CDA

CYBER DEFENCE ALLIANCE

CYBER DEFENCE ALLIANCE (CDA)

MEMBERSHIP

bsi

ISO/IEC 27001
Information Security
Management
CERTIFIED
IS 664985

> ***Over 20 years in the FS infosec... I have not come across another organisation like CDA. Not only is it our most accurate and focused source of threat intelligence, but it also provides a trusted space, where we can share experience and gain advice from peers across the industry (invaluable when we are under attack) and gives a channel into law enforcement...***
>
> CISO, UK Bank

ABOUT US

The Cyber Defence Alliance (CDA) is an international not for profit alliance focused on action and impact, relentlessly fighting cyber threats.

The CDA provides a trusted environment for financial institutions to work in partnership with governments, law enforcement, intelligence agencies, telecommunication operators and security agencies in the collective effort to fight for a better digital future.

Our Alliance was founded in 2014/15 by four Globally Systemically Important Financial Institutions (GSIFIs) with full spectrum capability who realised individually they would not be able to withstand future threats alone.

We have steadily grown and are entirely member owned and driven. Flexible and responsive to evolving cyber threats, the CDA acts as a force multiplier to enhance member collective response by providing preventative, actionable intelligence spanning active network defence, through to financial and cyber-crimes. By sharing resources, expertise and knowledge we identify, target and disrupt cyber threats.

Working closely with regulators, national and regional authorities our tight circle of trust is vital with very few other organisations operating at this level. Year on year, our contribution to national and international law enforcement successes grows both as a driving force or a key collaborator.

The CDA team is comprised of permanent CDA staff and member secondees (full and part time, both physically and virtually attached) and is headquartered in Canary Wharf, London.

We operate within the UK, EU and North America and with partners in the Far East and Australia.

OUR CAPABILITIES

Technical Intelligence (TECHINT)

Transforms open-source data into actionable insights through bespoke, in-house solutions. We develop powerful tools to identify, enrich, analyse, and securely share intelligence with our members. Our capabilities include advanced data analytics, threat monitoring, automated alerting, and proactive discovery of digital risks across a wide range of online environments.

Cyber Threat Intelligence (CTI)

Subject matter experts in IT network engineering, cyber threat intelligence analysis and adversary techniques, tactics and procedures, the team assists CDA members to bolster their cyber defences through the provision of high-quality intelligence on threats to networks and supply chains. We focus on providing actionable intelligence, allowing recipients to proactively hunt for threat actor activity in networks, rather than simple vague descriptions of generic actor TTPs.

Fraud & Cyber Investigations Team (FACIT)

Develops end-to-end understanding of the most impactive cyber-enabled frauds targeting members, finding opportunities to identify, target, disrupt and mitigate against threat actors and Cybercrime-as-a-Service operations using the CDA cyber-fraud kill chain. With collective knowledge, target packs created for law enforcement partners provide actionable intelligence opportunities whilst demonstrating the true scale and impact of offending.

