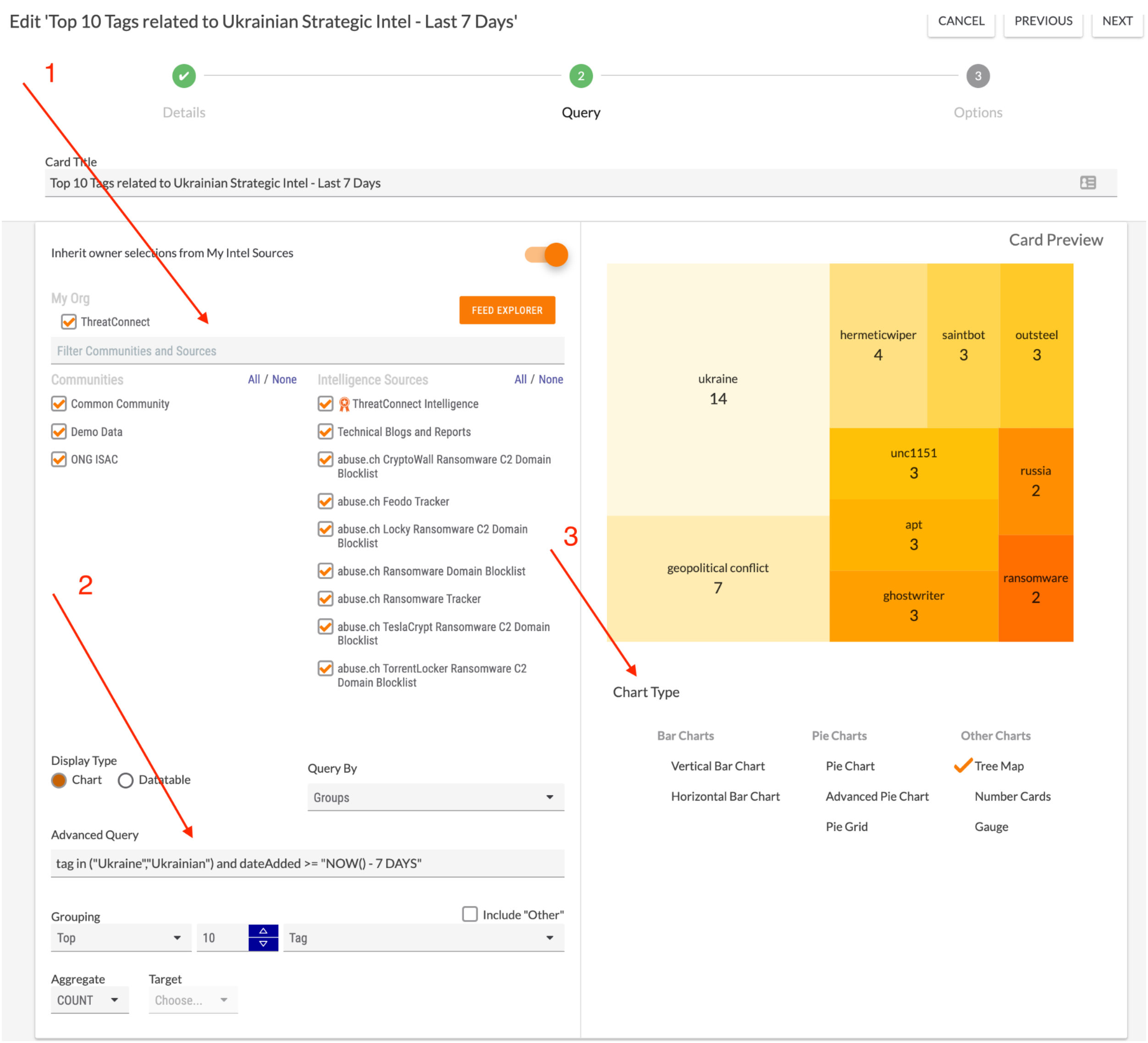
Russian Threat Actor Intelligence Dashboards

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

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 detailed in this guide. 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, start with this tutorial.
2) Next, choose your Intel Sources (step 1), define your query (step 2), and choose a Chart Type (step 3).


Edit 'Top 10 Tags related to Ukrainian Strategic Intel - Last 7 Days'

Card Title: Top 10 Tags related to Ukrainian Strategic Intel - Last 7 Days

Inherit owner selections from My Intel Sources

My Org: ☑ ThreatConnect

Communities: ☑ Common Community, ☑ Demo Data, ☑ ONG ISAC

Intelligence Sources: ☑ ThreatConnect Intelligence, ☑ Technical Blogs and Reports, ☑ abuse.ch CryptoWall Ransomware C2 Domain Blocklist, ☑ abuse.ch Feodo Tracker, ☑ abuse.ch Locky Ransomware C2 Domain Blocklist, ☑ abuse.ch Ransomware Domain Blocklist, ☑ abuse.ch Ransomware Tracker, ☑ abuse.ch TeslaCrypt Ransomware C2 Domain Blocklist, ☑ abuse.ch TorrentLocker Ransomware C2 Domain Blocklist

Display Type: ● Chart ○ Datatable

Query By: Groups

Advanced Query: tag in ("Ukraine","Ukrainian") and dateAdded >= "NOW() - 7 DAYS"

Grouping: Top 10 Tag ☐ Include "Other"

