CDAC
A CRDF GLOBAL INITIATIVE

Cyber Defense Assistance Collaborative (CDAC)
Case Study: Threat Intelligence Sharing
April 2024

This Case Study was a collaborative work by CDAC, ThreatQuotient, Cyber Threat Alliance (CTA) and Mandiant, now part of Google Cloud, based on a current operational deployment of the technologies mentioned.

CDAC
A CRDF GLOBAL INITIATIVE

Background

The Cyber Defense Assistance Collaborative (CDAC), a CRDF Global Initiative, is a volunteer group of cybersecurity and technology organizations that seek to provide threat intelligence, technology, training, advisory, and other cyber defense assistance to allied nation-states in conflict. CDAC was formed in response to the need to provide cyber defense assistance to Ukrainian public and private institutions following the Russian invasion of Ukraine in February 2022. Recognizing the acute cyber risk to Ukraine's critical infrastructure and the global cyber threat landscape, leading US cyber experts formed CDAC to galvanize and organize the US private sector to provide operational cyber defense assistance to Ukraine.

Since CDAC's inception in March 2022, over a dozen companies have volunteered to help Ukrainian cyber defenders secure networks, hunt for and counter malicious cyber intruders, improve attack surface monitoring, and provide cyber threat intelligence to protect critical infrastructure. CDAC has proven highly effective in helping Ukraine sustain its ability to operate in the digital space and shows a high potential for the initiative to provide support to other key partner nations around the world. CDAC was formed by a collection of cyber executives with pre-existing relationships, and they brought in people they knew and trusted to help Ukraine within days after an unprovoked invasion by a foreign adversary.

The Problem

Since the early days of the Ukrainian conflict, CDAC has had vigorous support from trusted companies and volunteers offering real-time threat intelligence information, software, and defensive technologies. Large companies, nonprofit organizations, and governmental organizations began to provide threat intelligence feeds to the many embattled critical infrastructure and defense organizations in Ukraine.

As Security Operation Centers across Ukraine started receiving this threat intelligence, it became almost unusable because of duplication and volume which exacerbated challenges: the data was coming into them in separate formats and separate priorities, and in many cases duplicate data was present. One threat intelligence provider would provide data on one day, another could give on another day with most of it being unique data, but the consumers in Ukraine would have to spend considerable effort cross-checking against previous sources. This problem grew exponentially with other threat feeds being delivered by new volunteer organizations, the US Government, and other sources. CDAC recognized this problem early on due to its deep experience with threat intelligence organizations of government and large commercial cyber defense teams.

Threat Intelligence needs to be delivered with broadly gathered threat intelligence from multiple external feeds (commercial, non-profit, open-source, government) as well as intelligence gathered from other trusted sources which can be in blog posts and reputable feeds. This data needs to be de-duplicated, normalized, and delivered to many different downstream entities.

Seeking a Solution

In January of 2023, leaders of CDAC worked with leaders of ThreatQuotient, Inc. to address the challenge of making all the intelligence data provided to the Ukrainians more useful.

ThreatQuotient donated a SOC2 Certified instance of the ThreatQ platform, which was hosted by ThreatQuotient in Europe to bring in threat intelligence—structured and unstructured—from different entities and distribute the intelligence to critical infrastructure and government organizations depending on the needs. The platform was set up as a centralized aggregator and distributor of threat intelligence with base requirements to:

- Ingest and de-duplicate intelligence from multiple sources and formats becoming the single source of truth of CDAC multi-vendor provided data.
- Distribute different sets of information to different entities downstream based on dynamic saved searches (i.e., If this is reported by two trusted sources, target country-Ukraine, target industry-energy, send to specified consumers).
- Automate enrichment of threat intelligence through integrations and distribute that information with the indicators.

Other CDAC participants also contribute to the platform: The Cyber Threat Alliance (CTA) worked with their contributors to set up feeds into the ThreatQ platform and worked with ThreatQuotient to develop an integration to ingest CTA data through API's. Recorded Future and Mandiant, now a part of Google Cloud, started sending their information into the platform as well. ThreatQuotient and CDAC worked with US CISA to ingest Department of Homeland Security (DHS)–Automated Indicator Sharing (AIS) feeds as well.