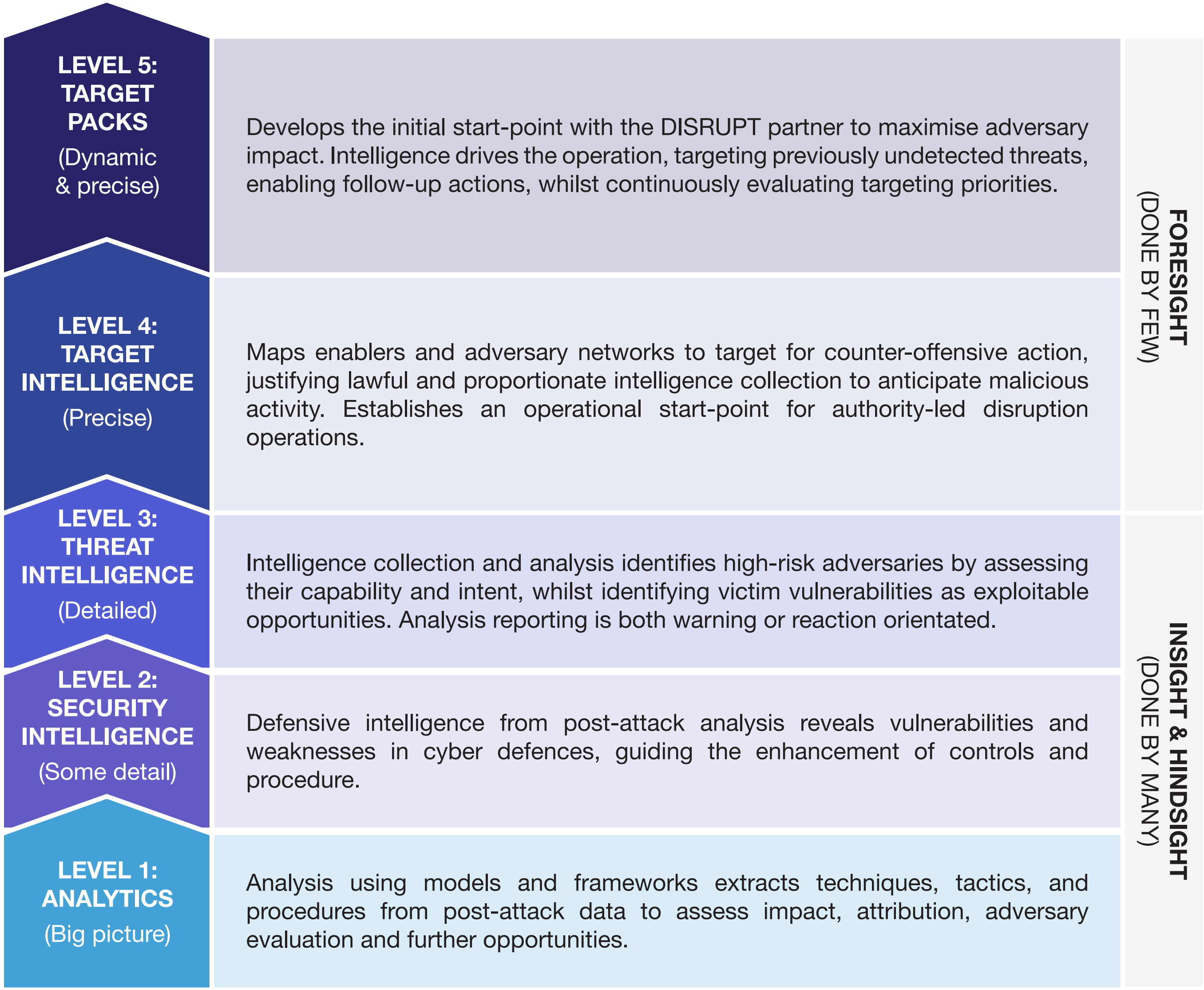
> ***Joining CDA has been a game changer for my team and I. In peacetime, the Alliance provides us with valuable intelligence, coaching, direct access to our peers. The spirit of non-competitive information sharing is incredible. In wartime, when members are under attack, the Alliance and its members all come together and really look out for each other.***
>
> \- CISO EU Bank

> ***Joining the CDA was one of the best decisions I've made as CISO. Together, we're stronger. The CDA turns trust into action and intelligence into defence – so an attack on one becomes a response from all.***
>
> **-** CISO UK Bank