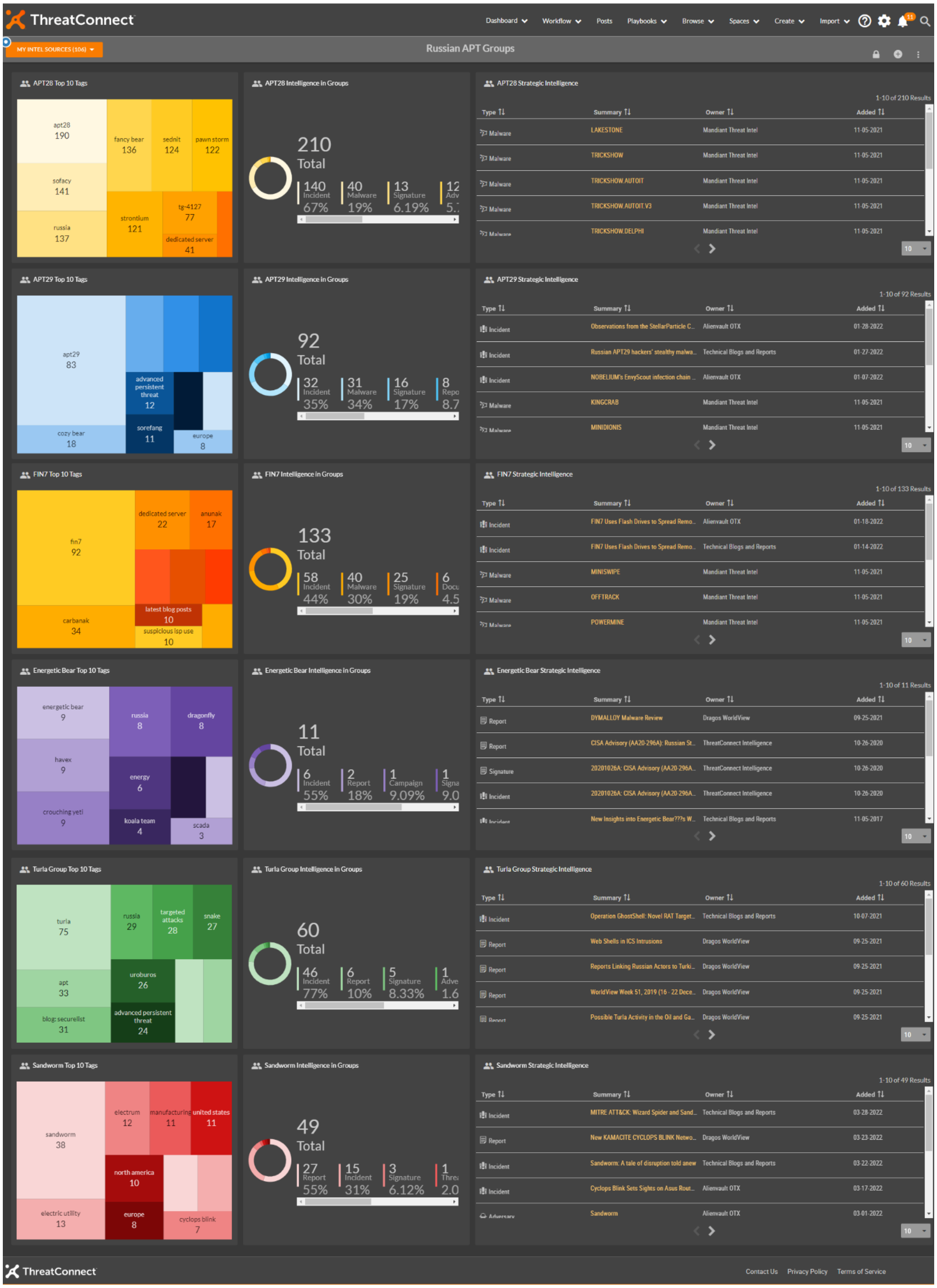
Aggregate: COUNT

Target: Choose...

Chart Type: Tree Map ✓

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.

Russian APT Groups Dashboard



APT28 Strategic Intelligence

1-10 of 210 Results

Type	Summary	Owner	Added
Malware	LAKESTONE	Mandiant Threat Intel	11-05-2021
Malware	TRICKSHOW	Mandiant Threat Intel	11-05-2021
Malware	TRICKSHOW.AUTOIT	Mandiant Threat Intel	11-05-2021
Malware	TRICKSHOW.AUTOIT.V3	Mandiant Threat Intel	11-05-2021
Malware	TRICKSHOW.DELPHI	Mandiant Threat Intel	11-05-2021

APT29 Strategic Intelligence

1-10 of 92 Results

Type	Summary	Owner	Added
Incident	Observations from the StellarParticle C...	Alienvault OTX	01-28-2022
Incident	Russian APT29 hackers' stealthy malwa...	Technical Blogs and Reports	01-27-2022
Incident	NOBELIUM's EnvyScout infection chain ...	Alienvault OTX	01-07-2022
Malware	KINGCRAB	Mandiant Threat Intel	11-05-2021
Malware	MINIDIONIS	Mandiant Threat Intel	11-05-2021

FIN7 Strategic Intelligence

1-10 of 133 Results

Type	Summary	Owner	Added
Incident	FIN7 Uses Flash Drives to Spread Remo...	Alienvault OTX	01-18-2022
Incident	FIN7 Uses Flash Drives to Spread Remo...	Technical Blogs and Reports	01-14-2022
Malware	MINISWIPE	Mandiant Threat Intel	11-05-2021
Malware	OFFTRACK	Mandiant Threat Intel	11-05-2021
Malware	POWERMINE	Mandiant Threat Intel	11-05-2021

Energetic Bear Strategic Intelligence

1-10 of 11 Results

Type	Summary	Owner	Added
Report	DYMALLOY Malware Review	Dragos WorldView	09-25-2021
Report	CISA Advisory (AA20-296A): Russian St...	ThreatConnect Intelligence	10-26-2020
Signature	20201026A: CISA Advisory (AA20-296A...	ThreatConnect Intelligence	10-26-2020
Incident	20201026A: CISA Advisory (AA20-296A...	ThreatConnect Intelligence	10-26-2020
Incident	New Insights into Energetic Bear???s W...	Technical Blogs and Reports	11-05-2017

Turla Group Strategic Intelligence

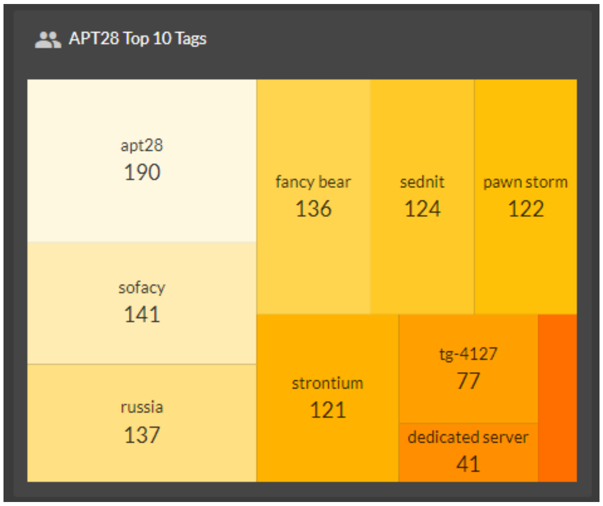
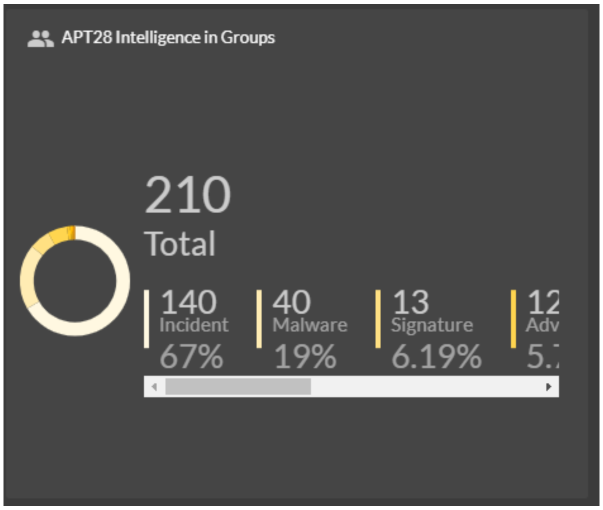
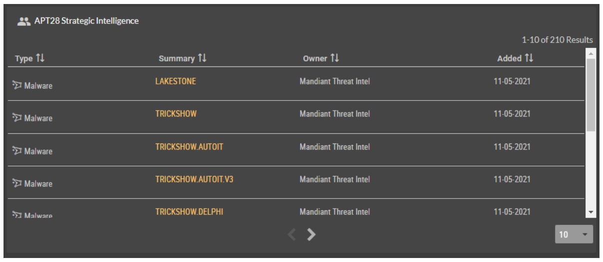
1-10 of 60 Results

Type	Summary	Owner	Added
Incident	Operation GhostShell: Novel RAT Target...	Technical Blogs and Reports	10-07-2021
Report	Web Shells in ICS Intrusions	Dragos WorldView	09-25-2021
Report	Reports Linking Russian Actors to Turki...	Dragos WorldView	09-25-2021
Report	WorldView Week 51, 2019 (16 - 22 Dece...	Dragos WorldView	09-25-2021
Report	Possible Turla Activity in the Oil and Ga...	Dragos WorldView	09-25-2021

