CYSIAM

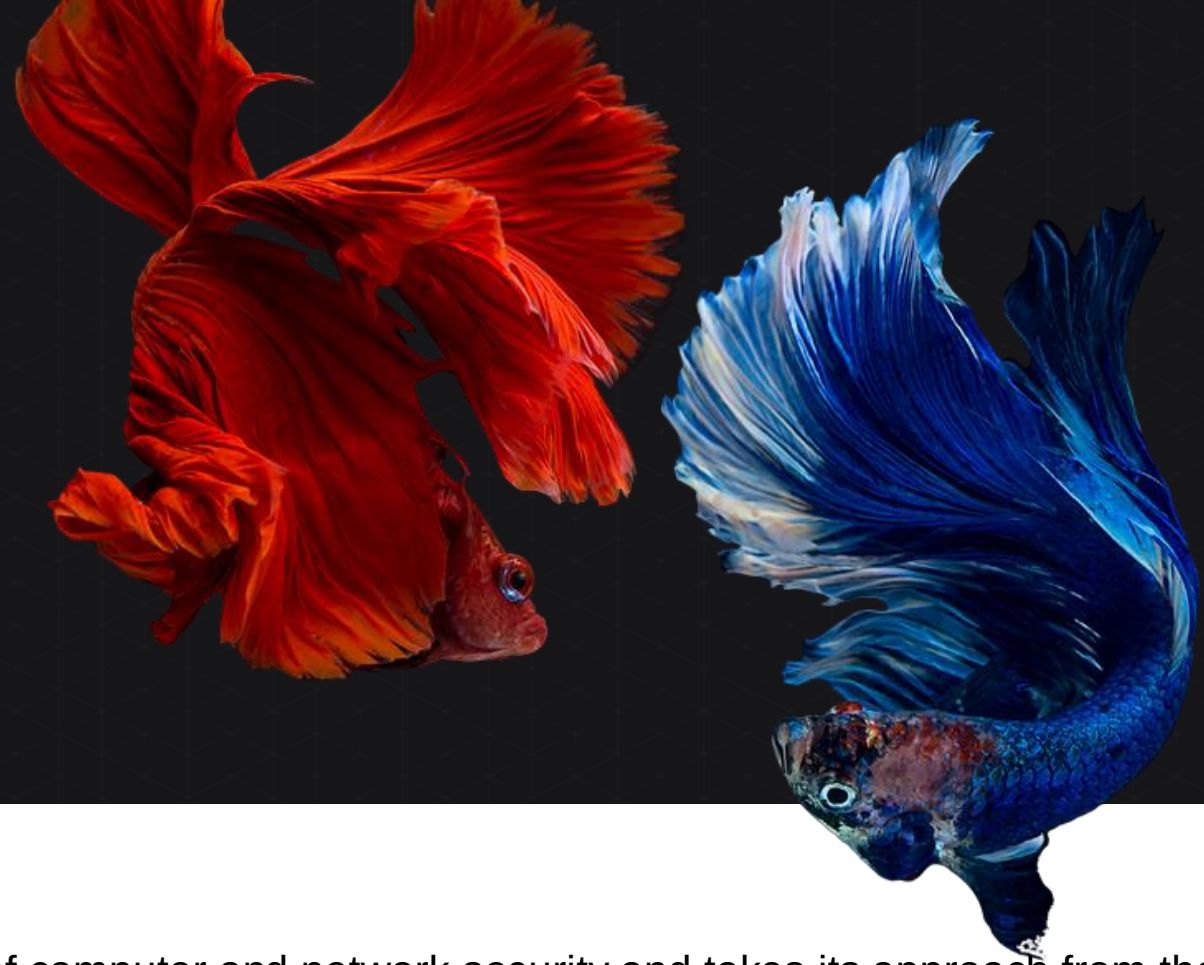
12-Feb-25

CYBER THREAT INTELLIGENCE OVERVIEW

It's more than just data…

PATHFINDERS IN CYBER INTELLIGENCE

Data Driven Cyber Threat Intelligence



CTI

Description:

Cyber Threat Intelligence (CTI) is a proactive part of computer and network security and takes its approach from the traditional intelligence cycle. CTI is more than a product; it is a complex process and a discipline that requires great skill to master.