Organizations in Ukraine started ingesting the threat intelligence in different ways. Some of the government and energy consumers had already been using ThreatQ in their SOCs. Thus, they were set up with a direct connection from their instance of ThreatQ to the hosted CDAC ThreatQ instance. Other government agencies and critical infrastructure were using MISP, the open-source Malware Intelligence Sharing Platform, which integrates with ThreatQ to bidirectionally share threat intelligence. Some entities required data to be sent to their SIEM directly, which was also enabled through direct integration into the ThreatQ platform. Furthermore, as time went on, other volunteer organizations such as Grey Noise and Nisos started feeding into the ThreatQ platform.

Steady State Architecture

As discussed above, the base architecture of any threat intelligence sharing capability begins with the ingestion, de-duplication, and normalization of the data. Figure 1 on the next page depicts the multiple sets of different types of threat data coming in—some structured and some unstructured. The data is de-duplicated based on provider time stamps and is shown as one record for the recipients to digest and take action. The architecture incorporates ThreatQ's Natural Language Processing (NLP) Capability called ACE to automatically parse reports and add data to the threat library being sent to the downstream consumers.

Generally, there is a baseline of data that is sent to all constituents based on adversary and geography. A second and unique collection is sent to different consumers based on varying requirements: CDAC collaborates with different private and public organizations to use intelligence scoring and TLP controls to determine which Smart Collections go to which consumer. Consumers can also express the type of data they would like as well as the timing of the export. The architecture also allows direct consumers of the CDAC ThreatQ instance to further distribute intelligence to downstream constituents of their own with another ThreatQ platform or MISP.

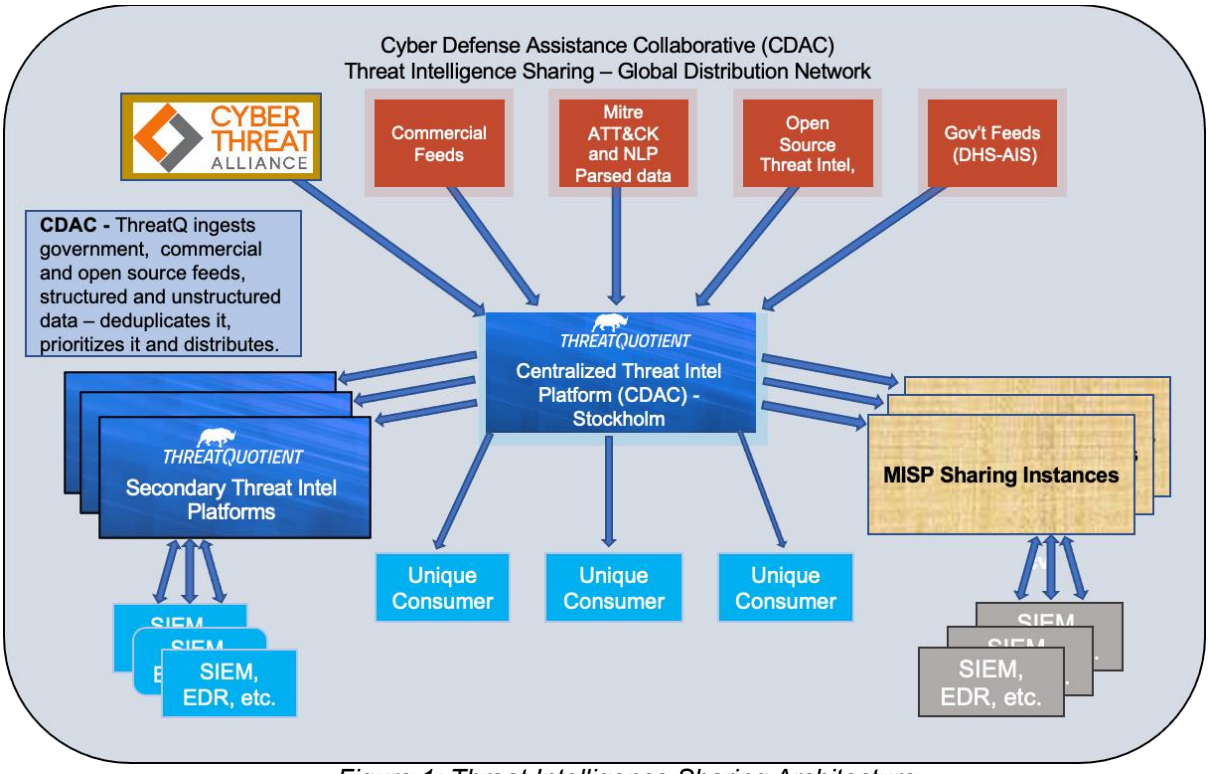

Figure 1: Threat Intelligence Sharing Architecture

The platform also allows air-gapped deployment: one Internet-facing platform passes data through a data diode to a second platform. This option is important for customers with classified environments and can work in multiple classification levels.