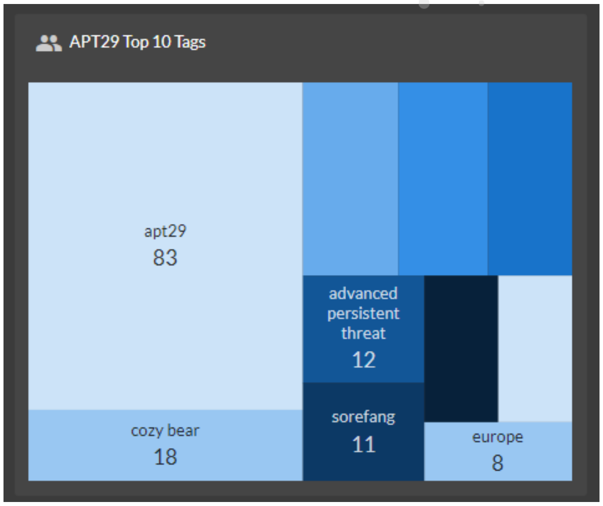
Sandworm Strategic Intelligence

1-10 of 49 Results

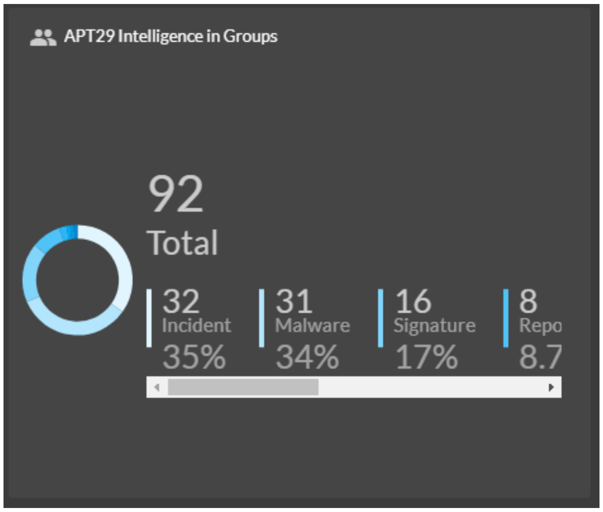
Type	Summary	Owner	Added
Incident	MITRE ATT&CK: Wizard Spider and Sand...	Technical Blogs and Reports	03-28-2022
Report	New KAMACITE CYCLOPS BLINK Netwo...	Dragos WorldView	03-23-2022
Incident	Sandworm: A tale of disruption told anew	Technical Blogs and Reports	03-22-2022
Incident	Cyclops Blink Sets Sights on Asus Rout...	Alienvault OTX	03-17-2022
Adversary	Sandworm	Alienvault OTX	03-01-2022

<table>
<tr><th>Card Build Information</th><th>Card Screenshot</th></tr>
<tr><td><strong>Title</strong>: APT28 Top 10 Tags
<strong>Display Type</strong>: Chart
<strong>Intelligence Sources</strong>: All
<strong>Query By</strong>: Groups
<strong>Advance Query</strong>: tag like "APT28"
<strong>Grouping</strong>: Top, 10, Tag
<strong>Chart Type</strong>: Tree Map</td><td>
</td></tr>
<tr><td><strong>Title</strong>: APT28 Intelligence in Groups
<strong>Display Type</strong>: Chart
<strong>Intelligence Sources</strong>: All
<strong>Query By</strong>: Groups
<strong>Advance Query</strong>: summary contains ("APT28","Sofacy","Fancy Bear") or tag in ("APT28")
<strong>Grouping</strong>:
<strong>Chart Type</strong>: Advanced Pie Chart</td><td>
</td></tr>
<tr><td><strong>Title</strong>: APT28 Strategic Intelligence
<strong>Display Type</strong>: Datatable
<strong>Intelligence Sources</strong>: All
<strong>Query By</strong>: Groups
<strong>Advance Query</strong>: summary contains ("APT28","Sofacy","Fancy Bear") or tag in ("APT28")
<strong>Grouping</strong>:
<strong>Chart Type</strong>:</td><td>
APT28 Strategic Intelligence
1-10 of 210 Results
<table>
<tr><th>Type ⇅</th><th>Summary ⇅</th><th>Owner ⇅</th><th>Added ⇅</th></tr>
<tr><td>Malware</td><td>LAKESTONE</td><td>Mandiant Threat Intel</td><td>11-05-2021</td></tr>
<tr><td>Malware</td><td>TRICKSHOW</td><td>Mandiant Threat Intel</td><td>11-05-2021</td></tr>
<tr><td>Malware</td><td>TRICKSHOW.AUTOIT</td><td>Mandiant Threat Intel</td><td>11-05-2021</td></tr>
<tr><td>Malware</td><td>TRICKSHOW.AUTOIT.V3</td><td>Mandiant Threat Intel</td><td>11-05-2021</td></tr>
<tr><td>Malware</td><td>TRICKSHOW.DELPHI</td><td>Mandiant Threat Intel</td><td>11-05-2021</td></tr>
</table>
</td></tr>
</table>

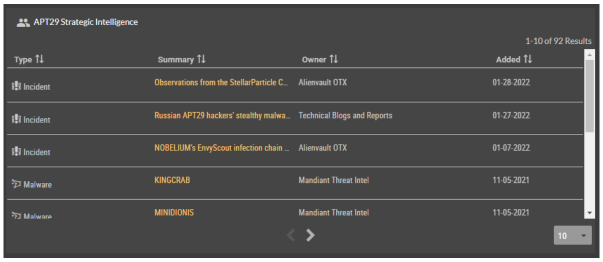
Title: APT29 Top 10 Tags
Display Type: Chart
Intelligence Sources: All
Query By: Groups
Advance Query: tag like "APT29"
Grouping: Top, 10, Tag
Chart Type: Tree Map



Title: APT29 Intelligence in Groups
Display Type: Chart
Intelligence Sources: All
Query By: Groups
Advance Query: summary contains ("APT29","Cozy Bear","CozyCar") or tag in ("APT29")
Grouping:
Chart Type: Advanced Pie Chart

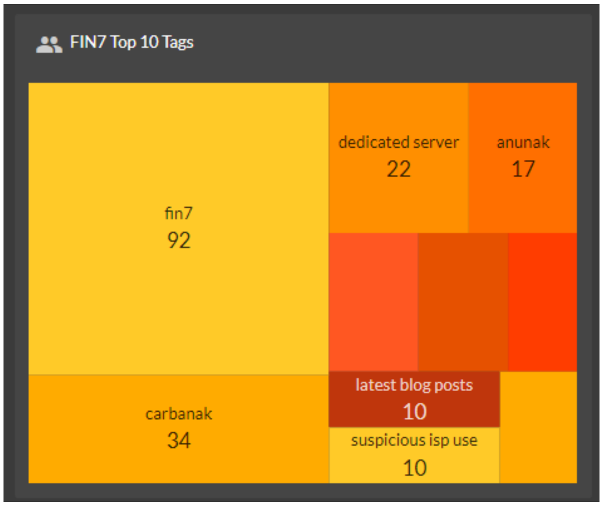
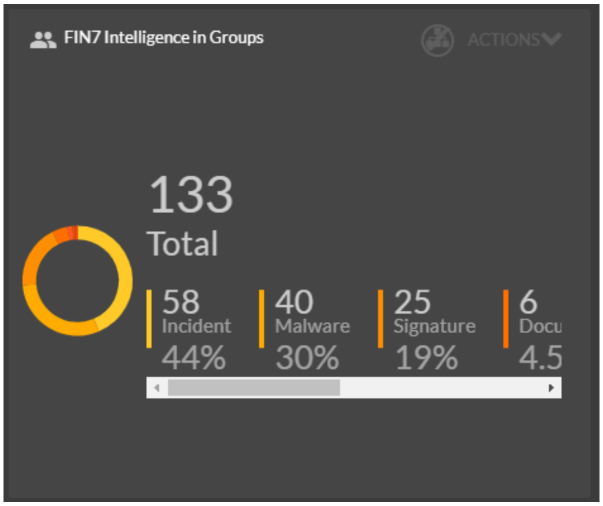
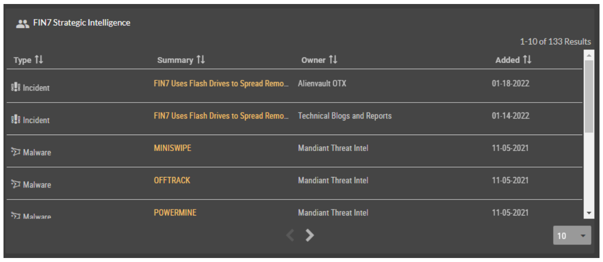


