

Upgrading from an Open Source TI Database:

A ThreatConnect Customer Success Story



Customer's Problem:

The customer needed a Threat Intelligence Platform to replace an open source database (CRITS) that had become overloaded and unusable. The replacement platform needed to make conducting analysis easy in order to identify and mitigate suspected threats in a highly-scripted and automated environment.

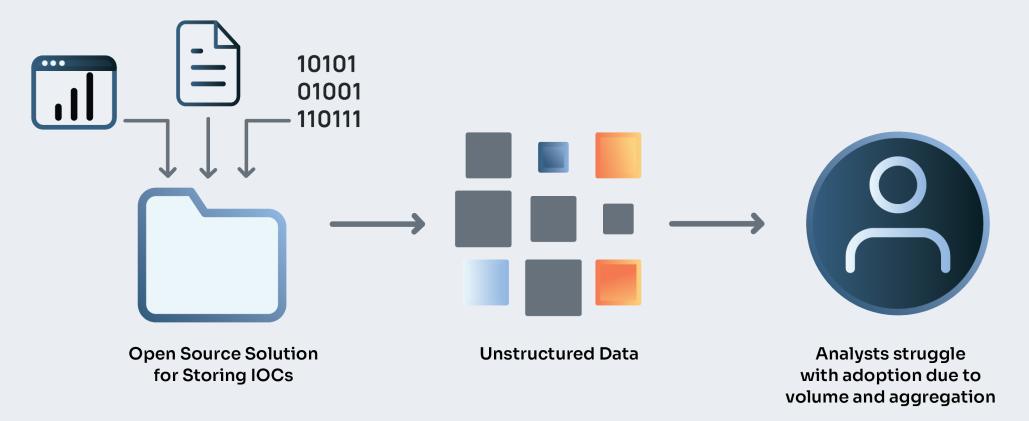
> Successfully transfer all existing data from the open source threat intel database to ThreatConnect.

CUSTOMER'S THREE PRIMARY OBJECTIVES:

- Maintain all original creation dates, as the customer relied upon the dates heavily for reporting, metrics, and memorialization.
- Because the customer had more than 3 million intelligence artifacts, the transition had to be fast and error free to ensure a seamless transition from a dev environment to production.

What Were They Doing Before ThreatConnect?

The customer was utilizing an open source solution to store data on indicators of compromise (IOCs) along with other data points.



ThreatConnect's Solution

Implementing the ThreatConnect Platform was the solution. The robust and scalable API allowed the organization to find a solution that met their primary objectives:

- Utilizing ThreatConnect's API, the customer was able to script the transition process with the Python SDK. ThreatConnect's Customer Success team assisted by providing recommendations on best practices once the data resided within the ThreatConnect platform.
- 2

The customer leveraged ThreatConnect's robust documentation throughout the data migration process to ensure they had a thoroughly documented API and SDK, which were paramount to the success of this transition.

3

ThreatConnect's Engineering team worked with the customer to provide a tailored solution that modified ThreatConnect's system dates to match the customer's existing 'first seen' and 'modified date' fields in their current solution.