- CTI is focussed on collecting and analysing data to meet strategic, operational and tactical level requirements.
- Effective CTI allows Cyber Defenders to proactively predict, identify and prevent attacks.
- During an incident, CTI underpins the response, investigation and recovery activities.

CYSIAM CTI CAPABILITY

"**Analysed** information about the hostile **intent**, **opportunity** and **capability** of an adversary that satisfies a requirement"

The Team:

The CYSIAM Threat Intelligence team collects and aggregates a variety of data feeds.

As well as open-source and commercial data sources, our team has access to private data feeds to help further contextualise analysis, hypotheses, and reporting. This removes the inherent bias that comes with single-source analysis.

We proactively identify and research threat actors to gain an understanding of their motives, their target organisations and industries, and their changing and evolving tactics.

CYSIAM CTI Process

DIRECTION

- Priority Intelligence Requirements (PIRs) are identified to provide analysts with clear direction.
- CYSIAM will work with the Partner organisation to determine their strategic-level requirements to produce consistently relevant intelligence.
- These PIRs will be frequently updated in routine collaboration with the Partner organisation and via RFIs and feedback.

COLLECTION

- Relevant data is collected in line with PIRs.
- CYSIAM will use the Partner organisation's PIRs to form an Intelligence Collection Plan (ICP).
- This ICP ensures only relevant and accurate data is collected, speeding up the analytical process.

DISSEMINATION

- Relevant intelligence is then passed to the Partner organisation.
- CYSIAM will ensure the Partner organisation receives the relevant hypotheses in a legible, concise, and appropriate format.
- RFIs and feedback from the Partner organisation encouraged to elicit further intelligence requirements and to tailor products to their needs.

ANALYSIS

- The collected data is analysed to answer the PIRs.
- CYSIAM will independently analyse the data, including the confidence of the sources, to create hypotheses in line with the Partner organisation's PIRs.
- References to source material and evidence supporting these hypotheses are also provided where possible.

CTI PRODUCTS

STRATEGIC REPORTING

Who is likely to attack, who is likely to be attacked, and why?

OPERATIONAL REPORTING

How will the threat actors conduct their attack? What infrastructure are they likely to target?

TACTICAL IOC SHARING

What indicators or artefacts are associated with attackers' tools and infrastructure?

VULNERABILITY ADVISORIES

How are organisations of interest likely vulnerable to relevant threat actors?

CTI as a Service (CTIaaS)

Data Driven CTI Direct to the Partner

CTI PARTNERSHIP - DIRECT ACCESS TO CYSIAM'S CTI TEAM:

- Security-cleared analysts
- Dedicated, CREST and SANS qualified CTI professionals
- Intelligence tailored to the Partner's requirements
- Aggregating and analysing data from open, closed and commercial sources

IDEAL FOR PARTNERS WHO:

- Have limited personnel
- Lack formal direction
- Have SOC analysts suffering from alert fatigue
- Require a quicker solution

PRIORITY IDENTIFICATION APPROACH:

- Define the threat landscape and key stakeholders/customers.
- Identify scope of critical assets and people.
- Define priority intelligence requirements against that scope.
- Define how CTI can answer those requirements.