Title: APT29 Strategic Intelligence
Display Type: Datatable
Intelligence Sources: All
Query By: Groups
Advance Query: summary contains ("APT29","Cozy Bear","CozyCar") or tag in ("APT29")
Grouping:
Chart Type:


APT29 Strategic Intelligence

1-10 of 92 Results

Type ⇅	Summary ⇅	Owner ⇅	Added ⇅
Incident	Observations from the StellarParticle C...	Alienvault OTX	01-28-2022
Incident	Russian APT29 hackers' stealthy malwa...	Technical Blogs and Reports	01-27-2022
Incident	NOBELIUM's EnvyScout infection chain ...	Alienvault OTX	01-07-2022
Malware	KINGCRAB	Mandiant Threat Intel	11-05-2021
Malware	MINIDIONIS	Mandiant Threat Intel	11-05-2021

Card Build Information	**Card Screenshot**
Title: FIN7 Top 10 Tags **Display Type**: Chart **Intelligence Sources**: All **Query By**: Groups **Advance Query**: tag like "FIN7" **Grouping**: Top, 10, Tag **Chart Type**: Tree Map	
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	
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**:	

FIN7 Strategic Intelligence

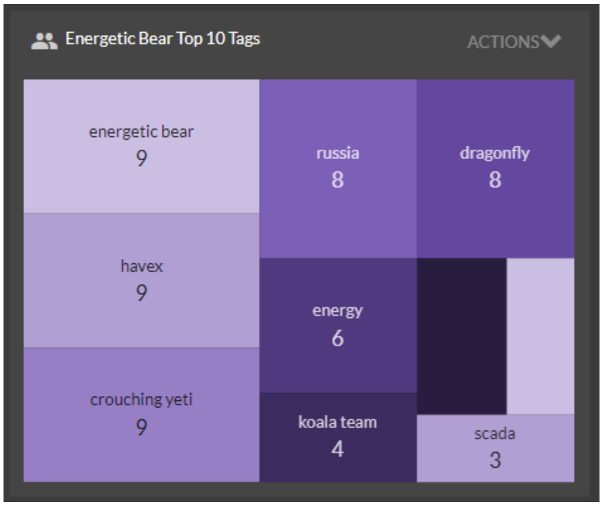
1-10 of 133 Results

Type ⇅	Summary ⇅	Owner ⇅	Added ⇅
Incident	FIN7 Uses Flash Drives to Spread Remo...	Alienvault OTX	01-18-2022
Incident	FIN7 Uses Flash Drives to Spread Remo...	Technical Blogs and Reports	01-14-2022
Malware	MINISWIPE	Mandiant Threat Intel	11-05-2021
Malware	OFFTRACK	Mandiant Threat Intel	11-05-2021
Malware	POWERMINE	Mandiant Threat Intel	11-05-2021

<table>
<tr><th>Card Build Information</th><th>Card Screenshot</th></tr>
<tr><td>

Title: Energetic Bear Top 10 Tags
Display Type: Chart
Intelligence Sources: All
Query By: Groups
Advance Query: tag like "Energetic Bear"
Grouping: Top, 10, Tag
Chart Type: Tree Map

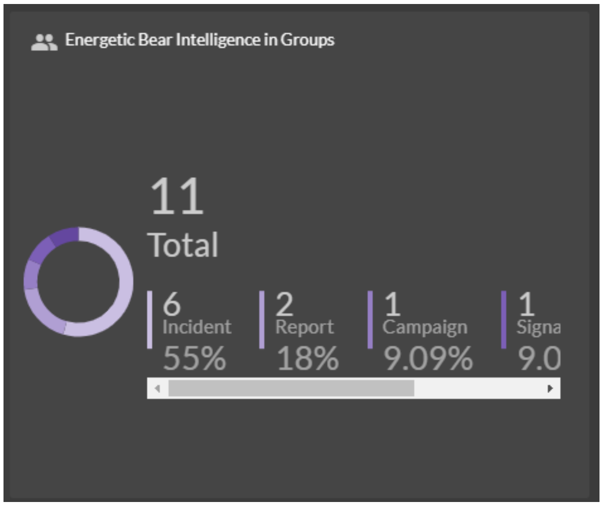
</td><td>



</td></tr>
<tr><td>

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

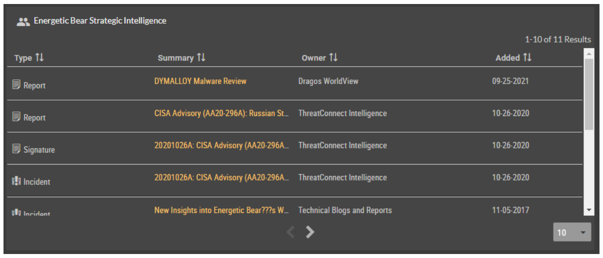
</td><td>



</td></tr>
<tr><td>

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:

</td><td>

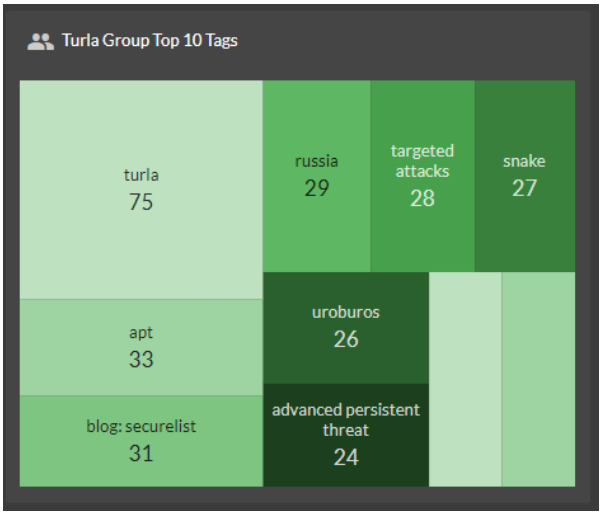
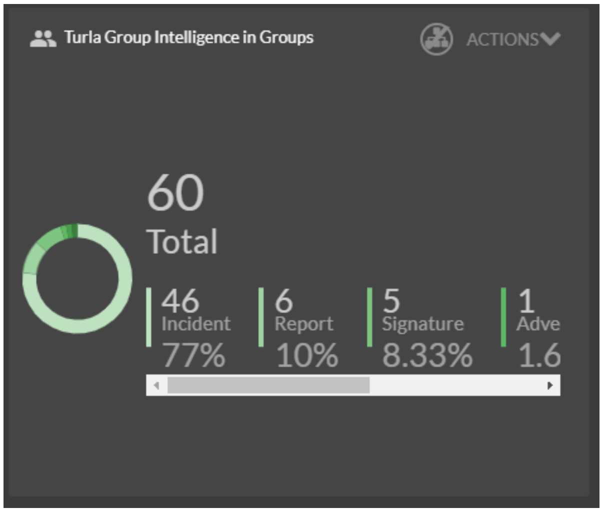
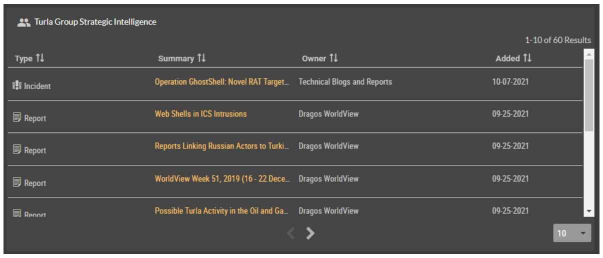


