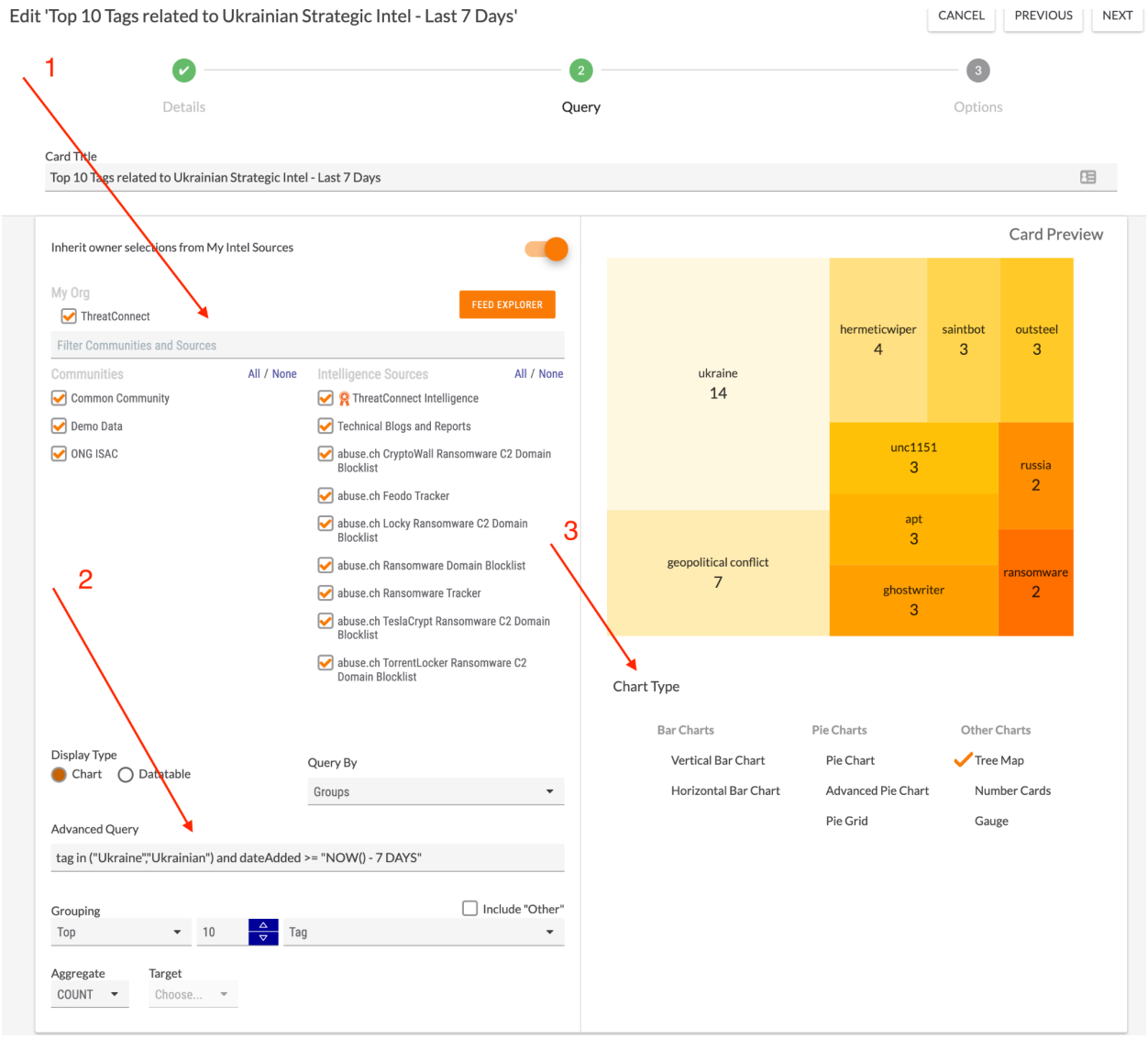
Ukraine Conflict Threat Intelligence Dashboards

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

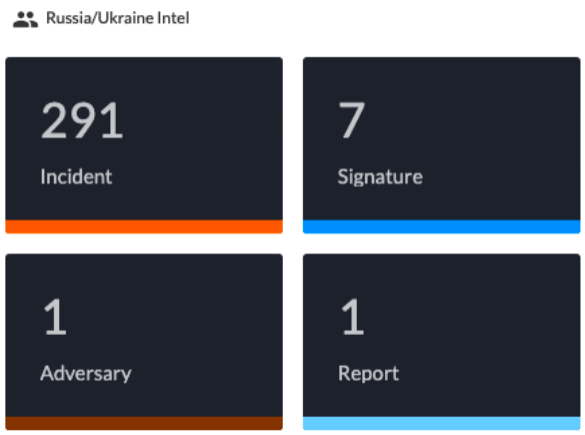
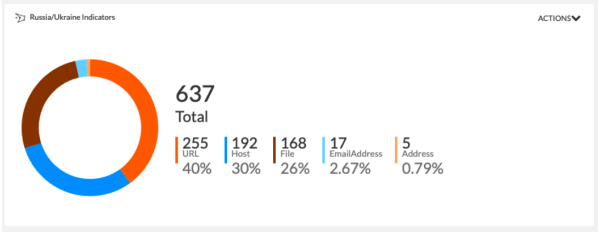
P: 1.800.965.2708 | **F:** +1.703.229.4489
www.ThreatConnect.com

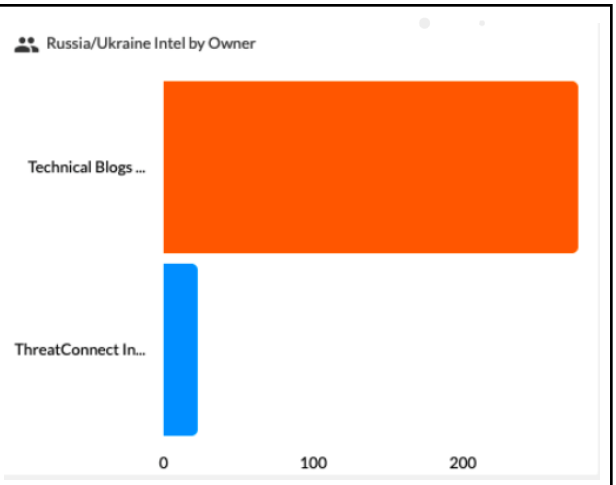
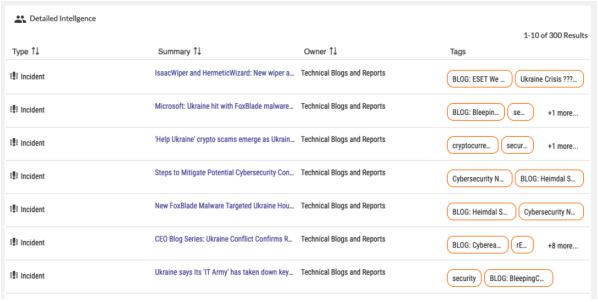
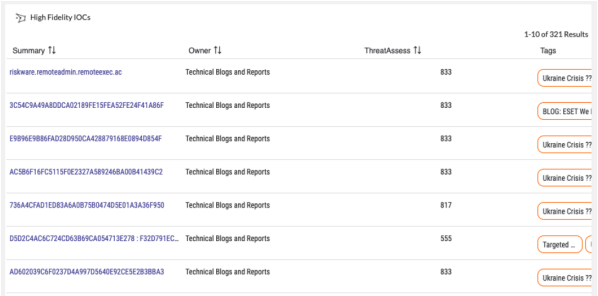
There are two example dashboards provided by ThreatConnect. The first is a compact dashboard while the second is one that offers additional depth of detail. For each dashboard, the card details that populate the dashboard are provided along with an example screenshot.

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).

