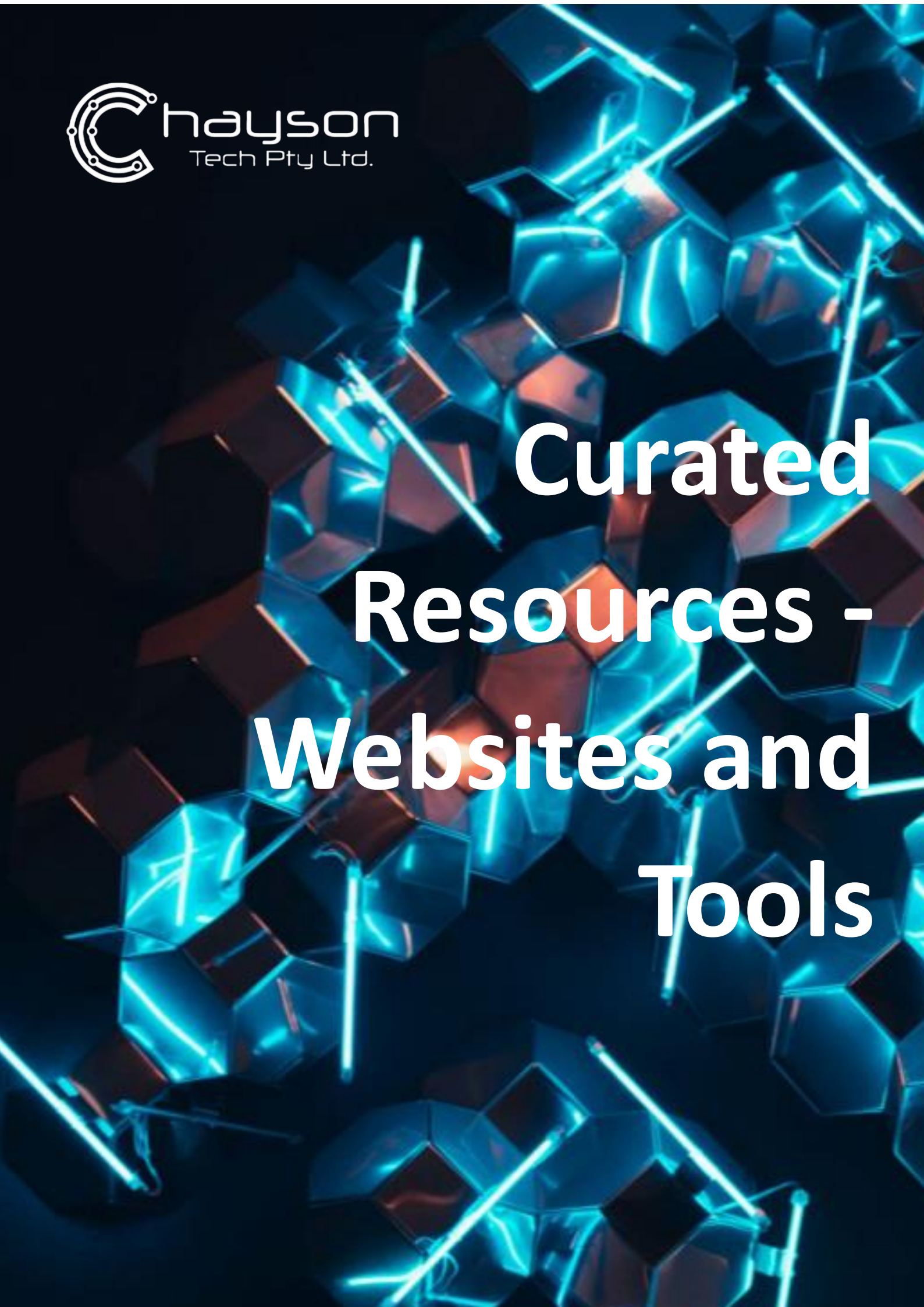
Chayson
Tech Pty Ltd.
Curated Resources - Websites and Tools

Introduction

Welcome to the comprehensive intelligence resources collection curated by Chayson Tech Pty Ltd. This guide provides an extensive compilation of valuable websites, across various domains of intelligence and cybersecurity. Whether you are an analyst, researcher, or enthusiast, this collection will aid in expanding your knowledge and enhancing your capabilities in the field.

This curated collection of intelligence and cybersecurity resources aims to provide you with comprehensive, up-to-date tools and materials to enhance your professional development and expertise in the field. With the rapid evolution of threats and technologies, staying informed and adaptable is critical. Whether you're just starting out in the intelligence domain or are a seasoned professional, the resources included here will support your ongoing learning journey and keep you at the forefront of developments in your field.

By leveraging the websites and platforms organized in this guide, you will gain access to valuable insights into various intelligence methodologies, from open-source intelligence (OSINT) to advanced cybersecurity frameworks. The resources on geospatial tools and MITRE frameworks will equip you with specialized skills for critical decision-making and threat mitigation. Additionally, the sections on technology and innovation, as well as government policies, will ensure you're prepared for the challenges posed by an increasingly interconnected and technology-driven world.

At Chayson Tech Pty Ltd, we are committed to fostering the growth of professionals in intelligence and cybersecurity through the provision of high-quality resources that are both practical and intellectually stimulating. As the global landscape continues to shift, we hope this collection will serve as an essential reference point to keep your skills sharp and your knowledge up to date. Through continued learning and application of these resources, you will be well-equipped to meet current and future challenges with confidence.

Thank you for exploring this collection. We encourage you to regularly revisit these resources, as we will continue to update and expand the content to reflect emerging trends and innovations in the ever-evolving fields of intelligence and cybersecurity.

Contents

Website Descriptions and Categorisation

1. News and Reports

1.1 Defence and Warfare

Institute for the Study of War (understandingwar.org)

Description: The Institute for the Study of War (ISW) is a non-partisan, non-profit organization that provides in-depth, real-time, and strategic analysis of defence and warfare issues. ISW offers reports, maps, and assessments on conflicts, focusing primarily on Middle Eastern regions, Russia, and other global hotspots.

Key Features:

- Detailed reports and assessments on current conflicts.
- Interactive maps and infographics.
- Expert analysis and policy recommendations.
- Regular publications and event briefings.

Notable Content/Services: ISW's "Situation Reports" and "Special Reports" provide comprehensive insights into ongoing military operations and strategic developments.

Cost: Free access to reports and analysis.

Small Wars Journal (smallwarsjournal.com)

Description: Small Wars Journal (SWJ) is an online magazine and professional community focused on irregular warfare, counterinsurgency, and military strategy. It serves as a platform for military professionals and academics to share insights and experiences.

Key Features:

- Articles and essays on military strategy and small wars.
- Open-source intelligence and news aggregation.
- Community forums and discussions.
- Comprehensive library of research and case studies.

Notable Content/Services: SWJ's "Journal Articles" and "Blog Posts" sections feature contributions from thought leaders in the field of defence.

Cost: Free access to most content; some premium content may require registration.

Centre for Strategic and International Studies (CSIS) (csis.org)

Description: CSIS is a bipartisan, nonprofit policy research organization dedicated to providing strategic insights and policy solutions to decision-makers. It covers a wide range of topics including defence, cybersecurity, economic policy, and global health.