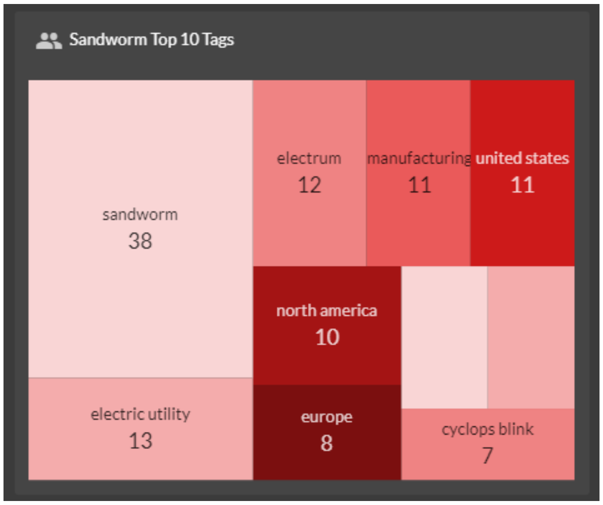
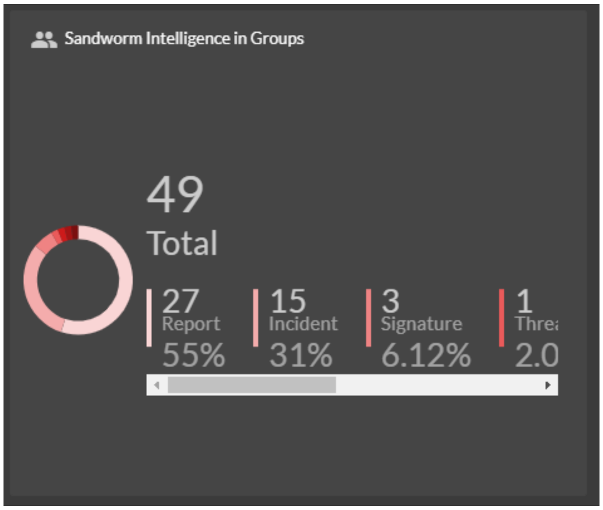
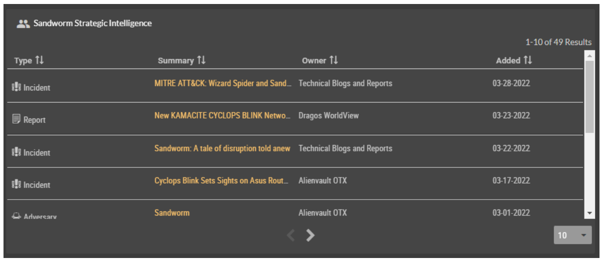
Energetic Bear Strategic Intelligence

1-10 of 11 Results

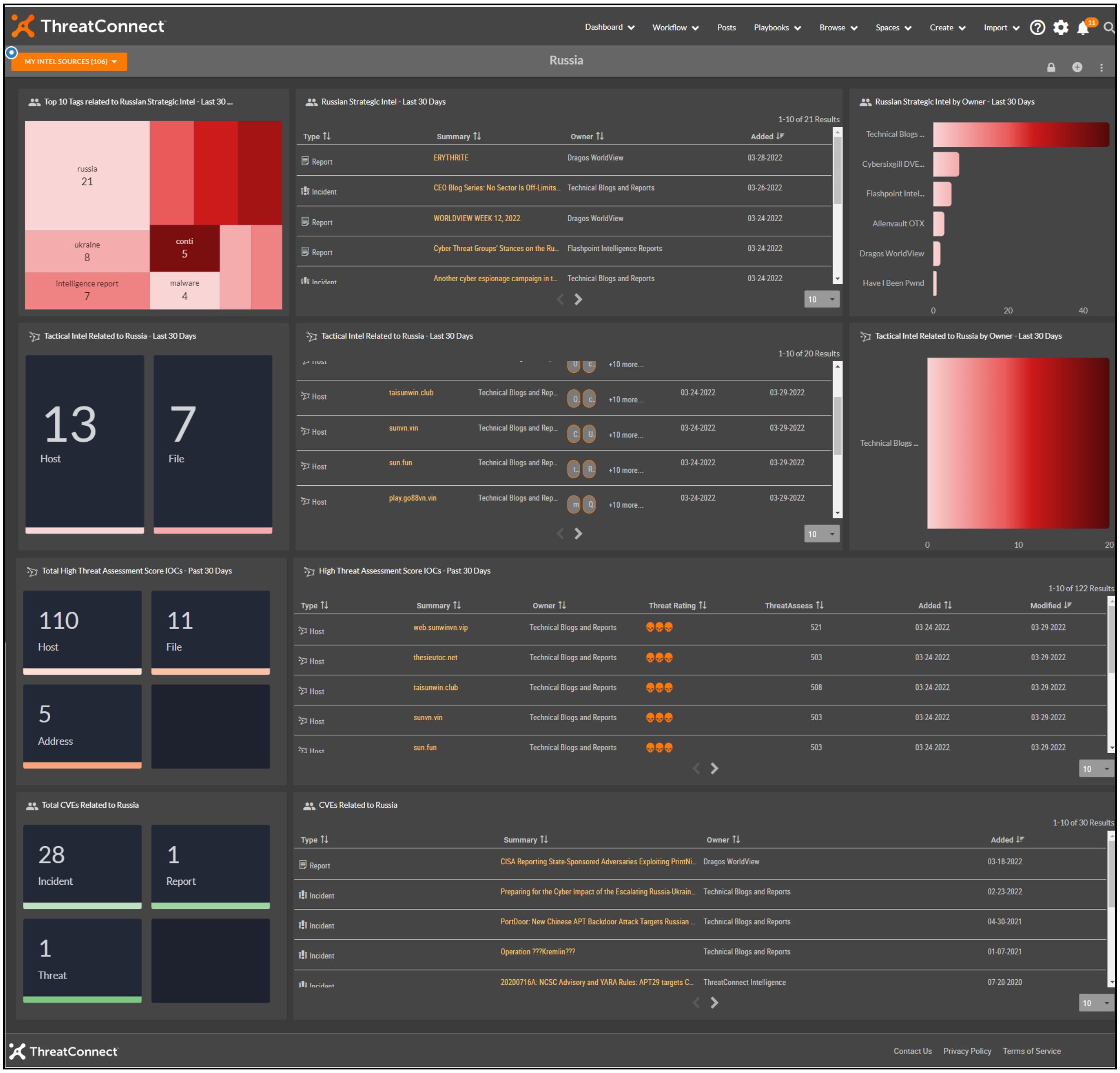
Type	Summary	Owner	Added
Report	DYMALLOY Malware Review	Dragos WorldView	09-25-2021
Report	CISA Advisory (AA20-296A): Russian St...	ThreatConnect Intelligence	10-26-2020
Signature	20201026A: CISA Advisory (AA20-296A...	ThreatConnect Intelligence	10-26-2020
Incident	20201026A: CISA Advisory (AA20-296A...	ThreatConnect Intelligence	10-26-2020
Incident	New Insights into Energetic Bear???s W...	Technical Blogs and Reports	11-05-2017

