



# THREATCONNECT™

**THE INDUSTRY'S MOST WIDELY-ADOPTED  
THREAT INTELLIGENCE PLATFORM (TIP)**

# THE THREATCONNECT PLATFORM

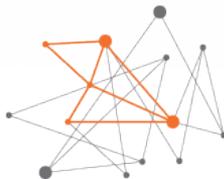
## AGGREGATE



Aggregate all available threat data in one place, using one platform.



## ANALYZE



Identify patterns quickly and identify threat actors further upstream.



## ACT



Take decisive action fast by uniting your team through data integration.

# INTEGRATIONS

# USE CASES



## SECURITY ANALYST

With ThreatConnect®, you now have a comprehensive platform to aggregate data into a common workable format, improving the speed and accuracy of your analysis. Our platform helps you work faster and more efficiently so you can detect threats and take action further upstream.



## SECURITY DIRECTOR

With ThreatConnect®, you can maximize the value of your threat intelligence by tracking historical data, fusing internal incidents with external information, and providing an opportunity for sharing threat data and community validation with trusted and secure Communities.



## CISO

ThreatConnect® allows you to empower your entire security team with a single platform that bridges process and data. With ThreatConnect, you'll understand more about who is attacking you and the methods they use, so you can better protect your most valuable assets.



## CEO/ BOARD

With ThreatConnect®, your CISO will be able to educate you and the Board on your most pressing cybersecurity challenges, so you can lead decisively and preserve the integrity of your brand.



## ISAC / ISAO

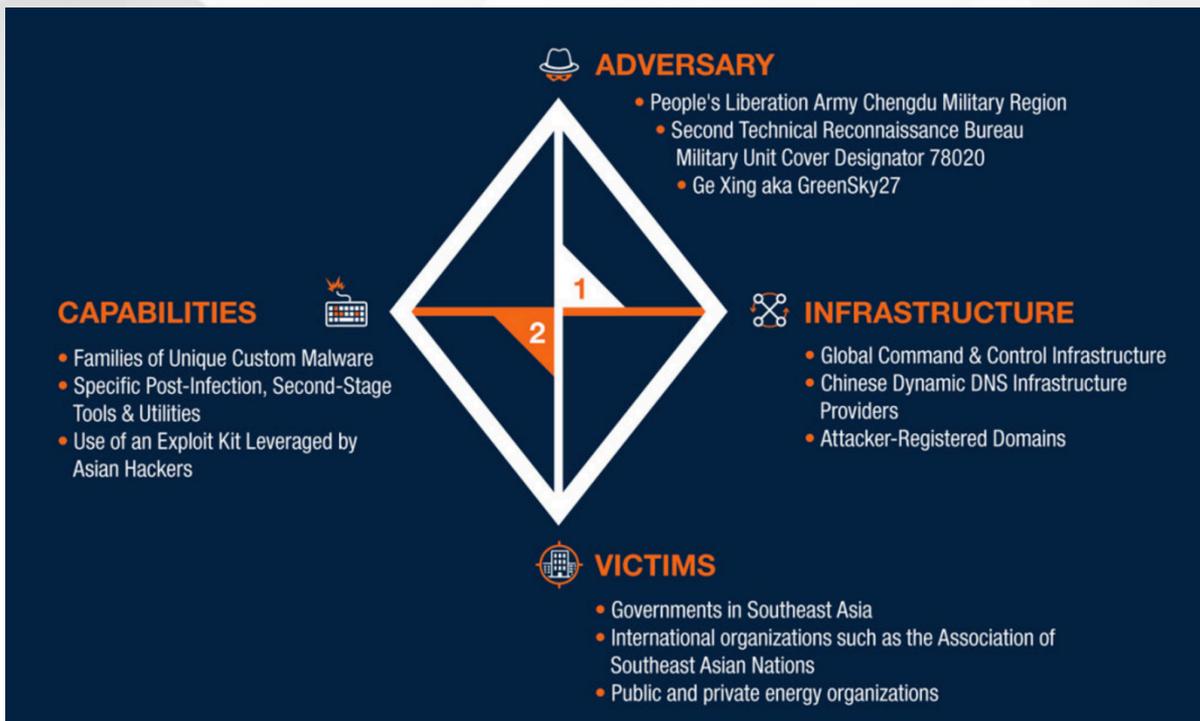
ISACs and ISAOs can provide a single TIP through which members aggregate threat data, analyze a complex set of indicators, and take corrective action against the group's combined adversaries. Members are able to maximize the value of community-validated TI by automatically incorporating it into existing network defense products.



## MSSP

ThreatConnect® is proud to partner with MSSPs to help you grow your business by offering your customers enriched threat intelligence as a service, making threat intelligence enabled Manage Services attainable.