Key Features:

- In-depth research reports and analysis.
- Expert commentary and podcasts.
- Interactive data and visualizations.
- Conferences and events.

Notable Content/Services: CSIS's "Defence and Security" program provides comprehensive analyses of military strategy, defence policy, and global security challenges.

Cost: Free access to reports and multimedia content.

2. Technology and Cybersecurity News

2.1 General Cybersecurity News

BleepingComputer (bleepingcomputer.com)

Description: BleepingComputer is a leading news source and community forum focused on cybersecurity, technology news, and troubleshooting guides. It provides timely updates on security threats, software issues, and tech news.

Key Features:

- Latest cybersecurity news and threat reports.
- Comprehensive guides and tutorials.
- Software reviews and recommendations.
- Active community forums for tech support.

Notable Content/Services: BleepingComputer's "News" section offers real-time updates on major cybersecurity incidents and software vulnerabilities.

Cost: Free access to most content; some advanced tutorials and forums may require registration.

The Hacker News (thehackernews.com)

Description: The Hacker News is a prominent online platform dedicated to information security news and updates. It covers a wide range of topics including hacking, cyber threats, data breaches, and information security.

Key Features:

- Daily updates on cybersecurity incidents and trends.
- In-depth articles on emerging threats and vulnerabilities.
- Expert opinions and analysis.
- Cybersecurity event coverage.

Notable Content/Services: The Hacker News offers a "THN Deals" section featuring discounts on cybersecurity tools and training courses.

Cost: Free access to articles and news; some deals and resources may have associated costs.

ITnews (itnews.com)

Description: ITnews is an Australian technology news website that provides up-to-date coverage on IT, telecommunications, and cybersecurity developments. It focuses on the business impact of technology trends and innovations.

Key Features:

- News articles on IT and cybersecurity trends.
- In-depth features on technology innovations.
- Industry analysis and reports.
- Event coverage and interviews.

Notable Content/Services: ITnews's "Security" section offers detailed insights into the latest cybersecurity threats and defences.

Cost: Free access to news articles; subscription may be required for premium content.

3. Government and Policy

3.1 Australia

Digital Transformation Agency (thedigital.gov.au)

Description: The Digital Transformation Agency (DTA) is an Australian government agency responsible for driving digital transformation across the public sector. It aims to improve government services through innovative digital solutions.

Key Features:

- Digital service standards and guidelines.
- Case studies and success stories.
- Resources and toolkits for digital projects.
- Training and events.

Notable Content/Services: DTA's "Projects and Initiatives" section highlights key digital transformation projects within the Australian government.

Cost: Free access to resources and publications.

Australian Defence Doctrine (theforge.defence.gov.au/doctrine)

Description: The Australian Defence Doctrine and Training Centre (ADFTC) provides the official doctrinal publications of the Australian Defence Force (ADF). It offers a comprehensive repository of military doctrine and strategic documents.

Key Features:

- Access to doctrinal publications and manuals.
- Training resources and educational materials.
- Research papers and analysis.
- Doctrine development and review.

Notable Content/Services: The "Doctrine Library" provides access to key doctrinal documents used by the ADF.

Cost: Free access to publications.

Critical Technologies Policy Coordination Office (industry.gov.au/publications/list-critical-technologies-national-interest)

Description: This office, part of the Australian Government Department of Industry, Science, Energy and Resources, focuses on coordinating policies related to critical technologies of national interest.

Key Features:

- Policy documents and strategic reports.
- Analysis of critical technology trends.
- Coordination of national efforts in technology innovation.
- Collaboration with industry and research institutions.

Notable Content/Services: The "Publications" section provides access to key policy documents and reports on critical technologies.

Cost: Free access to policy documents and reports.

Churchill Trust Projects and Fellows (churchilltrust.com.au)

Description: The Churchill Trust awards fellowships to Australians to travel overseas and conduct research in their field of interest. It supports a wide range of projects across various disciplines.

Key Features:

- Information on applying for Churchill Fellowships.
- Database of past fellows and their research projects.
- Resources for fellowship recipients.
- Success stories and impact assessments.

Notable Content/Services: The "Fellows and Projects" section provides detailed information on past fellowship projects and their outcomes.

Cost: Free access to information and resources; fellowship application process is competitive.

3.2 Ukraine

SSU (ssu.gov.ua)

Description: The Security Service of Ukraine (SSU) is the main government authority responsible for national security and intelligence. It provides updates and reports on security issues and threats facing Ukraine.

Key Features:

- News and updates on security operations.
- Reports on counterintelligence activities.
- Public announcements and alerts.
- Historical archives and research.

Notable Content/Services: The SSU's "News" section offers regular updates on the agency's activities and security operations.

Cost: Free access to news and reports.

4. Cyber Law

4.1 Cyber Law Resources

CCDCOE Cyber Law (cyberlaw.ccdcoe.org/wiki/Main_Page)

Description: The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) Cyber Law Wiki is an online resource that provides comprehensive information on international cyber law. It covers legal aspects of cyber operations and cyber security.

Key Features:

- Extensive legal resources and case studies.
- Analysis of international cyber law developments.
- Guidance on legal frameworks and policies.
- Collaboration with legal experts and institutions.

Notable Content/Services: The "Legal Resources" section offers a detailed wiki of cyber law topics and references.

Cost: Free access to resources and legal analysis.

5. Training and Education

5.1 OSINT and Cybersecurity

Chris Sanders Training (chrissanders.org/training)

Description: Chris Sanders provides a variety of cybersecurity training courses focused on network defence, threat hunting, and intrusion detection. His training materials are well-regarded for their practical approach and in-depth content.

Key Features:

- Courses on network security and threat detection.
- Practical labs and hands-on exercises.
- Video lectures and comprehensive course materials.
- Community forums and support.

Notable Content/Services: Chris Sanders offers the "Practical Packet Analysis" course, which is highly recommended for network security professionals.

Cost: Courses are available for purchase; prices vary by course.

Hatless1der OSINT Blog (hatless1der.com)

Description: Hatless1der OSINT Blog is a resource for open-source intelligence (OSINT) techniques and strategies. The blog covers various methods for gathering and analysing publicly available information for cybersecurity purposes.

Key Features:

- Articles and tutorials on OSINT techniques.
- Tools and resources for OSINT investigations.
- Case studies and real-world applications.
- Regular updates and expert insights.

Notable Content/Services: The blog's "Tool Reviews" section provides detailed evaluations of various OSINT tools.

Cost: Free access to blog content.

OSINT Techniques Blog (osinttechniques.com)

Description: OSINT Techniques Blog offers detailed guides and articles on methods and tools for open-source intelligence gathering. It aims to help individuals improve their OSINT skills through practical advice and tutorials.

Key Features:

- Step-by-step guides on OSINT methods.
- Reviews of OSINT tools and software.
- Practical examples and case studies.
- Tips for staying anonymous during investigations.

Notable Content/Services: The "Tutorials" section provides extensive step-by-step guides for beginners and advanced users alike.

Cost: Free access to blog content.

Benjamin Strick OSINT Blog (benjaminstrick.com)

Description: Benjamin Strick's OSINT Blog focuses on investigative journalism and open-source intelligence. It features insights and methodologies for conducting thorough OSINT investigations, often related to social issues and conflicts.

Key Features:

- Investigative articles and reports.
- Methodological guides and tools for OSINT.
- Case studies on various social issues and conflicts.
- Educational resources and training materials.

Notable Content/Services: The blog includes in-depth investigations into human rights abuses and conflict zones.

Cost: Free access to blog content.

Introduction to OSINT - Security Blue Team (elearning.securityblue.team/login#description)

Description: This online course by Security Blue Team provides a comprehensive introduction to OSINT. It covers the fundamental techniques and tools required to perform effective open-source intelligence investigations.

Key Features:

- Structured e-learning modules.
- Interactive exercises and labs.
- Access to a community of learners.
- Certification upon completion.

Notable Content/Services: The course includes practical labs that simulate real-world OSINT investigations.

Cost: Subscription-based access; pricing details available on the website.

Introduction to Dark Web Operations - Security Blue Team

Description: This course by Security Blue Team focuses on the tools and techniques used for navigating and investigating the dark web. It is designed for cybersecurity professionals who need to understand the threats and activities within dark web environments.

Key Features:

- Comprehensive modules on dark web concepts.
- Hands-on labs and exercises.
- Guidance on legal and ethical considerations.

- Certification upon completion.

Notable Content/Services: The course includes detailed tutorials on using dark web monitoring tools.

Cost: Subscription-based access; pricing details available on the website.

OSINT Workshop (courses.thecyberinst.org/courses/osintworkshop)

Description: Offered by The Cyber Institute, this OSINT Workshop provides hands-on training in open-source intelligence gathering. It is designed for both beginners and experienced practitioners.

Key Features:

- Interactive workshops and live sessions.
- Practical exercises and case studies.
- Access to course materials and resources.
- Certification upon completion.

Notable Content/Services: The workshop includes real-world scenarios to practice OSINT techniques.

Cost: Course fees apply; details available on the website.

Maltego for Cybercrime Investigations (academy.maltego.com/maltego-for-cybercrime-foundations?msg=not-logged-in)

Description: This course from Maltego Academy teaches how to use Maltego for cybercrime investigations. Maltego is a powerful tool for link analysis and data visualization, widely used in OSINT investigations.

Key Features:

- Training on Maltego's features and functionalities.
- Practical exercises and use cases.
- Video tutorials and interactive modules.
- Certification upon completion.

Notable Content/Services: The course includes detailed walkthroughs of Maltego investigations, focusing on cybercrime.

Cost: Subscription-based access; pricing details available on the website.

Threat Intelligence Lifecycle (threat.media)

Description: Threat.Media provides insights and training on the threat intelligence lifecycle. This includes the collection, analysis, and dissemination of threat intelligence to improve cybersecurity defences.

Key Features:

- Articles and tutorials on threat intelligence.

- Case studies and practical examples.
- Tools and resources for threat intelligence analysis.
- Regular updates and expert insights.

Notable Content/Services: The website offers in-depth articles on the various stages of the threat intelligence lifecycle.

Cost: Free access to articles and resources.

Diamond Model of Intrusion Analysis (recordedfuture.com)

Description: This resource by Recorded Future explains the Diamond Model of Intrusion Analysis, a framework used to understand and analyse cyber intrusions. It is designed for cybersecurity professionals involved in threat analysis and response.

Key Features:

- Detailed explanation of the Diamond Model.
- Practical examples and case studies.
- Tools and techniques for applying the model.
- Research papers and reports.

Notable Content/Services: Recorded Future provides comprehensive guides and practical applications of the Diamond Model in cybersecurity operations.

Cost: Free access to resources; some premium content may require a subscription.

6. e-Learning

6.1 Intelligence and Law Enforcement Training

ONI e-Learning (learning.intelligence.gov.au/user_login)

Description: ONI e-Learning is an online platform provided by the Office of National Intelligence (ONI) in Australia. It offers training courses designed to enhance the skills of intelligence personnel.

Key Features:

- Courses on intelligence analysis and techniques.
- Interactive modules and assessments.
- Resources and reference materials.
- Certification upon completion.

Notable Content/Services: The platform includes specialized courses tailored to the needs of intelligence professionals.

Cost: Access may be restricted to authorized personnel; pricing details not publicly available.

Police College - Effective Analysis (app.college.police.uk)

Description: This course, offered by the College of Policing, focuses on enhancing analytical skills within the law enforcement community. It covers various techniques and methodologies for effective analysis in policing.

Key Features:

- Structured training modules.
- Practical exercises and case studies.
- Interactive content and assessments.
- Certification upon completion.

Notable Content/Services: The course provides real-world scenarios to apply analytical techniques in law enforcement contexts.

Cost: Access may be restricted to law enforcement personnel; pricing details available upon registration.

7. Cybersecurity and Threat Intelligence

7.1 Threat Intelligence Platforms

GreyNoise (greynoise.io)

Description: GreyNoise is a cybersecurity platform that helps organizations understand and mitigate the noise in their network traffic. It provides context on IP addresses, identifying whether they are part of benign scanning activities or potential threats.

Key Features:

- IP context and reputation data.
- Noise filtering to reduce false positives.
- API access for integration with security tools.
- Real-time monitoring and alerts.

Notable Content/Services: GreyNoise offers a "Noise Explorer" tool for detailed IP analysis and a community plan with limited access to the platform.

Cost: Free tier available; subscription plans for advanced features.

TruKno (trukno.com)

Description: TruKno is a threat intelligence platform that aggregates and analyses threat data from various sources to provide actionable insights. It helps organizations stay informed about emerging threats and vulnerabilities.

Key Features:

- Threat data aggregation and analysis.
- Real-time threat alerts and updates.

- Dashboards and visualizations.
- Integration with other security tools.

Notable Content/Services: TruKno offers a comprehensive dashboard for monitoring and managing threat intelligence.

Cost: Subscription-based access; pricing details available on the website.

AlienVault OTX (otx.alienvault.com)

Description: AlienVault's Open Threat Exchange (OTX) is a community-powered threat intelligence platform. It enables security professionals to share and collaborate on threat data and indicators of compromise (IOCs).

Key Features:

- Community-driven threat intelligence sharing.
- Real-time threat data and IOCs.
- API access for integration with security tools.
- Interactive threat intelligence dashboards.

Notable Content/Services: OTX offers a robust community platform for sharing and accessing threat intelligence.

Cost: Free access to basic features; premium features available through AlienVault products.

ANY.RUN (app.any.run)

Description: ANY.RUN is an interactive online malware analysis sandbox. It allows users to analyse malware behaviour in a controlled environment, providing detailed insights into malicious activities.

Key Features:

- Interactive malware analysis.
- Real-time behaviour monitoring.
- Detailed reports and visualizations.
- Community sharing of analysis results.

Notable Content/Services: ANY.RUN's interactive analysis allows users to manipulate the environment to observe different behaviours of malware.

Cost: Free tier available; subscription plans for advanced features.

Censys (search.censys.io)

Description: Censys is a platform for discovering and monitoring devices and assets exposed on the internet. It provides comprehensive internet-wide scanning and data collection capabilities to help organizations manage their attack surface.

Key Features:

- Internet-wide scanning and asset discovery.
- Real-time monitoring and alerts.
- Detailed reports and data visualization.
- API access for integration with security tools.

Notable Content/Services: Censys offers in-depth visibility into exposed assets and potential vulnerabilities.

Cost: Free tier available; subscription plans for advanced features.

CriminalIP (criminalip.io)

Description: CriminalIP is a cybersecurity intelligence platform that provides detailed insights into IP addresses and domains involved in malicious activities. It helps organizations identify and mitigate potential threats.

Key Features:

- IP and domain reputation analysis.
- Threat intelligence data and reports.
- Real-time monitoring and alerts.
- API access for integration with security tools.

Notable Content/Services: CriminalIP offers detailed threat intelligence reports on suspicious IPs and domains.

Cost: Subscription-based access; pricing details available on the website.

Dehashed (dehashed.com)

Description: Dehashed is a data breach search engine and analysis platform. It allows users to search for compromised credentials and personal information across various data breaches.

Key Features:

- Comprehensive breach data search.
- Real-time monitoring and alerts.
- Detailed reports and data analysis.
- API access for integration with security tools.

Notable Content/Services: Dehashed provides detailed information on breached credentials, helping organizations manage compromised data.

Cost: Subscription-based access; pricing details available on the website.

FOFA (en.fofa.info)

Description: FOFA is an internet asset search engine and threat intelligence platform. It helps users discover and monitor internet-connected devices and systems for potential vulnerabilities.

Key Features:

- Internet asset discovery and monitoring.
- Real-time threat intelligence data.
- Detailed reports and visualizations.
- API access for integration with security tools.

Notable Content/Services: FOFA offers extensive search capabilities for discovering exposed assets and potential vulnerabilities.

Cost: Free tier available; subscription plans for advanced features.

GreyNoise Viz (viz.greynoise.io)

Description: GreyNoise Viz is a visualization tool that provides insights into internet noise and scanning activity. It helps organizations understand the background noise in their network traffic.

Key Features:

- Interactive visualizations of internet noise.
- Detailed reports and data analysis.
- Real-time monitoring and alerts.
- Integration with GreyNoise platform.

Notable Content/Services: GreyNoise Viz offers advanced visualization capabilities for analysing internet noise.

Cost: Free access; additional features available through GreyNoise subscription plans.

Have I Been Pwned (haveibeenpwned.com)

Description: Have I Been Pwned (HIBP) is a service that allows users to check if their email addresses or personal information have been compromised in data breaches. It aggregates data from various breaches to provide a comprehensive search tool.

Key Features:

- Data breach search engine.
- Real-time breach alerts and notifications.
- API access for integration with security tools.
- Educational resources on data security.

Notable Content/Services: HIBP offers a notification service to alert users when their information appears in new breaches.

Cost: Free access to search engine; premium services available for organizations.

Hybrid Analysis (hybrid-analysis.com)

Description: Hybrid Analysis is a malware analysis service provided by CrowdStrike. It offers in-depth analysis of malware samples, providing detailed reports on their behaviour and characteristics.

Key Features:

- Automated malware analysis.
- Detailed reports and visualizations.
- Community sharing of analysis results.
- API access for integration with security tools.

Notable Content/Services: Hybrid Analysis offers a community platform where users can share and access malware analysis results.

Cost: Free access to basic features; premium features available through CrowdStrike products.

Intezer (intezer.com)

Description: Intezer provides advanced threat detection and response capabilities by analysing the genetic code of malware. It helps organizations identify and mitigate threats through detailed code analysis.

Key Features:

- Genetic malware analysis.
- Real-time threat detection and alerts.
- Detailed reports and data visualization.
- Integration with other security tools.

Notable Content/Services: Intezer's unique approach to malware analysis provides deep insights into the origins and relationships of malware samples.

Cost: Subscription-based access; pricing details available on the website.

LeakCheck (leakcheck.io)

Description: LeakCheck is a platform that helps users search for compromised credentials and personal information across various data breaches. It provides detailed reports and real-time alerts on compromised data.

Key Features:

- Comprehensive breach data search.
- Real-time monitoring and alerts.
- Detailed reports and data analysis.

- API access for integration with security tools.

Notable Content/Services: LeakCheck offers a notification service to alert users when their information appears in new breaches.

Cost: Subscription-based access; pricing details available on the website.

MalwareBazaar (bazaar.abuse.ch)

Description: MalwareBazaar is a repository of malware samples provided by Abuse.ch. It allows researchers and security professionals to access and analyse malware samples for research and threat intelligence purposes.

Key Features:

- Extensive repository of malware samples.
- Detailed metadata and analysis reports.
- Community sharing and collaboration.
- API access for integration with security tools.

Notable Content/Services: MalwareBazaar offers detailed analysis reports on various malware samples.

Cost: Free access to repository and reports.

NerdyData (nerdydata.com)

Description: NerdyData is a search engine for source code. It allows users to search for specific code snippets, libraries, and technologies across millions of websites, helping developers and researchers find relevant code quickly.

Key Features:

- Comprehensive source code search engine.
- Real-time monitoring and alerts.
- Detailed reports and data analysis.
- API access for integration with development tools.

Notable Content/Services: NerdyData provides advanced search capabilities for discovering specific code snippets and technologies.

Cost: Subscription-based access; pricing details available on the website.

Onyphe (onyphe.io)

Description: Onyphe is a search engine for cyber threat intelligence data. It aggregates and analyses data from various sources to provide insights into internet-wide threats and vulnerabilities.

Key Features:

- Comprehensive threat intelligence data.
- Real-time monitoring and alerts.
- Detailed reports and visualizations.
- API access for integration with security tools.

Notable Content/Services: Onyphe offers detailed insights into internet-wide threats and vulnerabilities.

Cost: Free tier available; subscription plans for advanced features.

PublicWWW (publicwww.com)

Description: PublicWWW is a source code search engine that allows users to find HTML, JavaScript, and other code snippets within websites. It is used for web scraping, SEO research, and competitive analysis.

Key Features:

- Comprehensive source code search engine.
- Real-time monitoring and alerts.
- Detailed reports and data analysis.
- API access for integration with development tools.

Notable Content/Services: PublicWWW offers advanced search capabilities for discovering specific code snippets and technologies.

Cost: Subscription-based access; pricing details available on the website.

Pulsedive (pulsedive.com)

Description: Pulsedive is a threat intelligence platform that aggregates and analyses data from various sources to provide actionable insights. It helps organizations identify and mitigate potential threats through detailed threat intelligence data.

Key Features:

- Threat data aggregation and analysis.
- Real-time threat alerts and updates.
- Dashboards and visualizations.
- Integration with other security tools.

Notable Content/Services: Pulsedive offers a comprehensive dashboard for monitoring and managing threat intelligence.

Cost: Free tier available; subscription plans for advanced features.

Searchcode (searchcode.com)

Description: Searchcode is a source code search engine that allows users to find code snippets, libraries, and technologies across millions of public repositories. It helps developers and researchers quickly locate relevant code.

Key Features:

- Comprehensive source code search engine.
- Real-time monitoring and alerts.
- Detailed reports and data analysis.
- API access for integration with development tools.

Notable Content/Services: Searchcode provides advanced search capabilities for discovering specific code snippets and technologies.

Cost: Free access to basic features; premium features available through subscription plans.

Shodan (shodan.io)

Description: Shodan is a search engine for internet-connected devices. It allows users to discover and monitor devices exposed on the internet, providing detailed information on potential vulnerabilities and threats.

Key Features:

- Internet-wide scanning and asset discovery.
- Real-time monitoring and alerts.
- Detailed reports and data visualization.
- API access for integration with security tools.

Notable Content/Services: Shodan offers extensive search capabilities for discovering exposed assets and potential vulnerabilities.

Cost: Free tier available; subscription plans for advanced features.

VirusTotal (virustotal.com)

Description: VirusTotal is an online service that analyses files and URLs for malware. It aggregates data from various antivirus engines and tools to provide comprehensive analysis reports.

Key Features:

- File and URL malware analysis.
- Aggregation of data from multiple antivirus engines.
- Detailed reports and visualizations.
- API access for integration with security tools.

Notable Content/Services: VirusTotal offers a community platform for sharing and accessing malware analysis results.

Cost: Free access to basic features; premium features available through subscription plans.

ZoomEye (zoomeye.org)

Description: ZoomEye is a search engine for internet-connected devices and assets. It provides comprehensive scanning and data collection capabilities to help organizations manage their attack surface.

Key Features:

- Internet-wide scanning and asset discovery.
- Real-time monitoring and alerts.
- Detailed reports and data visualization.
- API access for integration with security tools.

Notable Content/Services: ZoomEye offers extensive search capabilities for discovering exposed assets and potential vulnerabilities.

Cost: Free tier available; subscription plans for advanced features.

8. MITRE Frameworks

8.1 Cybersecurity and Threat Intelligence

MITRE ATT&CK (attack.mitre.org)

Description: MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. It is used by cybersecurity professionals for threat intelligence, red teaming, and security operations.

Key Features:

- Comprehensive matrix of tactics and techniques.
- Detailed descriptions of adversary behaviours.
- Real-world use cases and examples.
- Integration with various security tools and platforms.

Notable Content/Services: The ATT&CK framework provides a structured approach to understanding and defending against cyber threats.

Cost: Free access to the framework and resources.

MITRE D3FEND (d3fend.mitre.org)

Description: MITRE D3FEND is a knowledge base of defensive countermeasures and techniques mapped to the MITRE ATT&CK framework. It provides a structured approach to implementing defence strategies.

Key Features:

- Detailed descriptions of defensive techniques.
- Mapping to ATT&CK tactics and techniques.
- Resources for implementing defensive measures.
- Integration with security tools and platforms.

Notable Content/Services: D3FEND helps organizations enhance their defence posture by providing actionable countermeasures.

Cost: Free access to the framework and resources.

MITRE ENGAGE (engage.mitre.org)

Description: MITRE ENGAGE is a framework for proactive cyber defence operations. It provides strategies and tactics for engaging with adversaries and managing cybersecurity risks.

Key Features:

- Guidance on proactive defence operations.
- Strategies for adversary engagement.
- Real-world examples and case studies.
- Resources for implementation and training.

Notable Content/Services: ENGAGE offers a structured approach to managing and mitigating cybersecurity risks through proactive defence.

Cost: Free access to the framework and resources.

MITRE ATLAS (atlas.mitre.org)

Description: MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) is a knowledge base that provides insights into adversarial threats against AI systems. It aims to enhance the security and robustness of AI technologies.

Key Features:

- Database of adversarial threats and techniques targeting AI.
- Guidance on securing AI systems.
- Resources for understanding AI vulnerabilities.
- Integration with other MITRE frameworks.

Notable Content/Services: ATLAS offers comprehensive insights into the security challenges of AI systems.

Cost: Free access to the framework and resources.

MITRE CREF NAVIGATOR (lnkd.in/dv6gecGY)

Description: The MITRE Cyber Resiliency Engineering Framework (CREF) Navigator is a tool for navigating the principles and practices of cyber resiliency. It provides resources for enhancing the resiliency of systems against cyber threats.

Key Features:

- Principles and practices of cyber resiliency.
- Tools and resources for implementation.
- Case studies and examples.
- Integration with other MITRE frameworks.

Notable Content/Services: CREF Navigator helps organizations enhance the resiliency of their systems through structured guidance.

Cost: Free access to the framework and resources.

MITRE ATT&CK NAVIGATOR (lnkd.in/ebjisdW6)

Description: The MITRE ATT&CK Navigator is an interactive tool for visualizing and exploring the ATT&CK framework. It allows users to create and share customized views of the ATT&CK matrix.

Key Features:

- Interactive visualization of ATT&CK tactics and techniques.
- Customizable views and layers.
- Collaboration and sharing features.
- Integration with other security tools.

Notable Content/Services: ATT&CK Navigator enhances the usability of the ATT&CK framework through interactive and customizable visualizations.

Cost: Free access to the tool.

MITRE CAR (car.mitre.org)

Description: MITRE Cyber Analytics Repository (CAR) is a collection of analytics for detecting adversary behaviours described in the ATT&CK framework. It provides guidance on implementing these analytics in security operations.

Key Features:

- Detailed analytics for detecting adversary behaviours.
- Mapping to ATT&CK techniques.
- Implementation guides and resources.
- Integration with security tools and platforms.

Notable Content/Services: CAR offers practical analytics that can be implemented in security operations to detect cyber threats.

Cost: Free access to the repository and resources.

MITRE MAEC (lnkd.in/drXBPvXm)

Description: MITRE Malware Attribute Enumeration and Characterization (MAEC) is a standardized language for describing malware attributes and behaviours. It facilitates the sharing of malware analysis information.

Key Features:

- Standardized malware descriptions.
- Tools for creating and sharing MAEC documents.
- Integration with malware analysis tools.
- Resources for implementing MAEC.

Notable Content/Services: MAEC enhances the sharing and understanding of malware characteristics through standardized descriptions.

Cost: Free access to the framework and resources.

MITRE CAPEC (capec.mitre.org)

Description: MITRE Common Attack Pattern Enumeration and Classification (CAPEC) is a comprehensive dictionary of known attack patterns. It helps organizations understand and mitigate common attack vectors.

Key Features:

- Detailed descriptions of attack patterns.
- Mapping to various cybersecurity frameworks.
- Resources for implementing defensive measures.
- Integration with security tools and platforms.

Notable Content/Services: CAPEC provides a structured approach to understanding and defending against common cyber-attacks.

Cost: Free access to the framework and resources.

MITRE Insider Threat Framework (lnkd.in/dbCD2BUD)

Description: The MITRE Insider Threat Framework provides guidance on identifying and mitigating insider threats within organizations. It includes strategies, best practices, and resources for managing insider risk.

Key Features:

- Strategies for identifying insider threats.

- Best practices for mitigating insider risk.
- Case studies and real-world examples.
- Integration with other MITRE frameworks.

Notable Content/Services: The framework helps organizations develop comprehensive insider threat programs.

Cost: Free access to the framework and resources.

MITRE SAF (saf.mitre.org)

Description: MITRE Systems Assurance Framework (SAF) is a set of practices and tools for ensuring the security and resiliency of systems throughout their lifecycle. It provides guidance on implementing security measures at each stage of system development.

Key Features:

- Practices for system security and resiliency.
- Tools and resources for implementation.
- Case studies and examples.
- Integration with other MITRE frameworks.