</td></tr>
</table>

<table>
<tr><th>Card Build Information</th><th>Card Screenshot</th></tr>
<tr><td><b>Title</b>: Turla Group Top 10 Tags
<b>Display Type</b>: Chart
<b>Intelligence Sources</b>: All
<b>Query By</b>: Groups
<b>Advance Query</b>: tag like "Turla"
<b>Grouping</b>: Top, 10, Tag
<b>Chart Type</b>: Tree Map</td><td>
</td></tr>
<tr><td><b>Title</b>: Turla Group Intelligence in Groups
<b>Display Type</b>: Chart
<b>Intelligence Sources</b>: All
<b>Query By</b>: Groups
<b>Advance Query</b>: summary contains ("Turla Group","Snake","Venomous Bear") or tag in ("Turla")
<b>Grouping</b>:
<b>Chart Type</b>: Advanced Pie Chart</td><td>
</td></tr>
<tr><td><b>Title</b>: Turla Group Strategic Intelligence
<b>Display Type</b>: Datatable
<b>Intelligence Sources</b>: All
<b>Query By</b>: Groups
<b>Advance Query</b>: summary contains ("Turla Group","Snake","Venomous Bear") or tag in ("Turla")
<b>Grouping</b>:
<b>Chart Type</b>:</td><td>
Turla Group Strategic Intelligence
1-10 of 60 Results
<table>
<tr><th>Type</th><th>Summary</th><th>Owner</th><th>Added</th></tr>
<tr><td>Incident</td><td>Operation GhostShell: Novel RAT Target...</td><td>Technical Blogs and Reports</td><td>10-07-2021</td></tr>
<tr><td>Report</td><td>Web Shells in ICS Intrusions</td><td>Dragos WorldView</td><td>09-25-2021</td></tr>
<tr><td>Report</td><td>Reports Linking Russian Actors to Turki...</td><td>Dragos WorldView</td><td>09-25-2021</td></tr>
<tr><td>Report</td><td>WorldView Week 51, 2019 (16 - 22 Dece...</td><td>Dragos WorldView</td><td>09-25-2021</td></tr>
<tr><td>Report</td><td>Possible Turla Activity in the Oil and Ga...</td><td>Dragos WorldView</td><td>09-25-2021</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Card Build Information</th><th>Card Screenshot</th></tr>
<tr><td><b>Title</b>: Sandworm Top 10 Tags
<b>Display Type</b>: Chart
<b>Intelligence Sources</b>: All
<b>Query By</b>: Groups
<b>Advance Query</b>: tag like "Sandworm"
<b>Grouping</b>: Top, 10, Tag
<b>Chart Type</b>: Tree Map</td><td>
</td></tr>
<tr><td><b>Title</b>: Sandworm Intelligence in Groups
<b>Display Type</b>: Chart
<b>Intelligence Sources</b>: All
<b>Query By</b>: Groups
<b>Advance Query</b>: summary contains ("Sandworm","Hades","Voodoo Bear") or tag in ("Sandworm")
<b>Grouping</b>:
<b>Chart Type</b>: Advanced Pie Chart</td><td>
</td></tr>
<tr><td><b>Title</b>: Sandworm Strategic Intelligence
<b>Display Type</b>: Datatable
<b>Intelligence Sources</b>: All
<b>Query By</b>: Groups
<b>Advance Query</b>: summary contains ("Sandworm","Hades","Voodoo Bear") or tag in ("Sandworm")
<b>Grouping</b>:
<b>Chart Type</b>:</td><td>
Sandworm Strategic Intelligence
1-10 of 49 Results
<table>
<tr><th>Type ⇅</th><th>Summary ⇅</th><th>Owner ⇅</th><th>Added ⇅</th></tr>
<tr><td>Incident</td><td>MITRE ATT&CK: Wizard Spider and Sand...</td><td>Technical Blogs and Reports</td><td>03-28-2022</td></tr>
<tr><td>Report</td><td>New KAMACITE CYCLOPS BLINK Netwo...</td><td>Dragos WorldView</td><td>03-23-2022</td></tr>
<tr><td>Incident</td><td>Sandworm: A tale of disruption told anew</td><td>Technical Blogs and Reports</td><td>03-22-2022</td></tr>
<tr><td>Incident</td><td>Cyclops Blink Sets Sights on Asus Rout...</td><td>Alienvault OTX</td><td>03-17-2022</td></tr>
<tr><td>Adversary</td><td>Sandworm</td><td>Alienvault OTX</td><td>03-01-2022</td></tr>
</table>
</td></tr>
</table>

Russian-specific Threat Intelligence Dashboard



Russia

Top 10 Tags related to Russian Strategic Intel - Last 30 ...

Russian Strategic Intel - Last 30 Days

1-10 of 21 Results

Type	Summary	Owner	Added
Report	ERYTHRITE	Dragos WorldView	03-28-2022
Incident	CEO Blog Series: No Sector Is Off-Limits...	Technical Blogs and Reports	03-26-2022
Report	WORLDVIEW WEEK 12, 2022	Dragos WorldView	03-24-2022
Report	Cyber Threat Groups' Stances on the Ru...	Flashpoint Intelligence Reports	03-24-2022
Incident	Another cyber espionage campaign in t...	Technical Blogs and Reports	03-24-2022

10

Russian Strategic Intel by Owner - Last 30 Days

Tactical Intel Related to Russia - Last 30 Days

13
Host

7
File

Tactical Intel Related to Russia - Last 30 Days

1-10 of 20 Results

Host			U. c.	+10 more...		
Host	taisunwin.club	Technical Blogs and Rep...	Q. c.	+10 more...	03-24-2022	03-29-2022
Host	sunvn.vin	Technical Blogs and Rep...	C. U.	+10 more...	03-24-2022	03-29-2022
Host	sun.fun	Technical Blogs and Rep...	t. R.	+10 more...	03-24-2022	03-29-2022
Host	play.go88vn.vin	Technical Blogs and Rep...	m Q.	+10 more...	03-24-2022	03-29-2022

10

Tactical Intel Related to Russia by Owner - Last 30 Days

Total High Threat Assessment Score IOCs - Past 30 Days

110
Host

11
File

5
Address

High Threat Assessment Score IOCs - Past 30 Days

1-10 of 122 Results

Type	Summary	Owner	Threat Rating	ThreatAssess	Added	Modified
Host	web.sunwinvn.vip	Technical Blogs and Reports	☠☠☠	521	03-24-2022	03-29-2022
Host	thesieutoc.net	Technical Blogs and Reports	☠☠☠	503	03-24-2022	03-29-2022
Host	taisunwin.club	Technical Blogs and Reports	☠☠☠	508	03-24-2022	03-29-2022
Host	sunvn.vin	Technical Blogs and Reports	☠☠☠	503	03-24-2022	03-29-2022
Host	sun.fun	Technical Blogs and Reports	☠☠☠	503	03-24-2022	03-29-2022