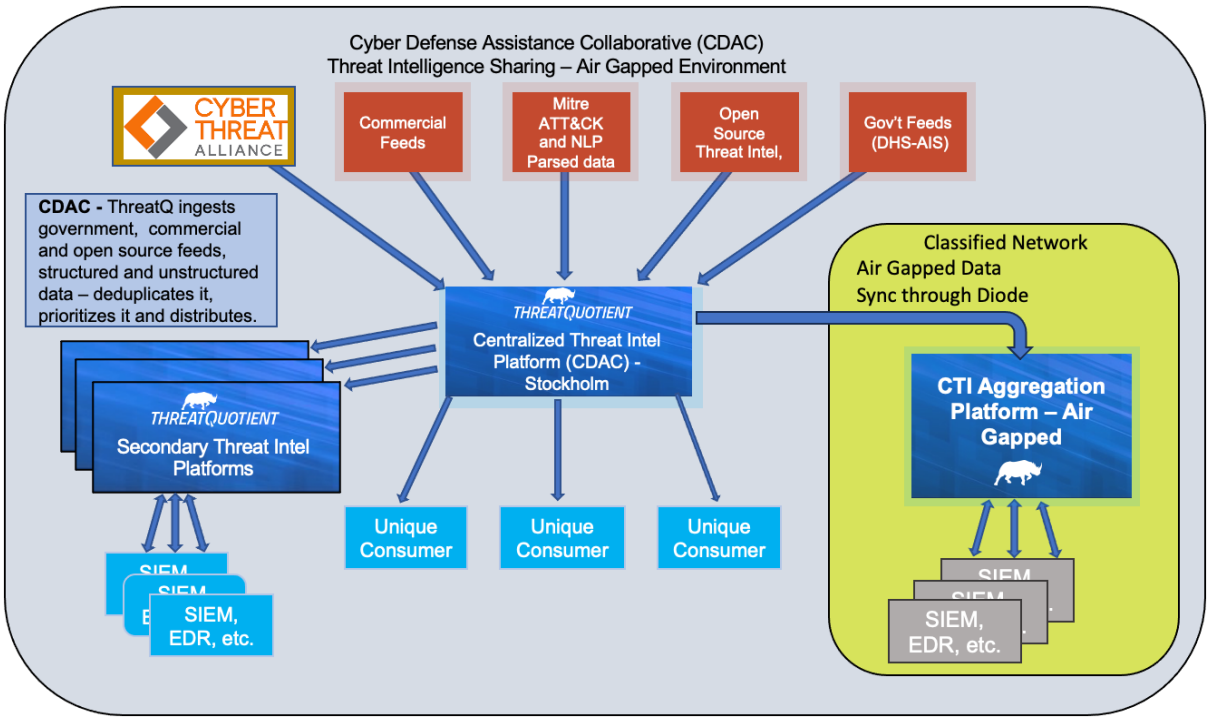

Figure 2: Threat Intelligence Sharing Platform Air-Gapped.

CDAC
A CRDF GLOBAL INITIATIVE

Future State

The model set up by this collective group of non-profit, commercial, and government agencies is a replicable model that can be quickly deployed and used across the globe. The platform created by this group can be a cyber crisis difference-maker today and in the future. The approach used in the collective approach of the CDAC threat intelligence sharing is ground-breaking as it was deeply enabled by a collaborative public and private partnership leveraging and integrating high-quality intelligence. Recipients can focus their limited defensive resources on high-risk threats and automatically feed defenses based on adversaries targeting them. The architecture and collaboration provide a ready-made construct for other situations, which can be tailored by input and output feeds as required by geography, policy, or security concerns. The construct is scalable and able to add additional feeds as required from other sources that a situation may require.