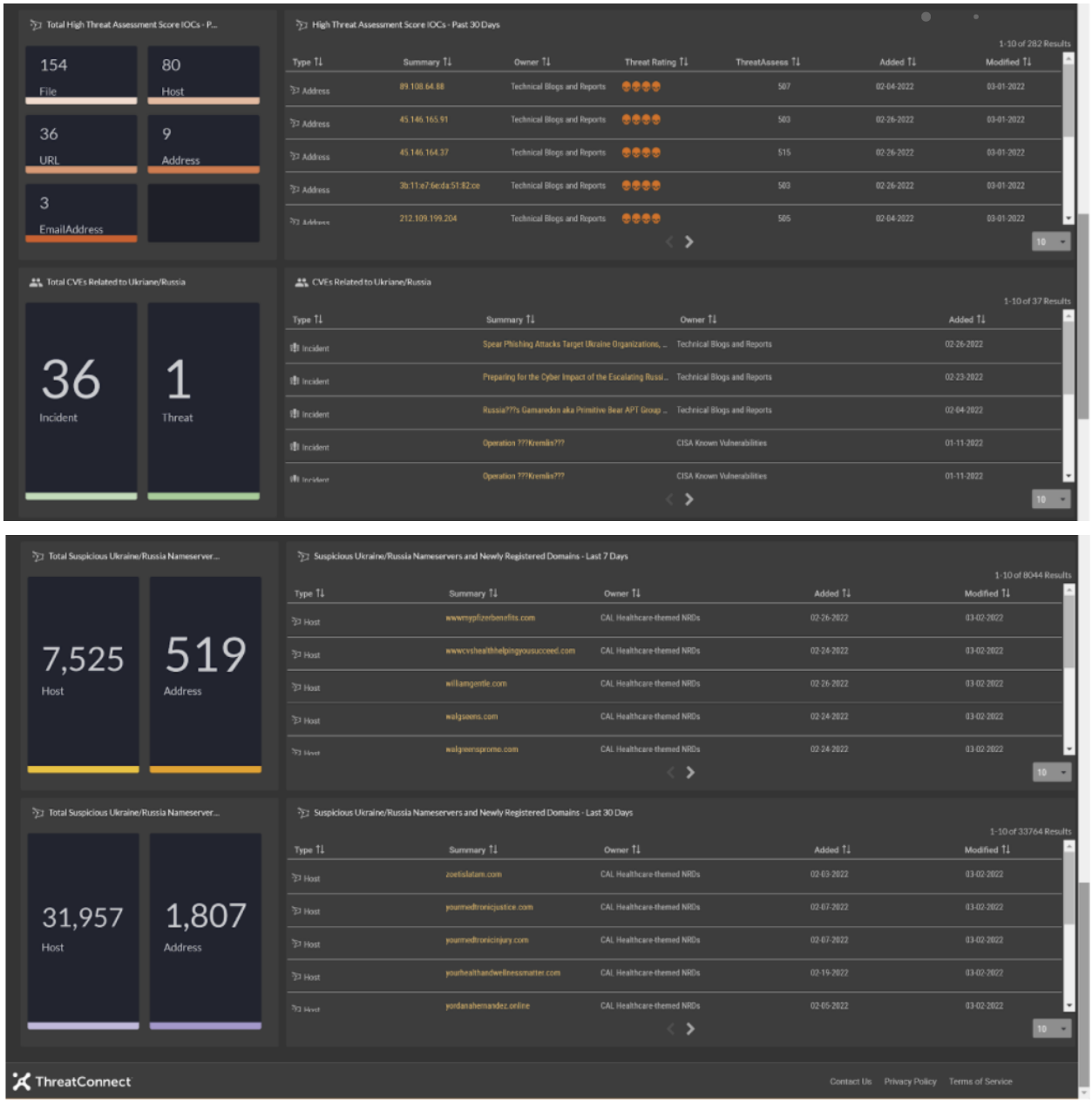


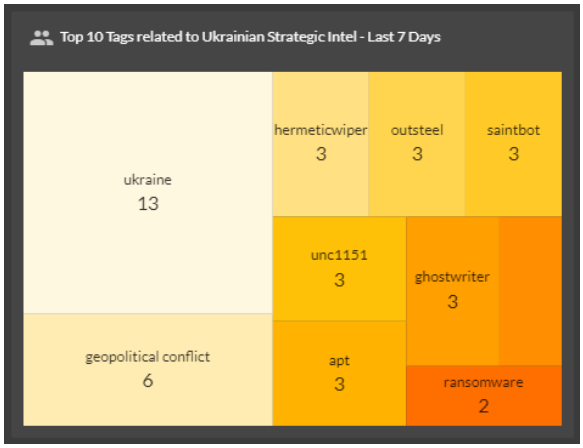
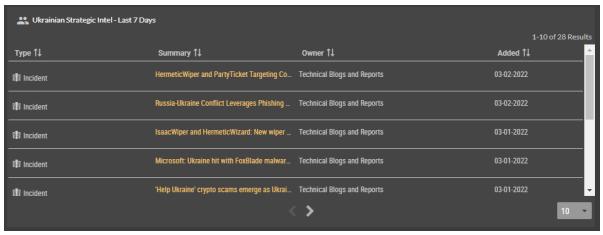
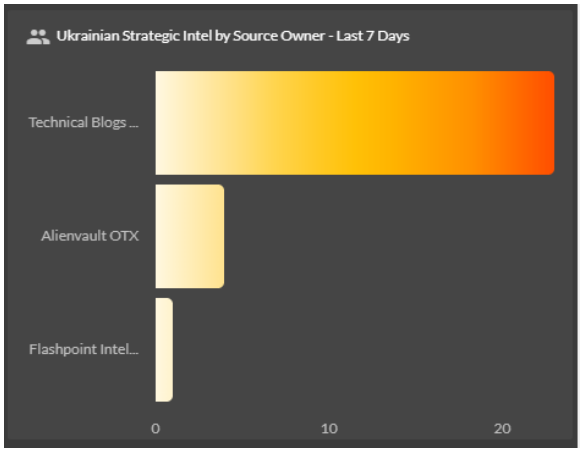
Dashboard Example #1 - Compact