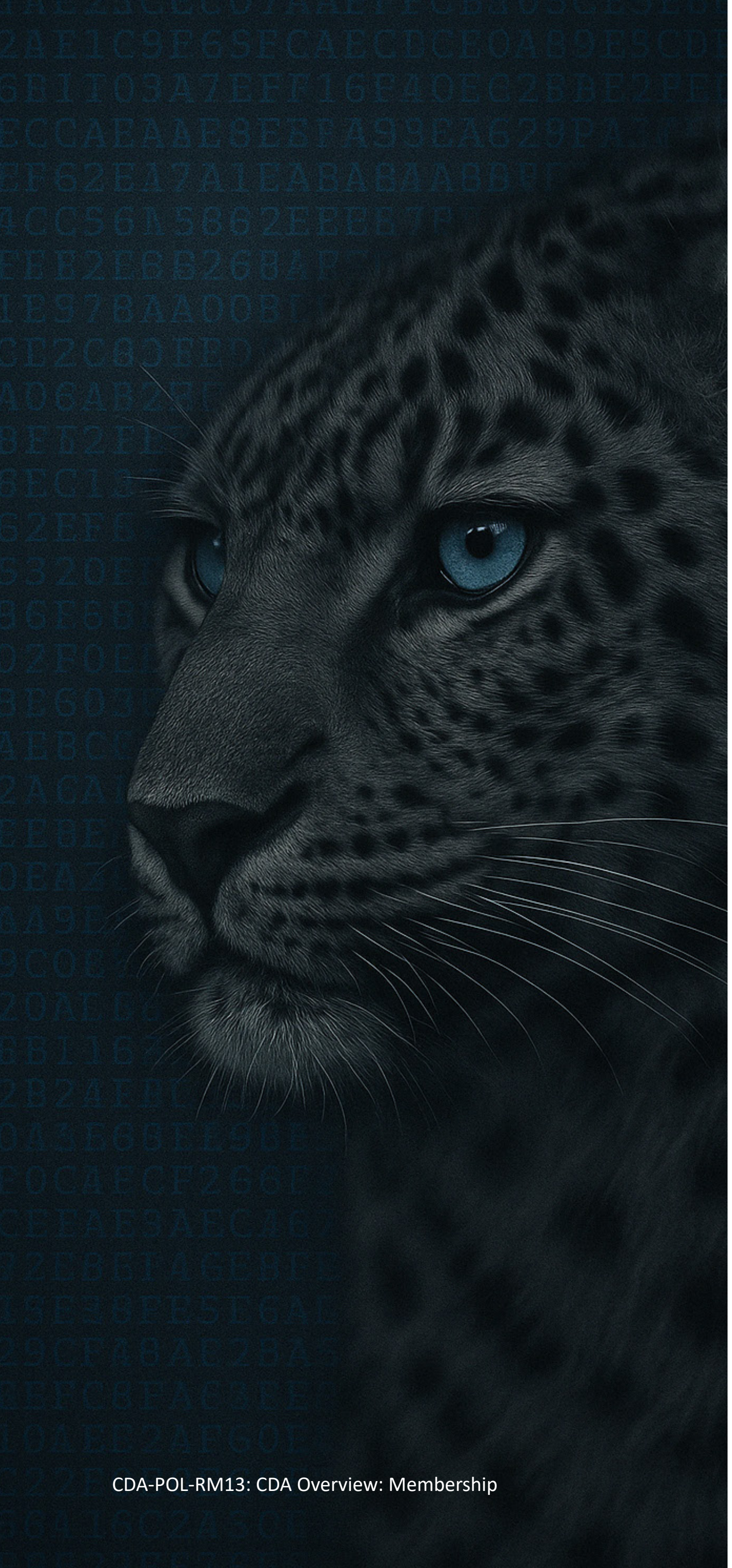
CYBER THREAT INTELLIGENCE

CDA Decision Support Analysis (DSA) provides our membership with genuine insight and foresight. This increases the agility of cyber defence, enhances the design of cyber security and informs cyber resilience. Our members achieve a return on tangible investment by reducing fraud losses and disrupting both cyber and cybercrime threats.

> ***CDA is an essential element of the defence of the bank, our clients and customers. CDA services are unique and go well beyond any other intelligence sharing organisation we are members of... The Alliance supports our collective defence but also allows us to fight back against criminals who target us, our customers and suppliers.***
>
> - Cyber MD UK Bank



LEVEL 5: TARGET PACKS (Dynamic & precise)	Develops the initial start-point with the DISRUPT partner to maximise adversary impact. Intelligence drives the operation, targeting previously undetected threats, enabling follow-up actions, whilst continuously evaluating targeting priorities.	**FORESIGHT** (DONE BY FEW)
LEVEL 4: TARGET INTELLIGENCE (Precise)	Maps enablers and adversary networks to target for counter-offensive action, justifying lawful and proportionate intelligence collection to anticipate malicious activity. Establishes an operational start-point for authority-led disruption operations.	
LEVEL 3: THREAT INTELLIGENCE (Detailed)	Intelligence collection and analysis identifies high-risk adversaries by assessing their capability and intent, whilst identifying victim vulnerabilities as exploitable opportunities. Analysis reporting is both warning or reaction orientated.	**INSIGHT & HINDSIGHT** (DONE BY MANY)
LEVEL 2: SECURITY INTELLIGENCE (Some detail)	Defensive intelligence from post-attack analysis reveals vulnerabilities and weaknesses in cyber defences, guiding the enhancement of controls and procedure.	
LEVEL 1: ANALYTICS (Big picture)	Analysis using models and frameworks extracts techniques, tactics, and procedures from post-attack data to assess impact, attribution, adversary evaluation and further opportunities.	



OUR APPROACH

Our purpose is to protect our members, their clients, customers and the societies they serve.

The CDA has a specific focus on the threat and the ability to turn this information into action on targets to impact the challenges our members face.

