

MINISTER'S VALUE-FOR-MONEY ACHIEVEMENT AWARD



Civil Aviation Authority of Singapore

MERIT AWARD

MANAGING EVOLVING CYBER THREATS TARGETING THE AVIATION SECTOR

Ransomware Monitoring	Website Monitoring	Vulnerability Monitoring	CAAS Cybersecurity Portal
<p>I-CDC Ransomware Mon 6 members</p> <p>upordown New Ransomware Victim Detected!</p> <p>Victim: Prosegur Country: SG Group: worldleaks Discovered: 2025-08-23 08:10:26.675811 Description: AI generated Prosegur is a global security company based in Spain. It offers a wide range of services including cash in transit, alarm monitoring, c... URL: https://www.ransomware.live/id/UHJvc2VndXJAd29ybGRsZWFrCW==</p>	<p>UpOrDown 16 members</p> <p>upordown Website is not reachable for 10 mins! Date & Time: 2025-08-28 08:18 URL: https://esoms.caas.gov.sg Redirected URL: https://esoms.caas.gov.sg/ HTTP Response Code: 403</p> <p>esoms.caas.gov.sg eSOMS - Enterprise Safety Oversight Management System Enterprise-Safety Oversight Management (eSOMS), an e-Service brought to you by the Civil Aviation Authority of Singapore (CAAS). eSOMS is a one-stop online portal...</p>	<p>I-CDC Vulnerability Mon 6 members</p> <p>cyint Zero Day Vulnerability Database Zero Day: Remote code execution in Microsoft SharePoint Server CVE: CVE-2025-53770 Disclosed Date: 2025-07-20 Patch Issued Date: 2025-07-21 https://www.zero-day.cz/database/1017/</p> <p>www.zero-day.cz Zero-day vulnerability in Microsoft SharePoint Server - zero-day.cz Zero-day (0day) vulnerability tracking project database. All zero-day vulnerabilities since</p>	<p>Welcome to the CAAS Cybersecurity Portal</p> <p>Get help with common cybersecurity issues, and connect with your cyber team</p> <p>GITSIR OPERATIONAL INSTRUCTIONS GITSIR SPECIAL TECHNICAL INSTRUCTIONS</p> <p>Cybersecurity Incidents Reporting and Self-help resources</p> <p>Frequently asked questions</p> <ul style="list-style-type: none"> How do I log tickets for cybersecurity issues? What can I contact for cybersecurity issues? When do I report outcomes with data protection? What should I do if suspected my system is infected... System outages - what should I do? How do I update my system's schedule? See more FAQs

PROJECT TEAM



- | | |
|---------------|-------------|
| Kee-Vin Ho | Advisor |
| Alan Ong | Team Leader |
| Jasmine Ang | Member |
| Wong Kok Yong | Member |
| Teo Wai Kiat | Member |
| Lim Kim Chong | Member |
| Charisse Tan | Member |

MINISTER'S VALUE-FOR-MONEY ACHIEVEMENT AWARD

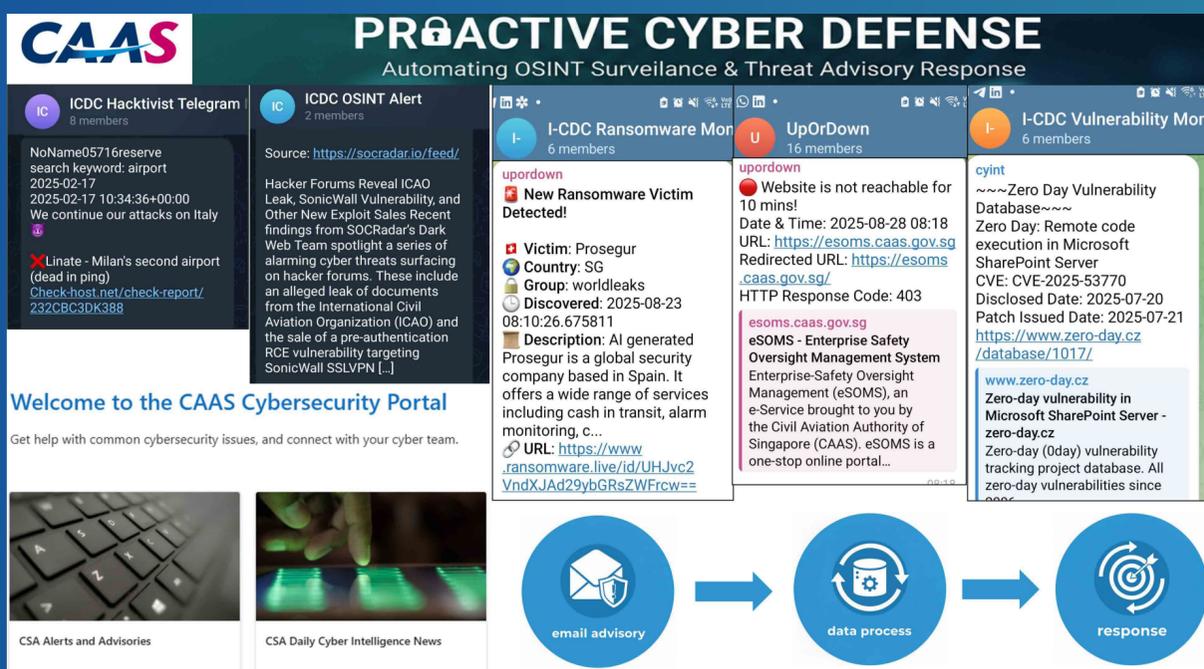


Civil Aviation Authority of Singapore

MERIT AWARD

MANAGING EVOLVING CYBER THREATS TARGETING THE AVIATION SECTOR

NEED FOR PROJECT



- CAAS, as the critical information infrastructure (CII) sector lead for the aviation sector, aims to enhance aviation sector cyber threat awareness by providing early warning detection and enabling faster sectoral response through cybersecurity monitoring and threat intelligence sharing.
- The evolving cyber threats required new detection methods as these involved threats beyond the conventional nation-state threat actors. In recent years, hacktivists had targeted both the aviation sector and Singapore. They organised their attacks via Telegram groups.
- The CAAS team envisioned ways to detect and disseminate information and their responses efficiently for CAAS and the sector stakeholders.

PROBLEM STATEMENT

Need to provide early warning detection and enable faster sectoral response by automating open source intelligence (OSINT) surveillance and threat alert and advisory response.

MINISTER'S VALUE-FOR-MONEY ACHIEVEMENT AWARD



MERIT AWARD

MANAGING EVOLVING CYBER THREATS TARGETING THE AVIATION SECTOR

SOLUTION

```
pythonProject venv > pip install google-news-feedparser
pythonProject venv > python search_google_rss_feeds.py

search_google_rss_feeds.py
def search_google_rss_feeds(keyword_list):
    feeds_data = []
    for keyword in keyword_list:
        GOOGLE_NEWS_RSS_URL = "https://news.google.com/rss/search?q=Aviation+Cyber+Incident&hl=en-US&gl=US&cid=US-en"
        GOOGLE_NEWS_RSS_URL = "https://news.google.com/rss/search?q=" + str(keyword) + "&hl=en-US&gl=US&cid=US-en"
        print("Attempting to fetch entries from: " + GOOGLE_NEWS_RSS_URL)
        news_entries = get_google_news_entries(GOOGLE_NEWS_RSS_URL, max_entries=5)
        if news_entries:
            print("Successfully fetched " + str(len(news_entries)) + " entries.")
            for i, entry in enumerate(news_entries[:100]):
                if check_today(entry['pubdate']):
                    date = convert_date(entry['pubdate'])
                    raw = str(date) + "\n" + \
                        str(entry['title']) + "\n" + \
                        str(entry['link']) + "\n" + \
                        str(entry['description'][:100])
                    feeds_data.append({
                        "source": "google news rss feeds",
                        "keyword": keyword,
                        "title": entry['title'],
                        "published_date": date,
                        "content": entry['description'][:100],
                        "link": entry['link'],
                        "raw": raw
                    })
    else:
        continue
    return feeds_data
```



- Wrote codes to automate monitoring of open source platforms for intelligence via APIs, RSS feeds, web scraping and custom scripts, and send notifications to respective Telegram groups.

- Designed an automation process on a Robotic Process Automation (RPA) platform to process and respond to email alerts and advisories, and develop a centralised SharePoint portal for alert collation and management.

SOLUTION STATEMENT

Developed in-house solutions to automate: 1) monitoring of open source intelligence for cyber threats relevant to the aviation sector and providing notifications on a messaging platform; and 2) processing email alerts and advisories from cybersecurity authorities and responses.

MINISTER'S VALUE-FOR-MONEY ACHIEVEMENT AWARD



MERIT AWARD

MANAGING EVOLVING CYBER THREATS TARGETING THE AVIATION SECTOR

IMPACT

 Economy	 Efficiency	 Effectiveness
<ul style="list-style-type: none"> Eliminates the need to procure separate external threat intelligence platforms 13,400 annual man-hours saved by automated monitoring and collation Central solution saves aviation sector members \$2.2M 	<ul style="list-style-type: none"> Prompt identification of cyber threats and risks Eliminates human intervention, reducing the risk of human error Reduces manual monitoring and collation requirements, allowing human analysts and CAAS officers to focus on high-value tasks 	<ul style="list-style-type: none"> Sectoral cyber threat awareness beyond traditional system monitoring, enabling timely preventative measures Correlation of identified cyber threats and risks with systems' activities to identify possible indication of compromise and impact Sectoral information can be used by CSA and MINDEF to enhance national cyber threat awareness

- In-house developed solutions achieved cost savings, and the automation achieved productivity gains by eliminating manual processes and enabling early warning and faster sectoral response.
- **Cost savings: \$2.20mil**
- **Time savings: 13,400 man-hours.**

OUTCOME STATEMENT

CAAS benefitted from substantial cost and man-hours savings, prompt identification of cyber threats, and enhanced sectoral cyber threat awareness beyond traditional system monitoring, leading to timely preventative measures.