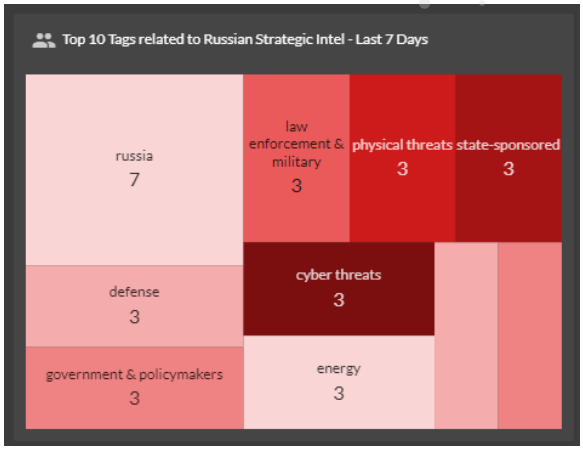
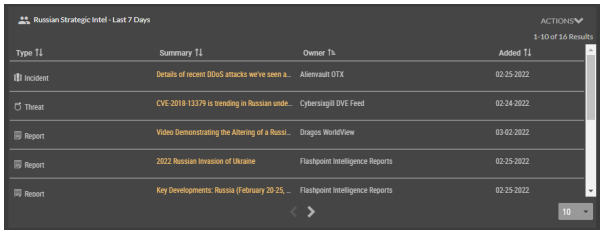
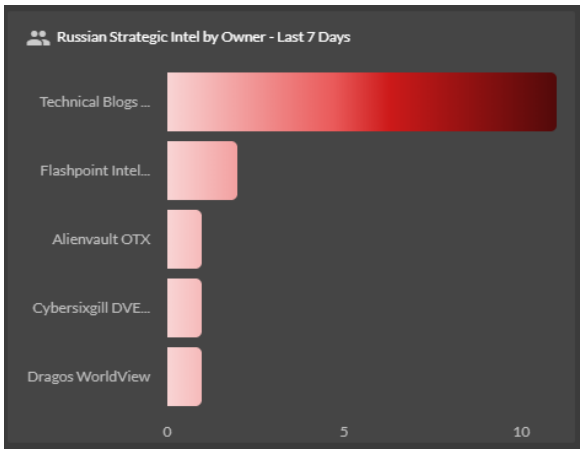
Card Build Information	Card Screenshot
Title: Russia/Ukraine Intel **Display Type**: Chart **Intelligence Sources**: All **Query By**: Groups **Advance Query**: dateAdded > "02-23-2022" and hasTag(summary like "ukrain%" or summary like "russia%") or summary contains "russia" or summary contains "ukraine" **Grouping**: Top 25 • Aggregate = COUNT **Chart Type**: Number Cards	
Title: Russia / Ukraine Indicators **Display Type**: Chart **Intelligence Sources**: All **Query By**: Indicators **Advance Query**: dateAdded > "02-23-2022" and hasTag(summary like "ukrain%" or summary like "russia%") or summary contains "russia" or summary contains "ukraine" **Grouping**: Top 25 • Aggregate = COUNT **Chart Type**: Advanced Pie Chart	

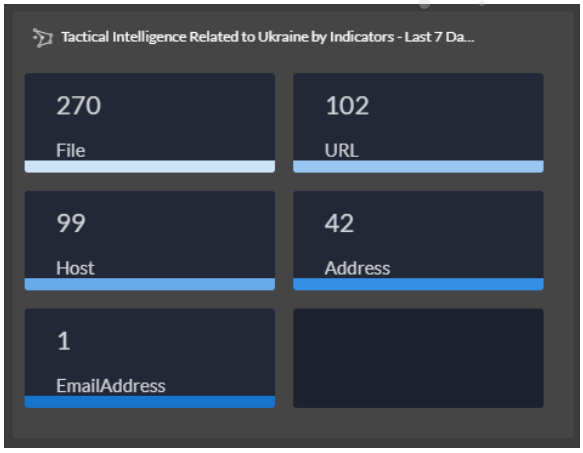
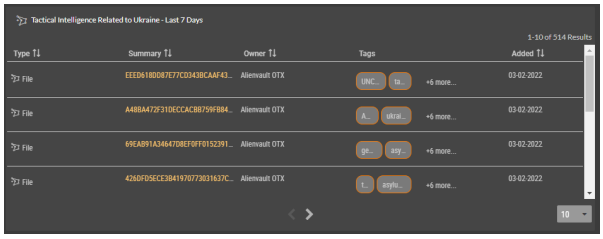
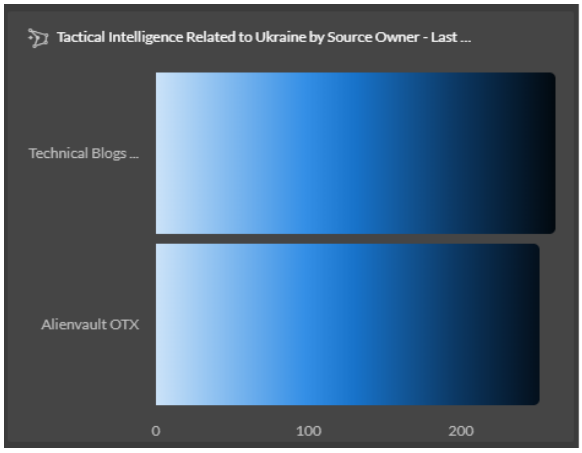
Title: Russia/Ukraine Intel by Owner **Display Type**: Chart **Intelligence Sources**: All **Query By**: Groups **Advance Query**: dateAdded > "02-23-2022" and hasTag(summary like "ukrain%" or summary like "russia%") or summary contains "russia" or summary contains "ukraine" **Grouping**: Top 25 • Aggregate = COUNT **Chart Type**: Horizontal Bar Chart	
Title: Detailed Intelligence **Display Type**: Datatable **Intelligence Sources**: All **Query By**: Groups **Advance Query**: dateAdded > "02-23-2022" and hasTag(summary like "ukrain%" or summary like "russia%") or summary contains "russia" or summary contains "ukraine" **Columns**: Type, Summary, Owner, Tags	
Title: High Fidelity IOCs **Display Type**: Datatable **Intelligence Sources**: All **Query By**: Indicators **Advance Query**: (dateAdded > "02-23-2022" and hasTag(summary like "ukrain%" or summary like "russia%") or summary contains "russia" or summary contains "ukraine") and threatAssessScore >= 500 **Columns**: Summary, Owner, ThreatAssess, Tags, Added	

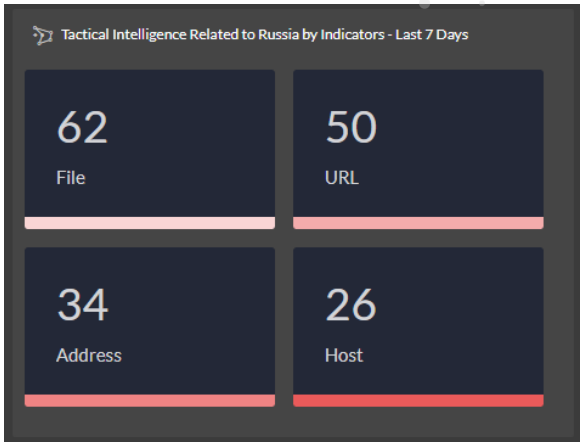
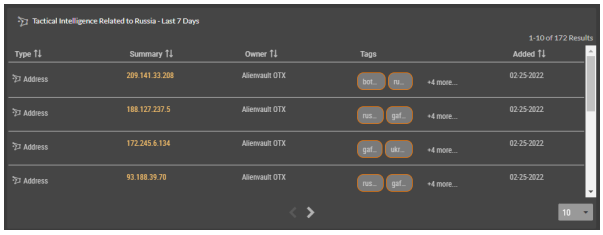
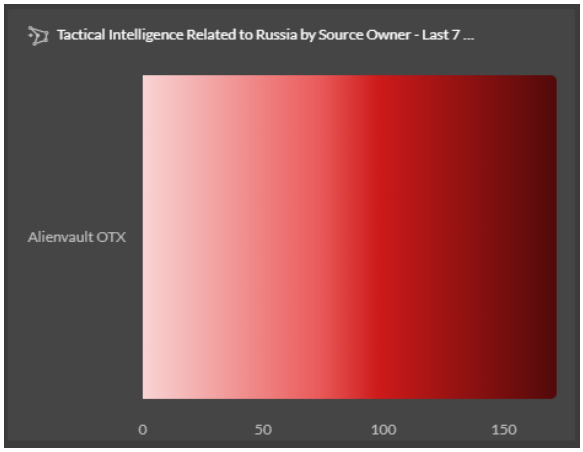
Dashboard Example #2 - Detailed