We operate a counter-offensive mindset to **identify, target** and **disrupt** the adversary and their networks that operate against our members. Our work is measured by high confidence signals, rather than overwhelming white noise, leading to positive outcomes.

There is an Article V element in our constitution that mobilises the Alliance to the defence of a member under extreme pressure.

Our values and culture are founded on **agility, impact, mission** and **security** with the operational security of our members being paramount in all our work.

Our intelligence collection and development drive operational effectiveness and efficiency, degrading the threat to our members, their clients and customers.

OUR MISSION

Our mission is to generate and exchange intelligence and knowledge to:

- Provide timely and accurate insights of new and emerging cyber threats
- Increase the effectiveness of cyber security and cyber resilience efforts
- Reduce the impact of cyber attacks
- Counter the attacks of cyber threat actors and networks
- Work collaboratively with cross-sector partners to identify and reduce threats

IDENTIFY
TARGET
DISRUPT

MEMBERSHIP

Membership of the CDA represents a mindset change to the challenge that cyber threats represent to our digital economy and digital democracy.

As an international, not-for-profit organisation, the CDA supports our members and associates in loss reduction, increasing their maturity levels and ultimately reducing their vulnerability to cyber-attack.

With in-house collection, research, and analysis capabilities, the CDA delivers actionable intelligence to counter threats faced by our members. We operate on their behalf, driving targeted projects and action groups aligned with their priorities.

A mindset change can achieve a paradigm shift.

> “
>
> ***The City-Of-London-Police has worked closely with the Cyber Defence Alliance over the last few years... The collaboration has saved UK businesses millions in losses and led to the arrest of dozens of sophisticated high impact fraudsters. We value this ongoing partnership...***
>
> Detective Superintendent Oliver Little,
> City of London Police

MEMBERSHIP SERVICES

» Network Defence & Cyber Threat Intelligence
» Cybercrime Intelligence
» Vulnerability Reporting
» Supply Chain Resilience Group
» Emerging Geo-Political Threats and Strategic Intelligence
» Domain Analysis and Blocking Requests
» Threat / Infrastructure Hunting
» Threat Modelling
» Telecommunication Group & Services
» Daily All-Member Operations Call
» Daily Media Monitoring
» Collective Support Plan

*For full details see appendix.

> ***The Metropolitan Police Cyber Crime Unit has enjoyed a long association with the Cyber Defence Alliance. A working partnership …[leading] to the identification, targeting and disruption of dozens of high-level cyber criminals including the international takedown of criminal cyber services such as 'iSpoof' and 'LabHost' that has led to hundreds of arrests worldwide.***
>
> Detective Chief Inspector David Birrell, Metropolitan Police Service, Cyber Crime Unit

BECOMING A MEMBER

Full membership is currently reserved for financial organisations. Applications for full membership are voted upon by the CDA Board for decision.

Our members recognise that collective defence and actions against the threats they face represents a paradigm shift that provides greater security to their organisation, customers, clients and the communities they serve.

The CDA operates on an active member model and members place secondees with the CDA either full or part time, remotely or in person. For their time with the Alliance, secondees are fully incorporated into the work of the CDA.

NEW MEMBERS RECEIVE

- Bespoke onboarding to capture your organisation's essential points of contact to receive relevant outputs for their role and interests and other key information
- Separate introduction and familiarisation briefings for leaders and operational teams (with quarterly update sessions for new joiners)
- CDA point of contact for the onboarding process
- Overview briefings for each working group that your staff join

CONTACT:

contact@cyberdefencealliance.org

www.cyberdefencealliance.org

APPENDIX

APPENDIX 1: CDA MEMBER SERVICES

Service or Capability	Description
Daily All-Member Operations Call	The CDA hosts a daily call attended by representatives from the cyber threat intelligence and cybercrime teams of each member bank and law enforcement (LE). This enables the sharing of close-to-real-time threats and provides insight into operationally significant events or incidents between peer banks. In this call, open-source briefing of pertinent global events, vulnerabilities and developments in technological and geopolitical spaces are also delivered, as well as updates from the daily FSCCC/NCSC call.
CDA Trust Groups (CTGs)	These enable secure email communication and sharing of information in real-time between trust groups based on specific areas of interest/business such as cybercrime/financial, pro-active network defence, special interest action groups (SIAGs) and others. The information can be enriched and/or more context added immediately by any of the members or the CDA, who may have additional insight or intelligence.
MiSP Sharing Platform	The CDA has a MISP instance that is connected to member' platforms to facilitate machine to machine distribution of structured cyber threat intelligence as collected by CDA.
Network Defence & Cyber Threat Intelligence	This CDA initiative supports real-time sharing of information between members relating to all types of cyber intelligence, including ongoing campaigns observed firsthand by CDA members, technical information, and IOCs (indicators of compromise). This enables the CDA and members to gain insight into the cyber landscape, discuss controls and mitigation as well as consume valuable intelligence for preventative/remedial action.
Cybercrime Intelligence	This CDA initiative supports real-time sharing of information between members relating to all types of banking cybercrime including enablers, such as mule herders, bullet proof hosting, OTP interception and other criminal services. This allows the CDA and members to get a greater insight into the cybercrime landscape, discuss controls and mitigation, and to develop investigations for LE action. The CDA will collate and develop this collective assessment of significant criminal activity to inform LE strategic tasking processes and prepare intelligence and/or evidential packages for LE operational action.
Cyber Crime Action Group (CAG)	The Cybercrime Action Group (CAG) is a fusion of fraud and cyber threat SMEs who are tasked with mitigating cyber enabled fraud. Meeting monthly, the group aims to mesh cyber and fraud team methodologies to reduce such fraud by creating a kill chain to mitigate the attack at various stages. Working groups are created from within this group to tackle the biggest threats as decided by the membership. Members can task the CDA via this process.
Daily Media Monitoring	The CDA employs a range of tools to assist in the identification of relevant journalistic and open-source content to produce the CDA Daily Security Threat Report; a summary of security issues and threats affecting the financial services sector. CDA analysts produce additional alerts from this intelligence collection as relevant.
Proactive Intelligence Collection	The CDA proactively collects intelligence from social media, messaging apps, paste sites, dark and clear web, and other closed sources. This service is mainly automated but includes development by CDA analysts who provide written alerts. This collection also allows the CDA to identify naming conventions for criminal services targeting the financial sector.

Service or Capability	Description
Exploited Vulnerability Reporting	The CDA reports upon vulnerabilities identified as being actively exploited and considered highly critical to the sector or supply chain. This alerts members to prioritise patch management and other mitigation actions.
Domain Analysis & Blocking	The CDA identifies newly created domains directly or indirectly targeting member banks. These domains are researched using in-house automation to ascertain full domain details for notification to members. Recovered phish kits are analysed for intelligence opportunities. Malicious domains are sent to MNOs, ISPs major browsers and reputation feeds for blocking.
RaaS Alerting	The CDA scrapes hourly across all identified RaaS blogs to identify victim companies and thereby potential third-party risks to members. This is collated with further relevant intelligence from CDA open and closed source collection. Any dumped breached data of potential relevance to members is retrieved and analysed to provide affected members with a full exposure and impact assessment. Monthly and weekly products containing statistics and thematic insights on RaaS breaches and alerts are provided to CDA members and LE partners to allow for further analysis.
Collective Support Plan	The CDA provides 24/7/365 support to CDA members via an on-call analyst and on-call manager. This service includes arranging a members' call to either seek input or make other members aware of the incident/threat. Calls can be arranged both in-hours or out of hours, as required. The CDA set-up, chair and provide the back-up administration for the call.
Cyber Trend Analysis and Operational Summaries	The CDA assesses composite data from members, identifying significant trends and emerging threats as part of the strategic assessment process to better understand the evolving cybercrime landscape. This information is used to prioritise resources, projects and interventions. Information, including statistics and work undertaken by the CDA is published in weekly, quarterly and annual formats.
Emerging Geo-Political Threats and Strategic Intelligence	The CDA identifies significant external events that may impact adversely on CDA members, financial sector or wider community. This is linked with technical assessments to provide a more complete understanding of the threat picture to inform strategic assessments and the Top Threats initiative.
Training and Development	The CDA coordinates cross-member access to training, awareness and personal development opportunities. Issues of common interest to members are established to inform the coordination of seminars, webinars and programmes to raise collective understanding, utilising external presenters, vendors and in-house expertise. The Expert Talk Series are 'deep dive presentations' aimed at technically advanced SMEs, whilst the Analyst 101 Series are interactive, practical workshops to empower and upskill analysts from across the cyber sphere regardless of background. CPE attendance certificates are issued.
Collective Support Plan	The CDA provides 24/7/365 support to CDA members via an on-call analyst and on-call manager. This service includes arranging a members' call to either seek input or make other members aware of the incident/threat. Calls can be arranged both in-hours or out of hours, as required. The CDA set-up, chair and provide the back-up administration for the call.

