97.201.98 63.162.55.98	TCP	22	جراخ	support-snapshots.threatgrid.com	ليمحتل مدختسي معدلا صيخشت يئاقلتلا  ةطحالم بلطتي رادصا جمانربلا 1.2+
ةهجاو ةرذق	63.97.201.99 63.162.55.99	TCP	22	جراخ	appliance-licensing.threatgrid.com	صيخارثلا ةرادا

ةنمآلا ةراضلا جماربلا تاليلحت ةباحس

(ةدحتملا تايالولا) ةدحتملا تايالولا

لوصولل URL ناوع: <https://panacea.threatgrid.com>

لڤ صافاتا	ذفنملا	IP	فڤضملا مسا
ةراضلا جماربلا تالڤلحت ةبوابلا ةجمدملا ةزهجال او ةنمالا (ESA/WSA/FTD/ODNS/Meraki)	443	IPv4: لوكوتورب 63.97.201.67 63.162.55.67 IPv6: لوكوتورب 2602:811:9007:6::61 2602:811:900b:6::6e	panacea.threatgrid.com
ةنڤعلال عافتلا ةذفان	443	IPv4: لوكوتورب 200.194.241.35 IPv6: لوكوتورب 2602:811:900f:6::6e	glovebox.chi.threatgrid.com
ةنڤعلال عافتلا ةذفان	443	IPv4: لوكوتورب 63.97.201.67 IPv6: لوكوتورب 2602:811:9007:6::61	glovebox.rcn.threatgrid.com
ةنڤعلال عافتلا ةذفان	443	IPv4: لوكوتورب 63.162.55.67 IPv6: لوكوتورب 2602:811:900b:6::6e	glovebox.scl.threatgrid.com
FMC/FTD تافلما لڤلحت ةمدخ	443	IPv4: لوكوتورب 63.97.201.67 63.162.55.67 IPv6: لوكوتورب 2602:811:9007:6::61	fmc.api.threatgrid.com

		2602:811:900b:6::6e	
--	--	---------------------	--

(يېروروال داخاتال) ابوروأ ةباحس

لوصول URL ناونع: <https://panacea.threatgrid.eu>

ليصافتال	ذفنمال	IP	فيضمال مسا
ةراضال جماربال تاليلحت ةباوبل ةجمدمل ةزهجال او ةنمال (ESA/WSA/FTD/ODNS/Meraki)	443	IPv4: لوكوتورب 62.67.214.195 200.194.242.35 200.194.245.35 IPv6: لوكوتورب 2602:811:9006:6::6e 2602:811:900c:6::6e	ددهملا بارش
ةنيعلال لعافتال ةذفان	3	IPv4: لوكوتورب 62.67.214.195 200.194.245.35 IPv6: لوكوتورب 2602:811:900c:6::6e	glovebox.muc.threatened.eu
ةنيعلال لعافتال ةذفان	443	IPv4: لوكوتورب 200.194.242.35 IPv6: لوكوتورب 2602:811:9006:6::6e	glovebox.fam.threatened.eu
FMC/FTDFile ليلحت ةمدخ	443	IPv4: لوكوتورب 62.67.214.195 200.194.242.35	fmc.api.threatened.eu

		200.194.245.35 IPv6: 2602:811:9006:6::6e 2602:811:900c:6::6e	
--	--	--	--

هذه IP نيوانع ماذختساب ةياملال رادج دعاوق ثيذحت يجرى ،ميدقلا 89.167.128.132 IP ءاغلإ مت

(CA) ادنك ةباحس

لوصول URL ناوع: <https://panacea.threatgrid.ca>

ليصافتلا	ذفنملا	IP	فيضملا مسا
ةراضلا جماربلا تاليلحت ةباوبل ةجمدمل ةزهجالاو ةنمألا (ESA/WSA/FTD/ODNS/Meraki)	443	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	ca.dedemla.bash
ةنيعلال لعافتلا ةذفان	443	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	glovebox.kam.threatened.ca
FMC/FTD تافللم ليلحت ةمدخ	443	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	fmc.api.threatened.ca

(يقيرفألا داخاتالا) ايلارلسأ ةباحس

لوصول URL ناوع: <https://panacea.threatgrid.com.au>

لي صافات	ذفنم	IP	فيضم المسا
عراض المارب الما لي لحت عباوبل عجمدم الما عزه الما لة نم الما (ESA/WSA/FTD/ODNS/Meraki)	443	IPv4: لوكوت ورب 200.194.246.35 200.194.247.35 IPv6: لوكوت ورب 2602:811:900e:6::6e 2602:811:9003:6::6e	panacea.threatgrid.com.au
ةني ع الما ل عافات الما ذفان	443	IPv4: لوكوت ورب 200.194.246.35 200.194.247.35 IPv6: لوكوت ورب 2602:811:900e:6::6e 2602:811:9003:6::6e	glovebox.syd.threatgrid.com.au
FMC/FTD تافلم لي لحت عمدخ	443	IPv4: لوكوت ورب 200.194.246.35 200.194.247.35 IPv6: لوكوت ورب 2602:811:900e:6::6e 2602:811:9003:6::6e	fmc.api.threatgrid.com.au

دنه الما عباحس

لوصول ل URL ناونع: <https://panacea.threatgrid.in>

لي صافات	ذفنم	IP	فيضم المسا
عراض المارب الما لي لحت عباوبل	443	IPv4: لوكوت ورب	ن.ا.دي رده. "ايس ان اب"

ةجمدملا ةزهجالو ةنمآلا (ESA/WSA/FTD/ODNS/Meraki)		200.194.244.35 IPv6: لوكوتورب 2602:811:9001:6::6e	
ةنيعلال عافتلا ةذفان	443	IPv4: لوكوتورب 200.194.244.35 IPv6: لوكوتورب 2602:811:9001:6::6e	glovebox.bom.threatened.in
FMC/FTD تافلما ليلحت ةمدخ	443	IPv4: لوكوتورب 200.194.244.35 IPv6: لوكوتورب 2602:811:9001:6::6e	fmc.api.threatgrid.com.in

ةزهجالو لثم Cisco نم ةنمآلا ةراضال جماربال تاليلحت تابلطتم نم ديزم ىلع لوصحلل
لاقملا اذه ىلع عالطالا ىجري

ةلصلال يذوتحملا

. عجار ، تابلطتملا ثدحأ ىلع لوصحلل

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا