

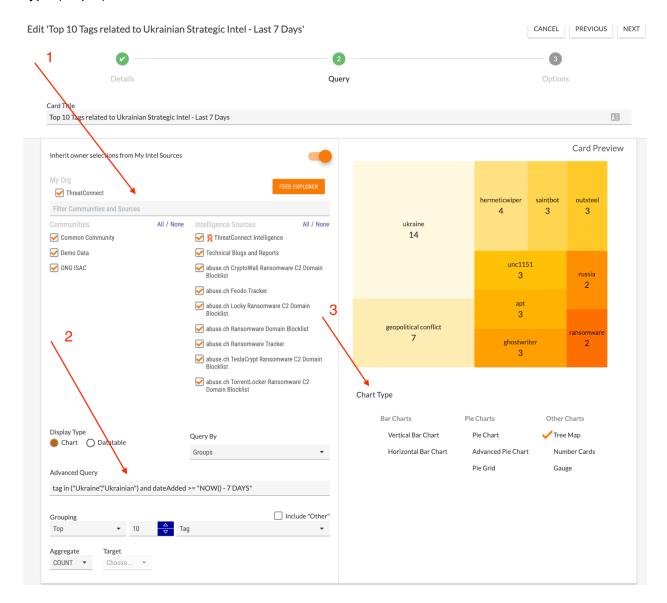
Russian Threat Actor Intelligence Dashboards

P: 1.800.965.2708 | F: +1.703.229.4489 www.ThreatConnect.com



There are two example dashboards provided by ThreatConnect. The first specifically covers Russian APT Groups. The second is an update dashboard previously <u>detailed in this guide</u>. For each dashboard, the card details that populate the dashboard are provided along with an example screenshot.

- 1) If you've never created a custom dashboard in ThreatConnect or need a fresher, <u>start</u> <u>with this tutorial.</u>
- Next, choose your Intel Sources (step 1), define your query (step 2), and choose a Chart Type (step 3).



As a reminder, if you need additional assistance, please reach out to the ThreatConnect Customer Service team and they will be happy to help you build out a dashboard.

ThreatConnect.com Copyright © 2022 ThreatConnect, Inc.

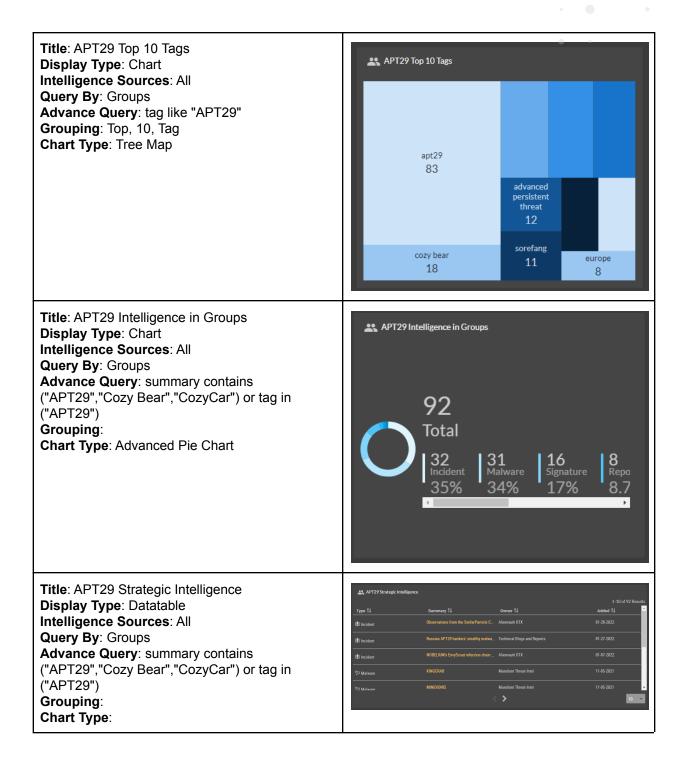
Russian APT Groups Dashboard

🔀 ThreatConnect		Dashboard 🗸 Workflow 🗸	Posts Playbooks 🗸 Brow	vse 🗸 Spaces 🗸 Create 🗸 Im	port 🗸 🕜 🏟 📌 Q
	Russian Al	PT Groups			A 0 :
🚉 APT28 Top 10 Tags 🚉 APT28 Intellige	ence in Groups	APT28 Strategic Intelligence			
190 fancy bear sedait power storm 136 124 122 210 Total	туре 11	Summary 11	Owner 11	1-10 of 210 Results Added 1	
			Mandiant Threat Intel	11-05-2021	
		TRICKSHOW	Mandiant Threat Intel	11-05-2021	
		TRICKSHOW.AUTOIT	Mandiant Threat Intel	11-05-2021	
	tg-4127 67% 19% 6.19% 5.		TRICKSHOW.AUTOIT.V3	Mandiant Threat Intel	11-05-2021
russia 121 137 dedicated server	,		TRICKSHOW.DELPHI	Mandiant Threat Intel	11-05-2021
41				\diamond	10 -
APT29 Top 10 Tags APT29 Intellige APT29 Intellige	ince in Groups	APT29 Strategic Intelligence			
		туре 1↓	Summary †1	Owner 11	Added 1
9	2	ILI Incident	Observations from the StellarParticle C_	Alienvault OTX	01-28-2022
100	_ otal	I!I Incident	Russian APT29 hackers' stealthy malwa.	_ Technical Blogs and Reports	01-27-2022
advanced persistent breat	32 31 16 8 Repo	III Incident	NOBELIUM's EnvyScout infection chain _	Alienvault OTX	01-07-2022
12	35% 34% 17% 8.7	²≿i Malware	KINGCRAB	Mandiant Threat Intel	11-05-2021
cozy bear sorefang 18 11 europe			MINIDIONIS	Mandiant Threat Intel	11-05-2021
10 8				< >	10 👻
FIN7 Top 10 Tags FIN7 Top 10 Tags	ce in Groups	FIN7 Strategic Intelligence			
dedicated server anunak		туре †↓	Summary Î↓	owner †↓	Added 1
22 17	33	III Incident			01-18-2022
	otal	illi Incident			01-14-2022
	58 40 25 6 ncident Malware Signature Docu	7⊐ Malware	MINISWIPE	Mandiant Threat Intel	11-05-2021
latest blog posts	4% 30% 19% 4.5	🌮 Malware			11-05-2021
carbanak 10 34 suspicious isp use			POWERMINE	Mandiant Threat Intel	11-05-2021
10					10
🚉 Energetic Bear Top 10 Tags	Intelligence in Groups	Energetic Bear Strategic Intell			1-10 of 11 Results
energetic bear 9 russia dragonfly		туре 1	Summary 11 DYMALLOY Malware Review	Owner 11 Dragos WorldView	Added 11 09-25-2021
9 russia draportiv 8 8 1	1	Report	CISA Advisory (AA20-296A): Russian St.		10-26-2020
havex	otal	Report	20201026A: CISA Advisory (AA20-290A). Russian St.		10-26-2020
	ncident Report Campaign Signa	Signature			
crouching yeti	55% 18% 9.09% 9.0	111 Incident			10-26-2020
9 koala team scada 4 3			New Insights into Energetic Bear???s W_	 Technical Blogs and Reports 	11-05-2017 -
🚉 Turla Group Top 10 Tags	elligence in Groups	Turla Group Strategic Intellige	nce		1-10 of 60 Results
russia targeted snake		Type 1↓	Summary 11 Operation GhostShell: Novel RAT Target	Owner 11	Added 1↓
turia russia targeted snake attaiks 75 29 28 27 6	0	I Incident	Web Shells in ICS Intrusions	Dragos WorldView	09-25-2021
	otal	Report	Web Shells in ICS Intrusions Reports Linking Russian Actors to Turki		
apt 26	46 icident 6 7% 10% 8.33% 1.6				09-25-2021
advanced persistent	7% 10% 8.33% 1.6	Report	WorldView Week 51, 2019 (16 - 22 Dece.		09-25-2021
blog:securelist 31 24				Dragos WorldView	09-25-2021 -
🎎 Sandworm Top 10 Tags 🗱 Sandworm Intel	Illigence in Groups	2 Sandworm Strategic Intelligen	0e		
🞎 Sundworm Top 10 Tags 🏦 Sundworm Intelligence in Groups					1-10 of 49 Results
electricultive encoded and the standard with a state of the standard with a state of the standard with a state of the stat	Type 11	Summary 11 MITRE ATT&CK: Wizard Spider and Sand.	Owner 11 Technical Blogs and Reports	Added 11 03-28-2022	
	Report	New KAMACITE CYCLOPS BLINK Netwo.		03-23-2022	
		Sandworm: A tale of disruption told anew		03-22-2022	
	1 th Incident	Cyclops Blink Sets Sights on Asus Rout		03-22-2022	
	1 ¹ Incident	Sandworm	Alienvault OTX	03-11-2022	
electric utility europe			Jule House		10 5
13 8 7					10
13 o Cyclops blink					

ThreatConnect.com Copyright © 2022 ThreatConnect, Inc.

Card Build Information	Card Screenshot				
Title: APT28 Top 10 Tags Display Type: Chart Intelligence Sources: All	🕰 APT28 Top 10 Tags				
Query By: Groups Advance Query: tag like "APT28" Grouping: Top, 10, Tag Chart Type: Tree Map	apt28 190 fancy bear sednit pawn storm 136 124 122				
	sofacy 141 tg-4127				
	russia 121 137 dedicated server 41				
Title: APT28 Intelligence in Groups Display Type: Chart Intelligence Sources: All Query By: Groups Advance Query: summary contains ("APT28","Sofacy","Fancy Bear") or tag in ("APT28") Grouping: Chart Type: Advanced Pie Chart	APT28 Intelligence in Groups 210 Total 140 Incident 67% 40 Malware 19% 13 Signature 6.19% 5. 12 Adv 5. 12 Adv 5. 12 Adv 5. 12 Adv 5. 12 Adv 5. 12 140 19%				
Title: APT28 Strategic Intelligence Display Type: Datatable Intelligence Sources: All Query By: Groups Advance Query: summary contains ("APT28","Sofacy","Fancy Bear") or tag in ("APT28") Grouping: Chart Type:	LL APT28 Strategic Intelligence 1:00/2100 Securits Type I1 Summary I1 Owner I1 Added I1 32 Malware LANESTONE Mandam Threat Intel 11:05:2021 32 Malware TROCKSHOW AUTOT Mandam Threat Intel 11:05:2021 32 Malware TROCKSHOW AUTOT Mandam Threat Intel 11:05:2021 32 Malware TROCKSHOW AUTOTY Mandam Threat Intel 11:05:2021				





• • • • •

Card Build Information	Card Screenshot				
Title: FIN7 Top 10 Tags Display Type: Chart Intelligence Sources: All	🚉 FIN7 Top 10 Tags				
Query By: Groups Advance Query: tag like "FIN7" Grouping: Top, 10, Tag Chart Type: Tree Map	dedicated server 22 17 92				
	Latest blog postscarbanak1034suspicious isp use10				
Title: FIN7 Intelligence in Groups Display Type: Chart Intelligence Sources: All Query By: Groups Advance Query: summary contains ("FIN7","Carbanak","Carbon Spider") or tag in ("FIN7") Grouping: Chart Type: Advanced Pie Chart	EIN7 Intelligence in Groups ACTIONS A				
Title: FIN7 Strategic Intelligence Display Type: Datatable Intelligence Sources: All Query By: Groups Advance Query: summary contains ("FIN7","Carbanak","Carbon Spider") or tag in ("FIN7") Grouping: Chart Type:	If FIN7 Strategic Intelligence 1-10 of 133 Results Type 11 Summary 11 Owner 11 Added 11 If Incident FIN7 Uses Flack Drives to Spread Remo. 011 V 2022 If Incident FIN7 Uses Flack Drives to Spread Remo. 011 V 2022 If Incident FIN7 Uses Flack Drives to Spread Remo. 011 V 2022 721 Malware MINSWPE Mandaust Threat Intel 1165 2021 721 Malware OFFTRACK Mandaust Threat Intel 1165 2021 721 Malware POMERMINE Mandaust Threat Intel 1165 2021				

Card Build Information	Card Screenshot			
Title: Energetic Bear Top 10 Tags Display Type: Chart Intelligence Sources: All Query By: Groups Advance Query: tag like "Energetic Bear"	Energetic Bear Top 10 Tags	ACTIONS♥ dragonfly		
Grouping: Top, 10, Tag Chart Type: Tree Map	havex 8	8		
	9 energy 6 crouching yeti 9 koala team 4	scada 3		
Title: Energetic Bear Intelligence in Groups Display Type: Chart Intelligence Sources: All Query By: Groups Advance Query: summary contains ("Energetic Bear", "Dragonfly", "Anger Bear") or tag in ("Energetic Bear") Grouping: Chart Type: Advanced Pie Chart	Energetic Bear Intelligence in Groups 11 Total 6 1ncident 55% 2 Report 18% 9.09% 9.0 1 1 1 1 2 1 1 2 1 2 1 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 2 1 1 2 1 1 2 1 2 1 2 1 1 2 1 1 1 2 1 2 1 1 1 1 1 2 1 1 1 1 1 1 1 1 1 1 1 1 1			
Title: Energetic Bear Strategic Intelligence Display Type: Datatable Intelligence Sources: All Query By: Groups Advance Query: summary contains ("Energetic Bear", "Dragonfly", "Anger Bear") or tag in ("Energetic Bear") Grouping: Chart Type:	Type 11 Summary 11 Owner 11 Breport DYUALLITY Malware Review Dragos Wold/Vew Breport DYUALLITY Malware Review Dragos Wold/Vew Breport CISA Advisory (AA23 2984). Horsand Str. ThreatConnect Intelligence Breport 202010284. CISA Advisory (AA23 2984). ThreatConnect Intelligence Breport Here Insights into Exception Barry The Wr. Technical Blogs and Reports	1-10+11 Results Added T1 0+25-227 10-26-2223 10-26-2029 19-26-2029 11-65-2017 10 10 10 10 10 10 10 10 10 10 10 10 10		

Card Build Information	Card Screenshot
Title: Turla Group Top 10 Tags Display Type: Chart Intelligence Sources: All Query By: Groups Advance Query: tag like "Turla" Grouping: Top, 10, Tag	turla Group Top 10 Tags turla russia 75 29 28 27
Chart Type: Tree Map	75 28 27 uroburos 33 26
	blog: securelist 31 24
Title: Turla Group Intelligence in Groups Display Type: Chart Intelligence Sources: All Query By: Groups Advance Query: summary contains ("Turla Group","Snake","Venomous Bear") or tag in ("Turla") Grouping: Chart Type: Advanced Pie Chart	Include the second
Title: Turla Group Strategic Intelligence Display Type: Datatable Intelligence Sources: All Query By: Groups Advance Query: summary contains ("Turla Group", "Snake", "Venomous Bear") or tag in ("Turla") Grouping: Chart Type:	Lists Group Strategic Intelligence 1:10 of 60 Results Type 11 Summary 11 Owner 11 Added 11 Image: Constraint Strategic Intelligence Image: Constraint Stra

Card Build Information	Card Screenshot				
Title: Sandworm Top 10 Tags Display Type: Chart	Sandworm Top 10 Tags				
Intelligence Sources: All Query By: Groups Advance Query: tag like "Sandworm" Grouping: Top, 10, Tag Chart Type: Tree Map	electrum manufacturing united states 12 11 11 38				
	north america 10				
	electric utility europe 13 8 7				
Title: Sandworm Intelligence in Groups Display Type: Chart Intelligence Sources: All Query By: Groups Advance Query: summary contains ("Sandworm","Hades","Voodoo Bear") or tag in ("Sandworm") Grouping: Chart Type: Advanced Pie Chart	Sandworm Intelligence in Groups 49 Total 27 Report 15 Incident 3 Signature 1 6.12% 2.0 *				
Title: Sandworm Strategic Intelligence Display Type: Datatable Intelligence Sources: All Query By: Groups Advance Query: summary contains ("Sandworm","Hades","Voodoo Bear") or tag in ("Sandworm") Grouping: Chart Type:	List Sundworm Strategic Intelligence 1:100 of 49 Results Type 11 Sunnmary 11 Owner 11 Added 11 12 Bocident MITER ATLICK Wixed Splot and Sand. Technical Blogs and Reports 03 28 2002 16 Report New KUMACITE CYCLOPS BLINK Network Disgos Workf/New 03 22 2002 16 Incident Sandworm: A take of disruption Indi anow Technical Blogs and Reports 03 22 2022 16 Incident Cyclopa Blink Sett Sights on Axea Read. Alienrault 01X 03 17 2022 V C Sandworm Alienrault 01X 03 01 2022 V				

Russian-specific Threat Intelligence Dashboard

C ThreatConnect	ť			Dashboard 🗸 Worl	kflow 🗸 Posts	Playbooks 🗸 Browse	✔ Spaces ✔ Create ✔ I	mport 🗸 🕐 🏟 🦛
MY INTEL SOURCES (106) -			R	ussia				₽ ⊕ :
2 Top 10 Tags related to Russian Stra	ategic Intel - Last 30	Russian Strategic Intel - Last 30 Days				1-10 of 21 Results	Russian Strategic Intel by Owner	- Last 30 Days
russia		Type 11 Summary		Owner 11 Dragos WorldView		Added 17	Cybersixgill DVE	
21		11 Incident CEO Blog Se	ries: No Sector Is Off-Limits	Technical Blogs and Reports		03-26-2022	Flashpoint Intel	
ukraine	conti		r WEEK 12, 2022	Dragos WorldView Flashpoint Intelligence Reports		03-24-2022	Alienvault OTX	
8 Intelligence report 7	5 malware 4	- mport		Technical Blogs and Reports		03-24-2022 • 10 •	Dragos WorldView Have I Been Pwnd	
🏷 Tactical Intel Related to Russia - La	ast 30 Days	ت Tactical Intel Related to Russia - Last 30 Day:		410 more		1-10 of 20 Results	∑ Tactical Intel Related to Russia by	
	_	わまた Taisunwin.club	Technical Blogs and Rep.	• • 10 more		03-29-2022		
13	/		Technical Blogs and Rep.	• C U +10 more		03-29-2022	Technical Blogs	
Host	File		Technical Blogs and Rep.	t. R. +10 more		03-29-2022		
		ঈ⊐ Host play.go88vm.vin	Technical Blogs and Rep.	• m Q +10 more		03-29-2022		
€ Total High Threat Assessment Score	105 0 1000	্যু High Threat Assessment Score IOCs - Past 30				10 -		
-y_ Total High Threat Assessment Scon	e locs - Past 30 Days	Type 14 Summary 14	Owner	1↓ Threa	it Rating 1↓	ThreatAssess 1↓	Added 1↓	1-10 of 122 Res Modified ↓₹
110 Host	11 File	≫ Host web.surwinvn.vip		I Blogs and Reports 😔 😞 😓				
HUSL	Flic			l Blogs and Reports 🛛 😞 😔			03-24-2022	
5		™ Host taisunwin.club ™ Host sunvin.vin		I Blogs and Reports 😞 😓 🤤			03-24-2022	
Address			Technica	l Blogs and Reports 🛛 😞 😓 🗧	< >			03-29-2022
Total CVEs Related to Russia		EX CVEs Related to Russia						1-10 of 30 Res
28	1	туре 1↓	Summary †↓		Owner †↓			Added 1
Incident	⊥ Report	I Report		ate-Sponsored Adversaries Exploiting Syber Impact of the Escalating Russia				
		RIN Incident		nese APT Backdoor Attack Targets R				
1		र्थिः Incident	Operation ???Kren			gs and Reports		
Threat					rgets C ThreatConnec	t Intelligence		07-20-2020
C ThreatConnect								

Card Build Information	Card Screenshot
Title: Top 10 Tags related to Russian Strategic Intel - Last 30 Days Display Type: Chart Intelligence Sources: All Query By: Groups Advance Query: tag in ("Russia", "Russian", "Soviet Union") and dateAdded >= "NOW() - 30 DAYS" Grouping: Top, 10, Tag Chart Type: Tree Map	russia 21 ukraine conti 8 5 intelligence report malware 7 4
Title: Russian Strategic Intel - Last 30 Days Display Type: Datatable Intelligence Sources: All Query By: Groups Advance Query: tag in ("Russia", "Russian", "Soviet Union") and dateAdded >= "NOW() - 30 DAYS" Grouping: Chart Type:	Lastian Strategic intel - Last 30 Days
Title: Russian Strategic Intel by Owner - Last 30 Days Display Type: Chart Intelligence Sources: All Query By: summary contains ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 30 DAYS" Advance Query: Grouping: Owner Name Chart Type: Horizontal Bar Chart	Russian Strategic Intel by Owner - Last 30 Days Technical Blogs Cybersixgill DVE Flashpoint Intel Alienvault OTX Dragos WorldView Have I Been Pwnd 0 20