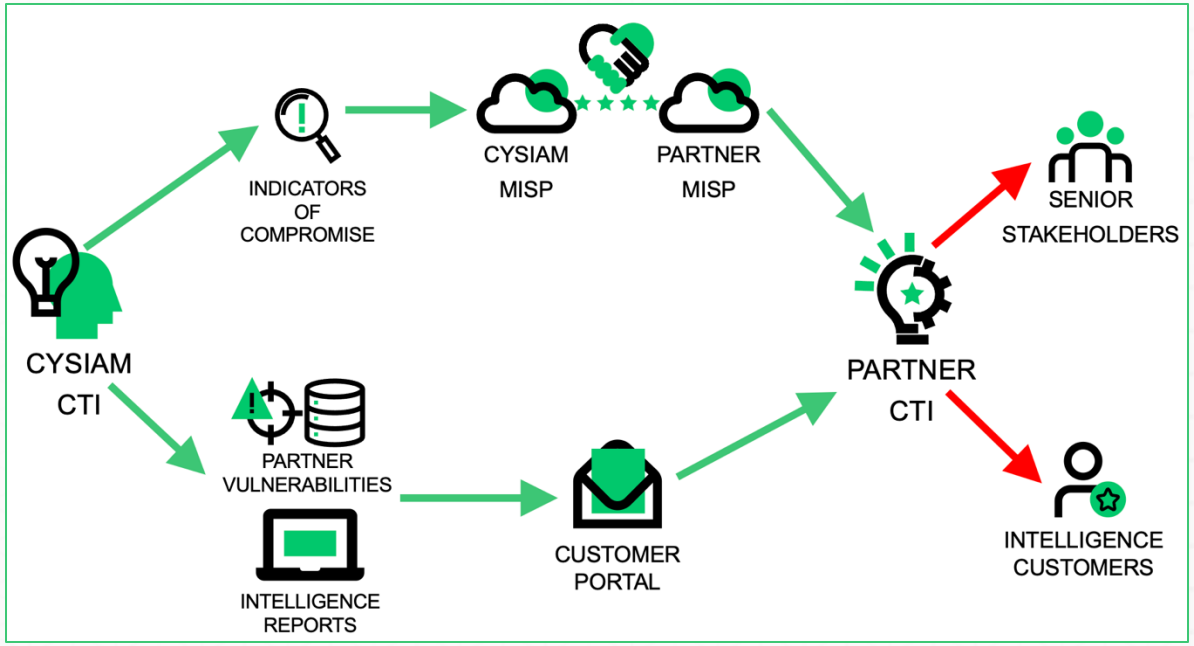
CTIaaS Operational Model and Onboarding

The CTIaaS offering comprises the following:

- Quarterly strategic CTI reporting
- Monthly operational CTI reporting
- Weekly tactical CTI research and sharing via MISP
- Ongoing vulnerability research and ad-hoc advisories
- On-demand RFI's subject to agreed scope

Partner onboarding will consist of the following activities:

- Collaboratively generating priority intelligence requirements (PIRs)
- Identifying critical assets and organisations of interest
- Create access to CYSIAM's MISP instance
- Provide CYSIAM with an email address for report notifications
- CYSIAM will then create an account (using the email provided) on our portal.
- Login, set up MFA and confirm access to all areas.
- Once service has started, continue to hone PIRs, and submit feedback and RFIs



Partner organisation responsibilities:

- Work with CYSIAM to develop PIRs
- Ingest CTIaaS products as a data source in their own intelligence lifecycle
- Use products to create independent hypotheses in conjunction with analysis of other data sources
- Disseminate their own intelligence products to senior stakeholders and customers

CTIaaS Client Portal

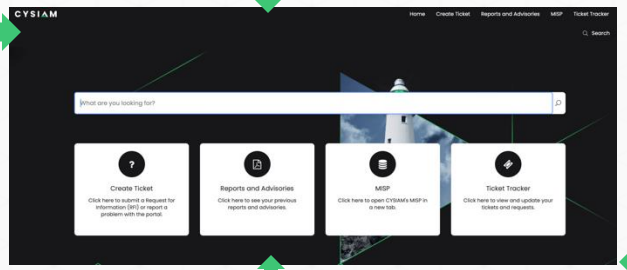
Interactive portal for accessing and requesting CTI products:

- Our custom portal allows you to securely download your own bespoke intelligence products, interact with the team by submitting RFI's and feedback on issued reports, access to a large repository of IOC data through our MISP instance and access to our knowledge base of articles, blogs, papers and threat advisories.

- When an RFI is submitted via our templated form, a ticket is generated in our portal for the relevant intelligence analyst to investigate and report. The same happens with feedback. This allows us to keep a record of all requests and provide trend analysis on the threats that you are most concerned with.

- Access a growing repository of threat advisories, white papers and blogs via our Knowledge Base

- From the portal, direct access to our MISP instance for IOC's or if the partner has their own MISP, we can set up syncing



Secure log on to the client portal

- Submit requests for information direct to our threat intelligence analysts and give them feedback on previous reports.
- When bespoke reports are ready, a notification will be sent to the client, informing them that a report is ready to collect from the portal.