4

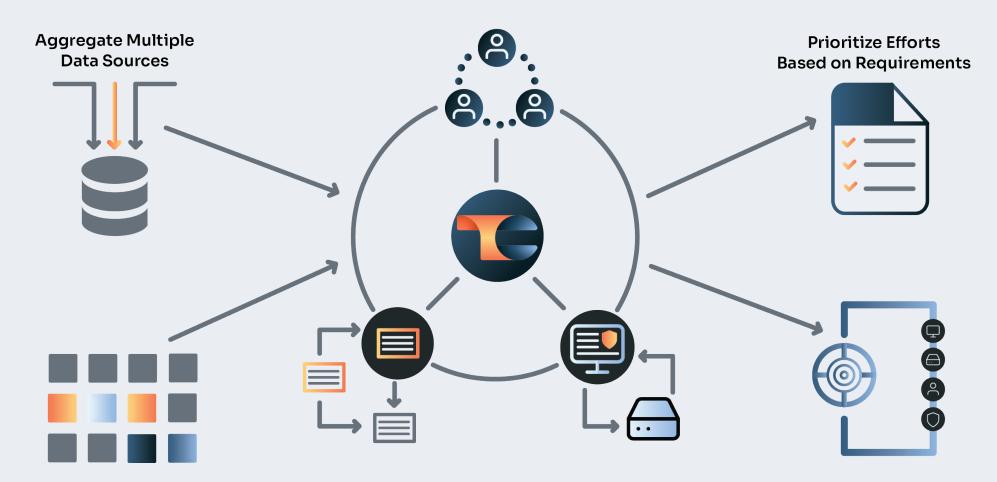
Custom indicators and attributes now give the customer greater flexibility in packaging their data within the Platform.

Results

In a matter of days, the customer completely transitioned from their old way of collecting and utilizing threat intelligence, and fully embraced the use of a customized and highly extensible security operations solution in order to meet their requirements. The customer is now able to provide a more efficient and robust capability to other parts of their organization that include the Incident Response team, the Security Operations Center, and the Network Operations Center.

MY THREATCONNECT (8) 🔻	Security	y Director Dashboard	d					:
My Open Tasks Actions ► 1-5 of 5 Resu	r iajuoonio i manonar olarinigo	Rules Deploye	Rules Deployed (SIEM / EDR / Firewall)		Recently Observed Indicators 1-9 of 9 Results			
Summary Owner Due Date					Summary 209.99.40.223	♦ Threat \$ 420		 False P ↓
A Next Month's PIR Updates System VT Threat Hunting Results System 02-22-2019	57,100				72.52.4.119	484	153	-
Investigate latest Fancy Bear Incl. System 02-20-2019 A Create Playbook for spearphishing System 02-21-2019	61 61 61 61 61 61 61 61 61 61 61 61 61 6	6			188.29.165.194 81.241.108.114		136	-
	01-31-2019 02-01-2019 02-02-2019 02-03-2019 02-04-2019 02-05-2019	02-06-2019			193.137.92.201		102	-
Popular Tags (This Week) dedicated server		0	500	1,000	209.99.40.222	453	51	-
suspicious name aerospace	Latest Incidents		hishing Incidents					
aviation retail	Type 🗢 Summary 🗢 Owner 🗢 /	Added \$ 87	18 bank		14 FINANCE		0 USSIA	
mirage	Image:)1-17-20						
apt28 finance	1 Incid 20190117A: Amazo ThreatCo 0	9)1-17-20	9 Dersis Dom	AIN SQUATTING	8 SPOOFED	7	IIDDLE EAST	
⑦ Popular Tags (This Week)	↓ Incid 20190115A: Obinna ThreatCo 0	6	6					
and the second s	Martin Contrattor Contrattor Contrattor	WHALING S	SCAM CVE-2	2012-0158				

What They Are Able To Do With ThreatConnect



BENEFITS:

- Data points (IOCs) automatically delivered to their SIEM, endpoint devices, vulnerability scanners, and other network devices through supported integrations.
- Provides context around related incidents and expedites the incident handling process by building associations with other data objects within the Platform.
- Ability to create custom dashboards and advanced queries that support daily operations, business requirements, and strategic objectives.
- Reduction in the number of resources and overhead costs required to support an open source solution in order to meet their operational requirements.



ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and Al-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights, and respond faster and more confidently than ever before. More than 200 enterprises and thousands of security operations professionals rely on ThreatConnect every day to protect their organizations' most critical assets. Learn more at <u>www.threatconnect.com</u>.

ThreatConnect.com 3865 Wilson Blvd., Suite 550 Arlington, VA 22203 sales@threatconnect.com +1 (800) 965.2708