10

Total CVEs Related to Russia

28
Incident

1
Report

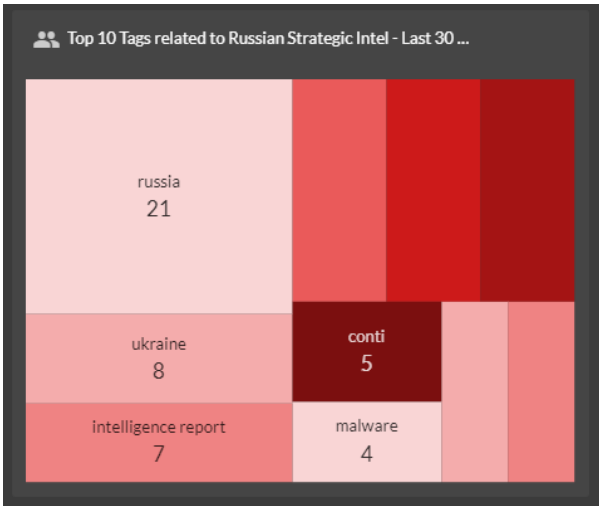
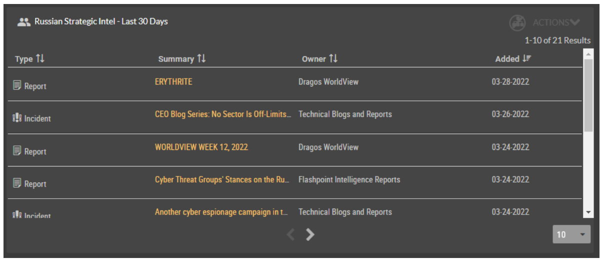
1
Threat

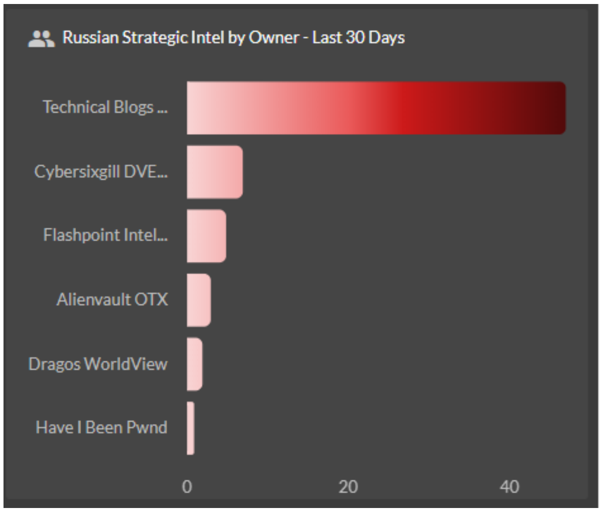
CVEs Related to Russia

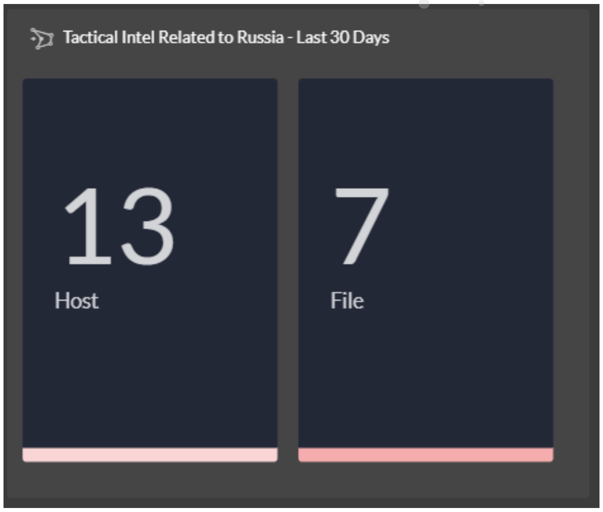
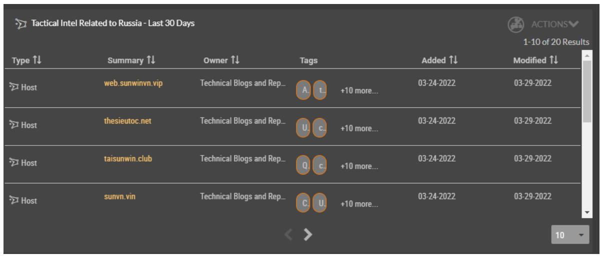
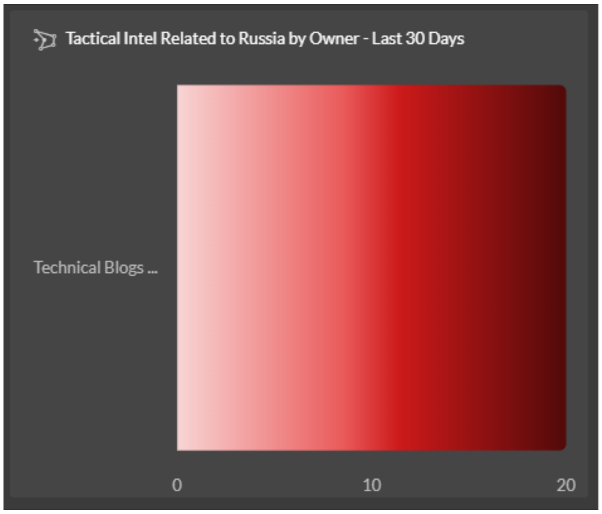
1-10 of 30 Results

Type	Summary	Owner	Added
Report	CISA Reporting State-Sponsored Adversaries Exploiting PrintNi...	Dragos WorldView	03-18-2022
Incident	Preparing for the Cyber Impact of the Escalating Russia-Ukrain...	Technical Blogs and Reports	02-23-2022
Incident	PortDoor: New Chinese APT Backdoor Attack Targets Russian ...	Technical Blogs and Reports	04-30-2021
Incident	Operation ???Kremlin???	Technical Blogs and Reports	01-07-2021
Incident	20200716A: NCSC Advisory and YARA Rules: APT29 targets C...	ThreatConnect Intelligence	07-20-2020

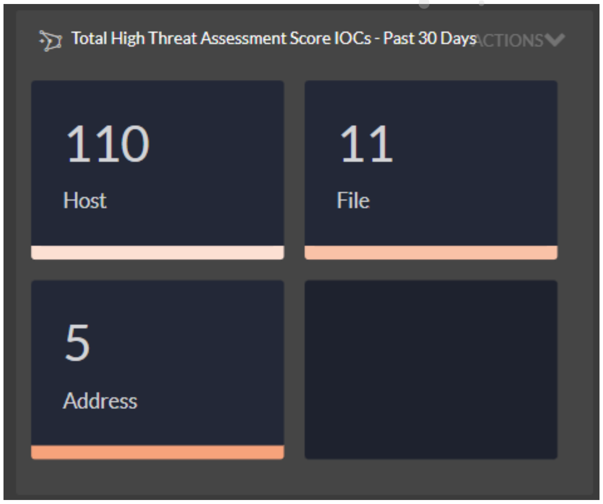
10

<table>
<tr><th>Card Build Information</th><th>Card Screenshot</th></tr>
<tr><td>**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</td><td>
Top 10 Tags related to Russian Strategic Intel - Last 30 ...
</td></tr>
<tr><td>**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:</td><td>
Russian Strategic Intel - Last 30 Days

1-10 of 21 Results
<table>
<tr><th>Type</th><th>Summary</th><th>Owner</th><th>Added</th></tr>
<tr><td>Report</td><td>ERYTHRITE</td><td>Dragos WorldView</td><td>03-28-2022</td></tr>
<tr><td>Incident</td><td>CEO Blog Series: No Sector Is Off-Limits...</td><td>Technical Blogs and Reports</td><td>03-26-2022</td></tr>
<tr><td>Report</td><td>WORLDVIEW WEEK 12, 2022</td><td>Dragos WorldView</td><td>03-24-2022</td></tr>
<tr><td>Report</td><td>Cyber Threat Groups' Stances on the Ru...</td><td>Flashpoint Intelligence Reports</td><td>03-24-2022</td></tr>
<tr><td>Incident</td><td>Another cyber espionage campaign in t...</td><td>Technical Blogs and Reports</td><td>03-24-2022</td></tr>
</table>
</td></tr>
<tr><td>**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</td><td>
Russian Strategic Intel by Owner - Last 30 Days
</td></tr>
</table>