Notable Content/Services: SAF offers a comprehensive approach to ensuring system security and resiliency from design to deployment.

Cost: Free access to the framework and resources.

MITRE Innovation Toolkit (itk.mitre.org)

Description: The MITRE Innovation Toolkit provides tools and resources to foster innovation within organizations. It includes methodologies, templates, and best practices for driving innovative solutions.

Key Features:

- Tools and methodologies for innovation.
- Templates and resources for implementation.
- Case studies and success stories.
- Community and collaboration features.

Notable Content/Services: The toolkit supports organizations in developing and implementing innovative solutions to complex problems.

Cost: Free access to the toolkit and resources.

9. Threat Maps

9.1 Cybersecurity Threat Visualization

Radware Live Threat Map (radware.com)

Description: Radware Live Threat Map provides real-time visualization of cyber threats and attacks occurring globally. It displays data on the origin and target of attacks, helping users understand the current threat landscape.

Key Features:

- Real-time visualization of cyber threats.
- Data on attack origins and targets.
- Types of threats and their frequencies.
- Interactive map with detailed attack information.

Notable Content/Services: The map provides insights into ongoing DDoS attacks, web application attacks, and other cyber threats.

Cost: Free access to the live threat map.

Kaspersky Cybermap (cybermap.kaspersky.com)

Description: Kaspersky Cybermap offers a real-time global view of cyber threats detected by Kaspersky's security network. It visualizes various types of threats and their distribution across different regions.

Key Features:

- Real-time visualization of detected threats.
- Data on malware, phishing, and spam attacks.
- Geographic distribution of threats.
- Interactive and user-friendly interface.

Notable Content/Services: The map provides a comprehensive overview of the global threat landscape with detailed information on different types of cyber threats.

Cost: Free access to the cybermap.

FortiGuard Threat Map (threatmap.fortiguard.com)

Description: FortiGuard Threat Map is an interactive tool that visualizes cyber threats detected by Fortinet's security network. It displays real-time data on global cyber-attacks, providing insights into threat patterns and trends.

Key Features:

- Real-time visualization of cyber threats.
- Information on attack types and origins.

- Detailed threat analysis and reports.
- Interactive map with filtering options.

Notable Content/Services: The threat map offers detailed insights into various types of attacks, including malware, botnets, and network intrusions.

Cost: Free access to the threat map.

Checkpoint Threat Map (threatmap.checkpoint.com)

Description: Checkpoint Threat Map provides a global view of cyber threats detected by Checkpoint's security solutions. It visualizes ongoing attacks, highlighting the sources and targets of cyber threats.

Key Features:

- Real-time visualization of cyber-attacks.
- Data on attack sources and destinations.
- Types of threats and their impact.
- Interactive and easy-to-use interface.

Notable Content/Services: The threat map offers a detailed view of the global threat landscape, helping users understand current cyber threats.

Cost: Free access to the threat map.

Talos Intelligence Threat Map (talosintelligence.com)

Description: Talos Intelligence Threat Map, operated by Cisco Talos, provides real-time data on cyber threats detected by Cisco's security systems. It offers insights into the volume and distribution of various cyber-attacks.

Key Features:

- Real-time threat visualization.
- Detailed information on attack types and sources.
- Geographic distribution of threats.
- Integration with Talos Intelligence services.

Notable Content/Services: The map provides comprehensive insights into global cyber threats, including malware, phishing, and network attacks.

Cost: Free access to the threat map.

Sophos Threat Dashboard (sophos.com)

Description: Sophos Threat Dashboard offers real-time insights into cyber threats detected by Sophos' security solutions. It provides detailed information on various types of threats and their global distribution.

Key Features:

- Real-time threat data and visualization.
- Information on malware, ransomware, and other threats.
- Geographic distribution of threats.
- Interactive dashboard with detailed reports.

Notable Content/Services: The dashboard provides a comprehensive overview of the global threat landscape with detailed threat analysis.

Cost: Free access to the threat dashboard.

SonicWall Threat Centre (sonicwall.com)

Description: SonicWall Threat Centre provides real-time data on cyber threats detected by SonicWall's security network. It visualizes ongoing attacks and provides detailed information on various types of threats.

Key Features:

- Real-time threat visualization.
- Data on attack types and origins.
- Detailed threat analysis and reports.
- Interactive and user-friendly interface.

Notable Content/Services: The threat centre offers insights into various cyber threats, including malware, ransomware, and phishing attacks.

Cost: Free access to the threat centre.

Bitdefender Threat Map (threatmap.bitdefender.com)

Description: Bitdefender Threat Map offers a real-time view of cyber threats detected by Bitdefender's security solutions. It visualizes global cyber-attacks, providing insights into threat patterns and trends.

Key Features:

- Real-time threat visualization.
- Information on attack types and origins.
- Geographic distribution of threats.
- Interactive map with detailed attack information.

Notable Content/Services: The map provides comprehensive insights into ongoing cyber threats, including malware and phishing attacks.

Cost: Free access to the threat map.

NetScout Horizon (horizon.netscout.com)

Description: NetScout Horizon provides real-time visibility into global internet traffic and cyber threats. It offers detailed data on DDoS attacks, network outages, and other security incidents.

Key Features:

- Real-time traffic and threat visualization.
- Data on DDoS attacks and network outages.
- Geographic distribution of threats.
- Interactive map with detailed reports.

Notable Content/Services: Horizon offers insights into global internet health and security threats, helping organizations understand the threat landscape.

Cost: Free access to the horizon map.

ThreatButt Map (threatbutt.com)

Description: ThreatButt Map is a humorous and satirical take on real-time cyber threat maps. It visualizes fake cyber-attacks and provides a light-hearted view of the global threat landscape.

Key Features:

- Humorous visualization of fake cyber-attacks.
- Interactive and user-friendly interface.
- Satirical commentary on cyber threats.

Notable Content/Services: The map offers a light-hearted perspective on the serious topic of cyber threats.

Cost: Free access to the threat map.

10. Internet Outages

10.1 Monitoring and Reporting

NetBlocks (netblocks.org)

Description: NetBlocks is a global internet observatory that monitors and reports on internet disruptions and outages. It provides real-time data on network availability and connectivity issues.

Key Features:

- Real-time monitoring of internet outages.
- Detailed reports on network disruptions.
- Geographic distribution of outages.
- Analysis of the impact of outages on various sectors.

Notable Content/Services: NetBlocks offers comprehensive insights into internet connectivity issues, helping organizations understand and respond to network disruptions.

Cost: Free access to monitoring reports and data.

11. Technology and Innovation

11.1 AI and Machine Learning

X Open AI (github.com/xai-org/grok-1)

Description: X Open AI provides a collection of open-source tools and resources for artificial intelligence research and development. It focuses on advancing AI technologies and making them accessible to researchers and developers.

Key Features:

- Open-source AI tools and frameworks.
- Resources for AI research and development.
- Community contributions and collaborations.
- Documentation and tutorials.

Notable Content/Services: The repository includes various AI models, algorithms, and tools that can be used for research and practical applications.

Cost: Free access to the repository and resources.

Meta AI (ai.meta.com)

Description: Meta AI, formerly known as Facebook AI, is Meta's dedicated research lab for artificial intelligence. It focuses on advancing the state of AI through research in machine learning, computer vision, natural language processing, and more.