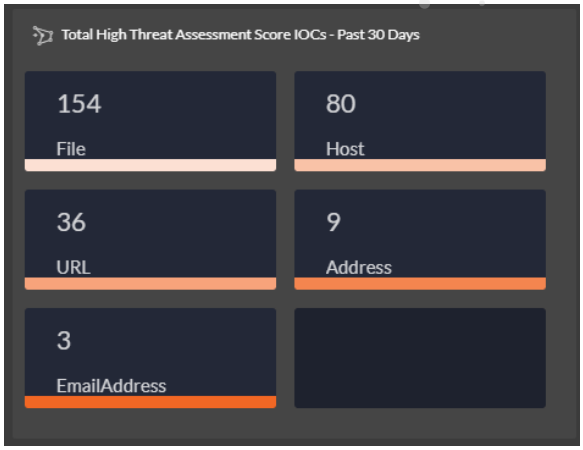
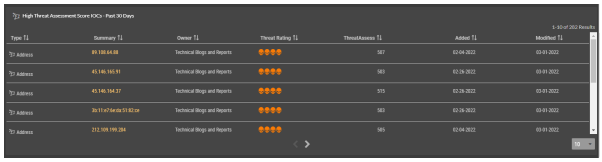
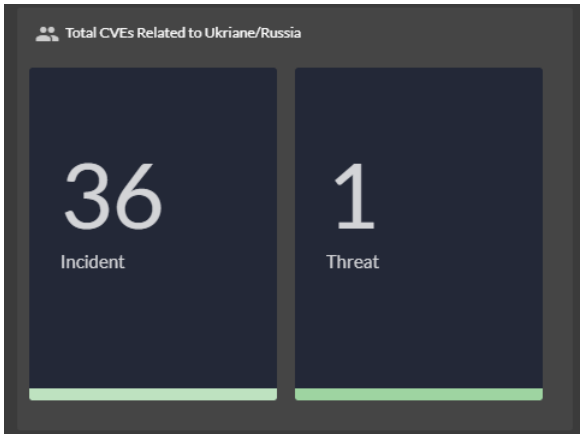
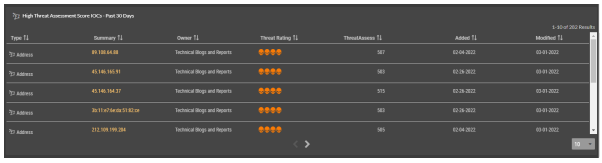

Total High Threat Assessment Score IOCs - P...
154
File
80
Host
36
URL
9
Address
3
EmailAddress
High Threat Assessment Score IOCs - Past 30 Days
1-10 of 282 Results
Type
Summary
Owner
Threat Rating
ThreatAssess
Added
Modified
Address
89.108.64.88
Technical Blogs and Reports
587
02-04-2022
03-01-2022
Address
45.146.165.91
Technical Blogs and Reports
583
02-26-2022
03-01-2022
Address
45.146.164.37
Technical Blogs and Reports
515
02-26-2022
03-01-2022
Address
3b:11:e7:6e:da:51:82:co
Technical Blogs and Reports
583
02-26-2022
03-01-2022
Address
212.109.199.204
Technical Blogs and Reports
585
02-04-2022
03-01-2022
Total CVEs Related to Ukriane/Russia
36
Incident
1
Threat
CVEs Related to Ukriane/Russia
1-10 of 37 Results
Type
Summary
Owner
Added
Incident
Spear Phishing Attacks Target Ukraine Organizations, ...
Technical Blogs and Reports
02-26-2022
Incident
Preparing for the Cyber Impact of the Escalating Russi...
Technical Blogs and Reports
02-23-2022
Incident
Russia???s Gamaredon aka Primitive Bear APT Group ...
Technical Blogs and Reports
02-04-2022
Incident
Operation ???Kremlin???
CISA Known Vulnerabilities
01-11-2022
Incident
Operation ???Kremlin???
CISA Known Vulnerabilities
01-11-2022
Total Suspicious Ukraine/Russia Nameserver...
7,525
Host
519
Address
Suspicious Ukraine/Russia Nameservers and Newly Registered Domains - Last 7 Days
1-10 of 8044 Results
Type
Summary
Owner
Added
Modified
Host
wwwmypfizerbenefits.com
CAL Healthcare-themed NRDs
02-26-2022
03-02-2022
Host
wwwcvshealthhelpingyousucceed.com
CAL Healthcare-themed NRDs
02-24-2022
03-02-2022
Host
wilkamgentle.com
CAL Healthcare-themed NRDs
02-26-2022
03-02-2022
Host
walgseens.com
CAL Healthcare-themed NRDs
02-24-2022
03-02-2022
Host
walgreenspromo.com
CAL Healthcare-themed NRDs
02-24-2022
03-02-2022
Total Suspicious Ukraine/Russia Nameserver...
31,957
Host
1,807
Address
Suspicious Ukraine/Russia Nameservers and Newly Registered Domains - Last 30 Days
1-10 of 33764 Results
Type
Summary
Owner
Added
Modified
Host
zoetislatam.com
CAL Healthcare-themed NRDs
02-03-2022
03-02-2022
Host
yourmedtronicjustice.com
CAL Healthcare-themed NRDs
02-07-2022
03-02-2022
Host
yourmedtronicinjury.com
CAL Healthcare-themed NRDs
02-07-2022
03-02-2022
Host
yourhealthandwellnessmatter.com
CAL Healthcare-themed NRDs
02-19-2022
03-02-2022
Host
yordanahernandez.online
CAL Healthcare-themed NRDs
02-05-2022
03-02-2022
ThreatConnect
Contact Us
Privacy Policy
Terms of Service