# THE DIAMOND MODEL



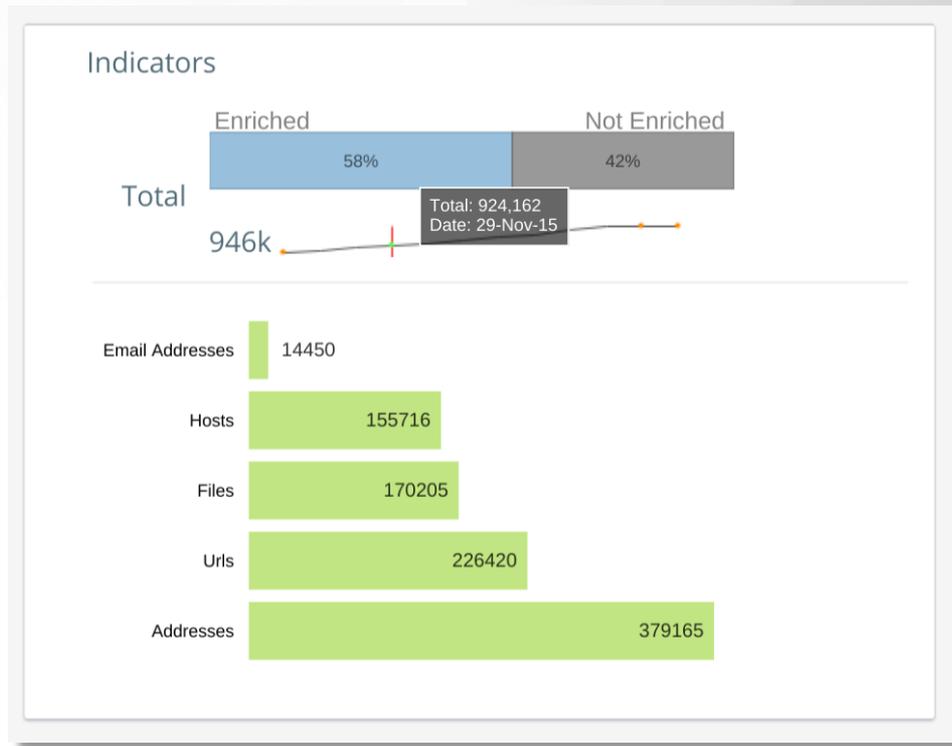
# THREATCONNECT DASHBOARD



<https://www.threatconnect.com/threatconnect-4-0-now-with-a-real-dashboard/>

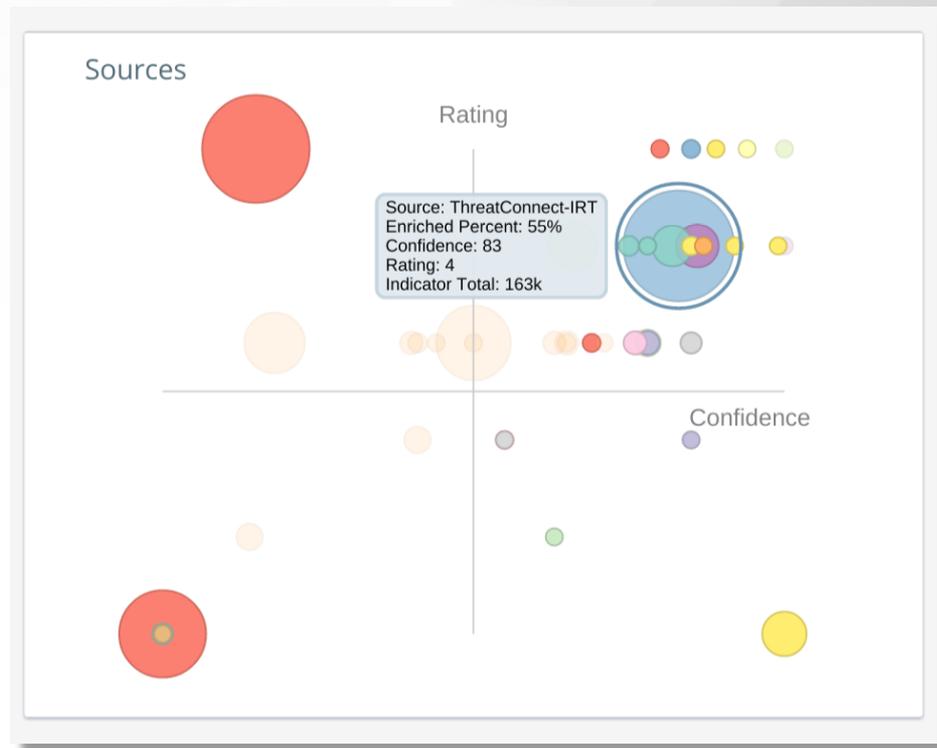
# INDICATOR ACTIVITY

- Distinguish between enriched and non-enriched indicators
- Shows a trend-line to indicate cumulative growth
- Shows a breakdown by indicator type
- Scope of the data can be global/community/organization/feed



# SOURCE MAGIC QUADRANTS

- Plots feed sources on threat ratings v/s confidence quadrants
- Size determines quantity and opacity determines enrichment
- Allows comparison of feeds
- One stop shop to get to know, compare, and evaluate TI feeds
- Current metrics are more subjective than objective



# INTELLIGENCE & ACTIVITIES



- Shows current value and a trend-line with historic data
- Trend-lines serve dual purpose

# WHAT'S COMING?

- Observations / false positives / local whitelisting will add more context to IOCs ergo making them more actionable
- More incentives for sharing data between community, with a symbiotic eco-system
- More powerful and interactive dashboard
- More meaningful and objective metrics for IOC/feed ratings/confidence
- More apps and features for data visualizations reporting and analysis
- More powerful, streamlined SIEM integrations



**THREATCONNECT™**

**THANK YOU!**