Key Features:

- Cutting-edge AI research and publications.
- Tools and frameworks for AI development.
- Open-source projects and collaborations.
- AI-driven solutions for various applications.

Notable Content/Services: Meta AI provides access to research papers, open-source tools, and datasets for the AI community.

Cost: Free access to research publications and open-source projects.

NVIDIA AI (nvidia.com)

Description: NVIDIA AI is a division of NVIDIA that focuses on developing AI hardware and software solutions. It provides tools and platforms for AI research, development, and deployment, leveraging NVIDIA's powerful GPUs.

Key Features:

- AI hardware and software solutions.
- Tools for deep learning and machine learning.
- Research and development resources.
- AI-driven applications and solutions.

Notable Content/Services: NVIDIA AI offers a wide range of tools, including the NVIDIA CUDA toolkit, TensorRT, and the DGX systems for AI research and deployment.

Cost: Free access to certain tools and resources; premium products available for purchase.

Awesome-GPT-Agents (github.com/fr0gger/Awesome-GPT-Agents)

Description: Awesome-GPT-Agents is an open-source collection of tools and resources for building AI agents using GPT models. It provides a curated list of projects, tutorials, and libraries for developing intelligent agents.

Key Features:

- Curated list of GPT-based projects and tools.
- Tutorials and guides for building AI agents.
- Community contributions and collaborations.
- Documentation and best practices.

Notable Content/Services: The repository offers a comprehensive collection of resources for developers interested in creating AI agents with GPT models.

Cost: Free access to the repository and resources.

11.2 GIS and Satellite Imagery

GovMap Israel (govmap.gov.il)

Description: GovMap Israel is a government-operated geographic information system (GIS) that provides detailed maps and spatial data for Israel. It offers various layers of information, including transportation, land use, and environmental data.

Key Features:

- Comprehensive GIS data for Israel.
- Interactive maps with multiple layers.
- Tools for spatial analysis and visualization.
- Public access to government spatial data.

Notable Content/Services: GovMap Israel provides valuable GIS data for urban planning, environmental monitoring, and public infrastructure projects.

Cost: Free access to maps and data.

Sentinel Hub (sentinel-hub.com)

Description: Sentinel Hub is a cloud-based platform for accessing, processing, and analysing satellite imagery. It supports various satellite data sources, including Sentinel, Landsat, and others, providing tools for remote sensing and environmental monitoring.

Key Features:

- Access to a wide range of satellite imagery.
- Tools for image processing and analysis.
- API for integration with other applications.
- Customizable visualization and analysis features.

Notable Content/Services: Sentinel Hub offers powerful tools for remote sensing applications, including agriculture, forestry, and disaster management.

Cost: Free tier available; subscription plans for advanced features and larger data access.

Maxar Satellite Imagery (maxar.com)

Description: Maxar provides high-resolution satellite imagery and geospatial data for various industries, including defence, intelligence, and commercial applications. It offers advanced imagery products and services for detailed earth observation.

Key Features:

- High-resolution satellite imagery.
- Geospatial data and analytics.
- Custom imagery solutions and services.
- Applications in defence, intelligence, and commercial sectors.

Notable Content/Services: Maxar's imagery is used for critical applications such as disaster response, environmental monitoring, and infrastructure planning.

Cost: Custom pricing based on services and data requirements.

Planet (planet.com)

Description: Planet operates a fleet of small satellites that capture high-resolution imagery of the entire Earth daily. It provides access to a vast archive of satellite imagery for various applications, including agriculture, forestry, and urban planning.

Key Features:

- Daily high-resolution satellite imagery.
- Archive of historical imagery.

- Tools for image analysis and visualization.
- API for integration with other applications.

Notable Content/Services: Planet's imagery is used for monitoring environmental changes, agricultural practices, and urban development.

Cost: Free tier available; subscription plans for advanced features and larger data access.

12. Geospatial and Mapping Tools

12.1 Location and Mapping Services

What3Words (what3words.com)

Description: What3Words is a geocoding system that divides the world into a grid of 3m x 3m squares, assigning each a unique combination of three words. This makes it easy to communicate precise locations using just three words.

Key Features:

- Unique three-word addresses for precise locations.
- Easy-to-use mobile app and web interface.
- Integration with mapping and navigation services.
- API for developers to incorporate into their applications.

Notable Content/Services: What3Words is used in various industries, including logistics, emergency services, and travel, for precise location sharing.

Cost: Free access to basic services; API access may have associated costs.

MarineTraffic (marinetraffic.com)

Description: MarineTraffic provides real-time information about the movements of ships and the current location of vessels in ports and harbors worldwide. It uses AIS data to track ship positions and movements.

Key Features:

- Real-time ship tracking and maritime traffic data.
- Interactive map with vessel details and routes.
- Port and harbor information.
- Historical data and analysis tools.

Notable Content/Services: MarineTraffic is widely used in the maritime industry for fleet management, logistics, and maritime safety.

Cost: Free access to basic features; subscription plans for advanced features and data.

ADSB Exchange (adsbexchange.com)

Description: ADSB Exchange is a community-driven platform that provides real-time tracking of aircraft using ADS-B data. It offers an open and unfiltered view of global air traffic.

Key Features:

- Real-time aircraft tracking and flight information.
- Interactive map with detailed aircraft data.
- Historical flight data and analytics.
- API access for integration with other applications.

Notable Content/Services: ADSB Exchange is popular among aviation enthusiasts, researchers, and professionals for its comprehensive and unfiltered air traffic data.

Cost: Free access to basic tracking; subscription plans for advanced features and data.

WikiMapia (wikimapia.org)

Description: WikiMapia is a collaborative mapping project that combines Google Maps with a wiki system, allowing users to add and edit information about locations worldwide. It aims to create a detailed and interactive map of the world.

Key Features:

- User-generated content and mapping data.
- Interactive map with detailed location information.
- Tools for adding and editing map features.
- Community collaboration and contributions.

Notable Content/Services: WikiMapia provides a rich, user-generated database of geographical information, making it useful for various research and educational purposes.

Cost: Free access to all features.

NASA FIRMS (firms.modaps.eosdis.nasa.gov)

Description: NASA's Fire Information for Resource Management System (FIRMS) provides near real-time satellite data on active fires and thermal anomalies. It supports fire management and monitoring by providing timely information on fire locations and behaviour.

Key Features:

- Near real-time fire detection and monitoring.
- Interactive map with fire locations and details.
- Downloadable data and analysis tools.
- Alerts and notifications for fire events.

Notable Content/Services: FIRMS is widely used by fire management agencies, researchers, and policymakers for monitoring and responding to fire events.

Cost: Free access to all features and data.

13. Privacy and Security Tools

13.1 Browser Extensions and Privacy Tools

User-Agent Switcher for Chrome (Chrome Web Store)

Description: User-Agent Switcher for Chrome is a browser extension that allows users to change the user-agent string of their browser. This can help in testing websites, bypassing restrictions, and enhancing privacy.

Key Features:

- Easy switching between different user-agent strings.
- Custom user-agent strings support.
- Integration with Chrome browser.
- Useful for web development and privacy enhancement.

Notable Content/Services: The extension is popular among developers for testing websites and among users who want to enhance their online privacy.