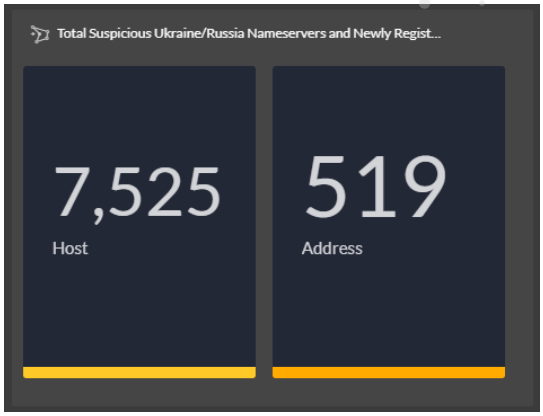
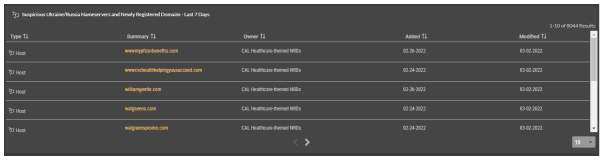
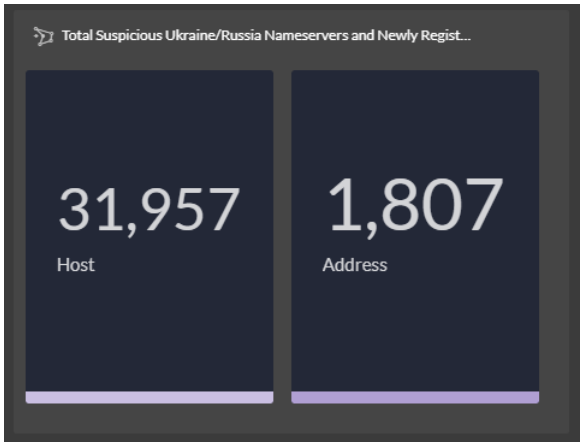
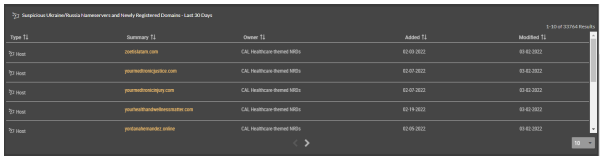
Card Build Information	Card Screenshot
Title: Top 10 Tags related to Ukrainian Strategic Intel - Last 7 Days **Intelligence Sources**: All **Display Type**: Chart **Query By**: Groups **Advanced Query**: tag in ("Ukraine","Ukrainian") and dateAdded >= "NOW() - 7 DAYS" **Grouping**: Tag • Top: 10 **Chart Type**: Tree Map	
Title: Ukrainian Strategic Intel - Last 7 Days **Intelligence Sources**: All **Display Type**: Datatable **Query By**: Groups **Advanced Query**: summary contains ("Ukraine","Ukrainian") and dateAdded >= "NOW() - 7 DAYS"	
Title: Ukrainian Strategic Intel by Source Owner - Last 7 Days **Intelligence Sources**: All **Display Type**: Chart **Query By**: Groups **Advanced Query**: summary contains ("Ukraine","Ukrainian") and dateAdded >= "NOW() - 7 DAYS" **Grouping**: Owner Name **Chart Type**: Horizontal Bar Chart	

Title: Top 10 Tags related to Russian Strategic Intel - Last 7 Days **Intelligence Sources**: All **Display Type**: Chart **Query By**: Groups **Advanced Query**: tag in ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 7 DAYS" **Grouping**: Tag **Top**: 10 **Chart Type**: Tree Map	
Title: Russian Strategic Intel - Last 7 Days Intelligence Sources: All **Display Type**: Datatable **Query By**: Groups **Advanced Query**: summary contains ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 7 DAYS"	
Title: Russian Strategic Intel by Owner - Last 7 Days **Intelligence Sources**: All **Display Type**: Chart **Query By**: Groups **Advanced Query**: summary contains ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 7 DAYS" **Grouping**: Owner Name **Chart Type**: Horizontal Bar Chart	