<table>
<tr>
<td><b>Title</b>: Tactical Intel Related to Russia - Last 30 Days
<b>Display Type</b>: Chart
<b>Intelligence Sources</b>: All
<b>Query By</b>: Indicators
<b>Advance Query</b>: tag in ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 30 DAYS"
<b>Grouping</b>:
<b>Chart Type</b>: Number Cards</td>
<td>
</td>
</tr>
<tr>
<td><b>Title</b>: Tactical Intel Related to Russia - Last 30 Days
<b>Display Type</b>: Datatable
<b>Intelligence Sources</b>: All
<b>Query By</b>: Indicators
<b>Advance Query</b>: tag in ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 30 DAYS"
<b>Grouping</b>:
<b>Chart Type</b>:</td>
<td>
Tactical Intel Related to Russia - Last 30 Days
ACTIONS
1-10 of 20 Results
<table>
<tr><th>Type ⇅</th><th>Summary ⇅</th><th>Owner ⇅</th><th>Tags</th><th></th><th>Added ⇅</th><th>Modified ⇅</th></tr>
<tr><td>Host</td><td>web.sunwinvn.vip</td><td>Technical Blogs and Rep...</td><td>A. t..</td><td>+10 more...</td><td>03-24-2022</td><td>03-29-2022</td></tr>
<tr><td>Host</td><td>thesieutoc.net</td><td>Technical Blogs and Rep...</td><td>U. c..</td><td>+10 more...</td><td>03-24-2022</td><td>03-29-2022</td></tr>
<tr><td>Host</td><td>taisunwin.club</td><td>Technical Blogs and Rep...</td><td>Q. c..</td><td>+10 more...</td><td>03-24-2022</td><td>03-29-2022</td></tr>
<tr><td>Host</td><td>sunvn.vin</td><td>Technical Blogs and Rep...</td><td>C. U..</td><td>+10 more...</td><td>03-24-2022</td><td>03-29-2022</td></tr>
</table>
10</td>
</tr>
<tr>
<td><b>Title</b>: Tactical Intel Related to Russia by Owner - Last 30 Days
<b>Display Type</b>: Chart
<b>Intelligence Sources</b>: All
<b>Query By</b>: Indicators
<b>Advance Query</b>: tag in ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 30 DAYS"
<b>Grouping</b>: Owner Name
<b>Chart Type</b>: Horizontal Bar Chart</td>
<td>
</td>
</tr>
</table>

Title: Total High Threat Assessment Score IOCs - Past 30 Days
Display Type: Chart
Intelligence Sources: All
Query By: Indicators
Advance Query: tag in ("Russia", "Ukraine", "Wiper", "HermeticWiper", "Cyclops", "Whispergate", "Conti") and threatAssessScore >= 500 and dateAdded >= "NOW() - 30 DAYS"
Grouping:
Chart Type: Number Cards



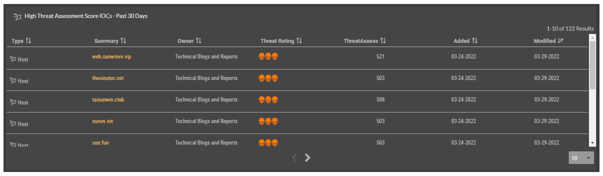
Total High Threat Assessment Score IOCs - Past 30 Days

110 Host

11 File

5 Address

Title: High Threat Assessment Score IOCs - Past 30 Days
Display Type: Datatable
Intelligence Sources: All
Query By: Indicators
Advance Query: tag in ("Russia", "Wiper", "HermeticWiper", "Cyclops", "Whispergate", "Conti","FoxBlade") and threatAssessScore >= 500 and dateAdded >= "NOW() - 30 DAYS"
Grouping:
Chart Type:

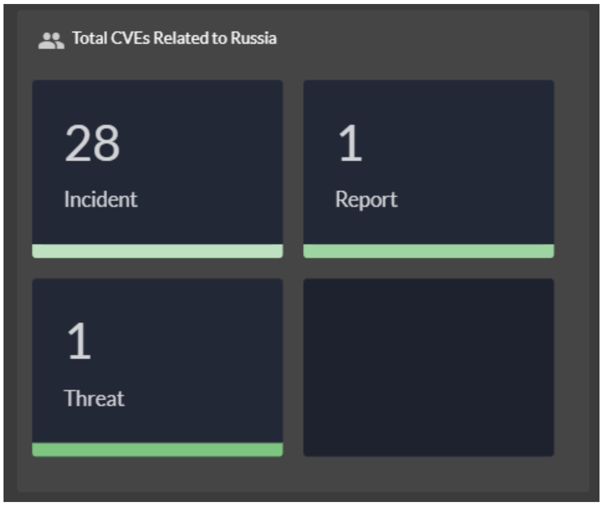


High Threat Assessment Score IOCs - Past 30 Days

1-10 of 122 Results

Type	Summary	Owner	Threat Rating	ThreatAssess	Added	Modified
Host	web.sunwinvn.vip	Technical Blogs and Reports	●●●	521	03-24-2022	03-29-2022
Host	thesieutoc.net	Technical Blogs and Reports	●●●	503	03-24-2022	03-29-2022
Host	taisunwin.club	Technical Blogs and Reports	●●●	508	03-24-2022	03-29-2022
Host	sunvn.vin	Technical Blogs and Reports	●●●	503	03-24-2022	03-29-2022
Host	sun.fun	Technical Blogs and Reports	●●●	503	03-24-2022	03-29-2022

Title: Total CVEs Related to Russia
Display Type: Chart
Intelligence Sources: All
Query By: Groups
Advance Query: tag in ("Russia", "Russian") and tag like "CVE%"
Grouping:
Chart Type: Number Cards



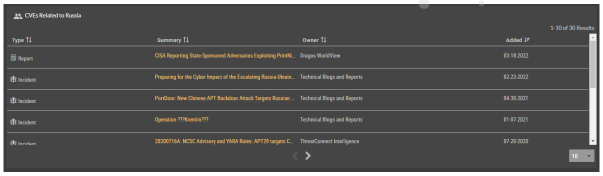
Total CVEs Related to Russia

28 Incident

1 Report

1 Threat

Title: CVEs Related to Russia
Display Type: Datatable
Intelligence Sources: All
Query By: Groups
Advance Query: tag in ("Russia", "Russian") and tag like "CVE%"
Grouping:
Chart Type:



CVEs Related to Russia

1-10 of 30 Results

Type	Summary	Owner	Added
Report	CISA Reporting State-Sponsored Adversaries Exploiting PrintNi...	Dragos WorldView	03-18-2022
Incident	Preparing for the Cyber Impact of the Escalating Russia-Ukrain...	Technical Blogs and Reports	02-23-2022
Incident	PortDoor: New Chinese APT Backdoor Attack Targets Russian ...	Technical Blogs and Reports	04-30-2021
Incident	Operation ???Kremlin???	Technical Blogs and Reports	01-07-2021
Incident	20200716A: NCSC Advisory and YARA Rules: APT29 targets C...	ThreatConnect Intelligence	07-20-2020

10