Service or Capability	Description
CDA Data Analytics Platform	The CDA's data search and analysis platform ingests structured, unstructured, real-time and LE data to search and analyse. In-house tools allow the CDA to deconstruct data and extract entities of interest. Structured data is mapped to provide dashboards, trends and graphics.
Special Interest Action Groups (SIAGs)	The CDA coordinates SIAGs to bring together subject matter experts from members, financial sector and others (as relevant) to share knowledge, in a trusted environment. SIAGs include Cybercrime; Top Threats, Network Defence; Insider Threat; Geo-Political; Telco (includes membership from all Roi & UK MNOs and other large ISPs) and Cloud Security. The CDA also forms temporary communities of relevant stakeholders/groups for specific event-driven topics for member discussion and benchmarking.
Threat / Infrastructure Hunting	The CDA seeks to identify offensive command and control infrastructure directly related to CDA Top Threats, enabling members to implement proactive blocking at network boundaries. The CDA facilitate the sharing of rulesets across the membership for organisations who also undertake infrastructure hunting in-house.
Threat Modelling	As part of the Top Threats and CAG initiatives, the CDA works with members to understand and assess top cyber and cybercrime threats affecting CDA membership. Analysis and modelling provide banks with actionable intelligence and up-to-date threat baselines to inform operational response.
Control Mapping and Benchmarking	As part of the Top Threats and CAG initiatives, CDA members map controls to detailed threat models to enable membership-wide benchmarking exercises, gap analysis and facilitate information sharing.
Executive & Operational Requests for Information (RFIs)	Both executive and operational members can send RFIs across relevant Trust Platforms or Working Groups to ask questions or request information from suitable colleagues in fellow member organisations in real time.
Strategic Partnerships	The CDA maintains and develops a network of global partnerships across multiple sectors including, law enforcement, industry bodies, regulatory authorities, CERTs and vendors for the benefit of the membership.
Telecommunication Group & Services	The CDA maintains a sharing group which consists of members and telecommunication organisation partners. The group works jointly to address cyber and fraud attacks impacting cross-sector. The CDA also provides a malicious telephone number takedown service for the UK & Eiré and a call data application service whereby call data relating to fake bank call centres is obtained for mitigation and analysis.
Supply Chain Resilience Group	The CDA coordinates a group of organisations involved in supply chain governance and/or oversight to exchange intelligence to build insight and understanding, leading to a more resilient supply chain.

APPENDIX 2: CDA MEMBER PRODUCTS

Product	Cadence	Per Annum Volume	Content
Daily Security Threat Report	Daily (working days only)	253	Curated open-source reporting on significant cyber and cybercrime events including (but not limited to) vulnerabilities, exploits, compromises, APT activity, geo-political activity and other such relevant reporting.
Monthly Summary Report	Monthly	12	Trend analysis, statistic reporting and other such updates.
Book Of Knowledge -relating to threat model/mapping	Occasional	15	Deep Analysis on threat groups/actors, TTPs
Daily Member Operations Call Summary	Monthly	12	Summarised notes of all associate members meeting, highlighting subjects discussed and actions planned.
Trust groups outputs	Ad Hoc	Unknown	Real time bi-directional sharing with other associate members relating to cyber & cybercrime resilience/mitigation.
MiSP threat hunting feed	Daily	365	MiSP feed of identified C2, e.g. Cobalt Strike beacons and other malicious infrastructure.
Strategic partnership sharing	Daily	500 -estimated	Curated cyber & cybercrime reports produced by global partners.
RaaS alerting	Daily	4,500 - estimated	A raw automated feed of identified victims from RaaS blogs.
Emerging daily geo-political reporting	Daily (working days only)	253	Reporting on significant external events that may impact adversely on associate members or the wider community.
Emerging geo-political deep dive products	Occasional	35 - estimated	In-depth reporting outlining the 'so what' in relation to exterior events. This will occasionally include technical assessments to provide a more complete understanding of the threat picture.
Training & development	Ad Hoc	6	Educational, expert presentations on a range of subjects relating to cyber & cybercrime. CPD/CPE credits available for all events. Additional access to previously recorded presentations.
Critical vulnerability reporting	Ad hoc	250	Curated alerts on critical vulnerabilities that require priority patching/mitigation as they are likely to be exploited or are subject to threat actor/dark web chatter.