Title: Tactical Intelligence Related to Ukraine by Indicators - Last 7 Days **Intelligence Sources**: All **Display Type**: Chart **Query By**: Indicators **Advanced Query**: tag in ("Ukraine","Ukrainian") and dateAdded >= "NOW() - 7 DAYS" **Grouping**: Type Name **Chart Type**: Number Cards	
Title: Tactical Intelligence Related to Ukraine - Last 7 Days **Intelligence Sources**: All **Display Type**: Datatable **Query By**: Indicators **Advanced Query**: tag in ("Ukraine","Ukrainian") and dateAdded >= "NOW() - 7 DAYS"	
Title: Tactical Intelligence Related to Ukraine by Source Owner - Last 7 Days Intelligence Sources: All **Display Type**: Chart **Query By**: Indicators **Advanced Query**: tag in ("Ukraine","Ukrainian") and dateAdded >= "NOW() - 7 DAYS" **Grouping**: Owner Name **Chart Type**: Horizontal Bar Chart	

Title: Tactical Intelligence Related to Russia by Indicators - Last 7 Days **Intelligence Sources**: All **Display Type**: Chart **Query By**: Indicators **Advanced Query**: tag in ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 7 DAYS" **Chart Type**: Number Cards	
Title: Tactical Intelligence Related to Russia - Last 7 Days **Intelligence Sources**: All **Display Type**: Datatable **Query By**: Indicators **Advanced Query**: tag in ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 7 DAYS"	
Title: Tactical Intelligence Related to Russia by Source Owner - Last 7 Days **Intelligence Sources**: All **Display Type**: Chart **Query By**: Indicators **Advanced Query**: tag in ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 7 DAYS" **Grouping**: Owner Name **Chart Type**: Horizontal Bar Chart	

Title: Total High Threat Assessment Score IOCs - Past 30 Days **Intelligence Sources**: All **Display Type**: Chart **Query By**: Indicators **Advanced Query**: tag in ("Russia","Russian","Soviet Union") and dateAdded >= "NOW() - 7 DAYS" **Chart Type**: Number Cards	
Title: High Threat Assessment Score IOCs - Past 30 Days **Intelligence Sources**: All **Display Type**: Datatable **Query By**: Indicators **Advanced Query**: tag in ("Russia", "Ukraine", "Wiper", "HermeticWiper", "Cyclops", "Whispergate", "Conti","FoxBlade") and threatAssessScore >= 500 and dateAdded >= "NOW() - 30 DAYS"	
Title: Total CVEs Related to Ukraine/Russia **Intelligence Sources**: All **Display Type**: Chart **Query By**: Groups **Advanced Query**: tag in ("Russia", "Russian", "Ukraine", "Ukrainian") and tag like "CVE%" Chart Type: Number Cards	
Title: CVEs Related to Ukriane/Russia **Intelligence Sources**: All **Display Type**: Datatable **Query By**: Groups **Advanced Query**: tag in ("Russia", "Russian", "Ukraine", "Ukrainian") and tag like "CVE%"	

Title: Total Suspicious Ukraine/Russia Nameservers and Newly Registered Domains - Last 7 Days **Intelligence Sources**: CAL sources only **Display Type**: Chart **Query By**: Indicators **Advanced Query**: tag in ("Host.RecentlyRegistered.7D","Rel.NSClients.Malicious","DNSHost.Malicious.Current","Usage.DedicatedServer.Suspected","Ukraine","Russia","Russian","Ukrainian") and dateAdded >= "NOW() - 7 DAYS" **Chart Type**: Number Cards	
Title: Suspicious Ukraine/Russia Nameservers and Newly Registered Domains - Last 7 Days **Intelligence Sources**: CAL sources only **Display Type**: Datatable **Query By**: Indicators **Advanced Query**: tag in ("Host.RecentlyRegistered.7D","Rel.NSClients.Malicious","DNSHost.Malicious.Current","Usage.DedicatedServer.Suspected") and dateAdded >= "NOW() - 7 DAYS"	
Title: Total Suspicious Ukraine/Russia Nameservers and Newly Registered Domains - Last 30 Days **Intelligence Sources**: CAL sources only **Display Type**: Chart **Query By**: Indicators **Advanced Query**: tag in ("Host.RecentlyRegistered.7D","Rel.NSClients.Malicious","DNSHost.Malicious.Current","Usage.DedicatedServer.Suspected","Ukraine","Russia","Russian","Ukrainian") and dateAdded >= "NOW() - 30 DAYS" **Chart Type**: Number Cards	
Title: Suspicious Ukraine/Russia Nameservers and Newly Registered Domains - Last 30 Days **Intelligence Sources**: CAL sources only **Display Type**: Datatable **Query By**: Indicators **Advanced Query**: tag in ("Host.RecentlyRegistered.7D","Rel.NSClients.Malicious","DNSHost.Malicious.Current","Usage.DedicatedServer.Suspected") and dateAdded >= "NOW() - 30 DAYS"=