Cost: Free access to the extension.

Privacy Badger (privacybadger.org)

Description: Privacy Badger is a browser extension developed by the Electronic Frontier Foundation (EFF) that automatically blocks trackers and third-party cookies that track your browsing activities.

Key Features:

- Automatic tracker blocking.
- Real-time privacy protection.
- Easy-to-use interface.
- Integration with major browsers.

Notable Content/Services: Privacy Badger enhances user privacy by preventing advertisers and other third-party trackers from monitoring your online behaviour.

Cost: Free access to the extension.

14. Social and Community Platforms

14.1 Social Networks

Untappd (untappd.com)

Description: Untappd is a social networking service for beer enthusiasts. It allows users to check in and rate beers, share their experiences, and discover new beers and breweries.

Key Features:

- Check-in and rate beers.
- Discover new beers and breweries.
- Connect with friends and see their beer activities.
- Participate in beer-related events and promotions.

Notable Content/Services: Untappd provides a platform for beer lovers to explore new beers, share their experiences, and connect with a community of like-minded individuals.

Cost: Free access to basic features; premium features available through a subscription.

Strava (strava.com)

Description: Strava is a social network for athletes that allows users to track and share their workouts. It supports a wide range of activities, including running, cycling, swimming, and more, providing detailed performance analytics.

Key Features:

- Activity tracking and performance analysis.
- Social features to connect with friends and join clubs.
- Challenges and competitions to motivate users.
- Integration with various fitness devices and apps.

Notable Content/Services: Strava is popular among athletes for its detailed performance metrics, social features, and community-driven challenges.

Cost: Free access to basic features; premium subscription for advanced features and analytics.

15. Educational Institutes and Projects

15.1 Defence and Strategic Studies

Unitracker (unitracker.aspi.org.au)

Description: Unitracker is an interactive tool by the Australian Strategic Policy Institute (ASPI) designed to map and analyse international academic collaborations with Chinese universities involved in defence research. It helps identify the scope and nature of these partnerships.

Key Features:

- Interactive map of global collaborations with Chinese defence universities.
- Detailed information on research projects and partnerships.
- Analysis of trends and patterns in academic collaborations.
- Search and filter options for specific institutions and countries.

Notable Content/Services: Unitracker provides valuable insights into the global network of academic collaborations that support China's defence research initiatives.

Cost: Free access to the online tool and data.

15.2 Psychology and Consciousness

Monroe Institute (monroeinstitute.org)

Description: The Monroe Institute is a non-profit educational and research organization dedicated to exploring human consciousness. It offers programs and resources designed to help individuals achieve expanded states of awareness and personal transformation through the use of sound technology and other methods.

Key Features:

- Workshops and retreats on consciousness exploration.
- Research on human consciousness and altered states.
- Hemi-Sync® audio technology for brainwave synchronization.
- Online courses and educational materials.

Notable Content/Services: The Monroe Institute is known for its Hemi-Sync® audio technology, which is used to facilitate meditation, relaxation, and expanded states of consciousness.

Cost: Workshops and programs have associated costs; some online resources and introductory materials are available for free.

16. OSINT and Intelligence Gathering

16.1 Resources and Collections

Start.me Rae Baker Deep Dive OSINT (https://start.me/p/7kYgk2/rae-baker-deep-dive-osint**)**

Description: Rae Baker's Deep Dive OSINT on Start.me is a comprehensive collection of open-source intelligence (OSINT) tools and resources curated by OSINT expert Rae Baker. It focuses on advanced techniques and methodologies for in-depth OSINT investigations.

Key Features:

- Advanced OSINT tools and resources.
- Focus on deep dive techniques and specialized tools.
- Regular updates and expert recommendations.
- Organized categories for different aspects of OSINT.

Notable Content/Services: This collection is particularly useful for experienced OSINT practitioners looking to enhance their skills and explore advanced techniques.

Cost: Free access to the start page and resources.

GitHub OSINT for Countries (github.com/wddadk/OSINT-for-countries)

Description: GitHub OSINT for Countries is a repository that provides OSINT resources categorized by country. It includes tools, datasets, and information sources tailored to specific geographic regions, helping users conduct geographically focused investigations.

Key Features:

- OSINT resources organized by country.
- Links to country-specific tools and datasets.
- Community contributions and updates.
- Documentation and usage guidelines.

Notable Content/Services: The repository offers a valuable resource for conducting OSINT investigations with a geographic focus, providing tailored tools and information for each country.

Cost: Free access to the repository and resources.

GitHub OSINT Mindset (github.com/OSINT-mindset)

Description: GitHub OSINT Mindset is a repository that focuses on the mindset and methodologies of OSINT investigations. It provides guides, tools, and resources to help practitioners adopt a systematic and effective approach to OSINT.

Key Features:

- Guides and methodologies for OSINT investigations.
- Tools and resources for systematic OSINT.
- Community contributions and collaboration.
- Documentation and best practices.

Notable Content/Services: The repository emphasizes the importance of adopting a structured approach to OSINT, offering resources to develop and refine investigative techniques.

Cost: Free access to the repository and resources.

16.2 Training and Education

Packet Capture Training (chrissanders.org/training)

Description: Packet Capture Training by Chris Sanders offers specialized courses focused on network security and intrusion detection through packet analysis. The training is designed to enhance the skills of cybersecurity professionals.

Key Features:

- Courses on packet analysis and network security.
- Hands-on labs and practical exercises.
- Video lectures and comprehensive course materials.
- Community forums and support.

Notable Content/Services: Chris Sanders' training includes the "Practical Packet Analysis" course, which is highly regarded for its practical approach to network security.

Cost: Courses are available for purchase; prices vary by course.

Priority Intelligence Requirements (smallwarsjournal.com)

Description: Priority Intelligence Requirements (PIR) on Small Wars Journal is a collection of articles and resources focused on defining and understanding priority intelligence requirements in military and strategic contexts. It provides insights into how PIRs are developed and used.

Key Features:

- Articles and essays on priority intelligence requirements.
- Case studies and real-world applications.
- Resources for developing and implementing PIRs.
- Expert analysis and commentary.

Notable Content/Services: Small Wars Journal offers valuable insights into the role of PIRs in military and intelligence operations, making it a useful resource for professionals in the field.

Cost: Free access to articles and resources.

17. Other Specific Tools and Platforms

17.1 Threat Intel Bots and Tools

Malware Analyst GPT (Malware Analyst GPT)

Description: Malware Analyst GPT is an AI-powered tool designed to assist in the analysis of malware. It leverages advanced machine learning algorithms to identify, classify, and provide detailed insights into malicious software.

Key Features:

- Automated malware analysis and classification.
- Detailed reports on malware behaviour and characteristics.
- Integration with security tools and platforms.
- Real-time analysis and threat detection.

Notable Content/Services: Malware Analyst GPT helps security professionals quickly understand and respond to malware threats, reducing the time needed for manual analysis.

Cost: Information not provided; likely varies based on usage and integration.

Threat Intel Bot (Threat Intel Bot)

Description: Threat Intel Bot is an AI-driven tool that provides real-time threat intelligence updates and analysis. It aggregates data from multiple sources to deliver actionable insights into emerging threats.

Key Features:

- Real-time threat intelligence updates.
- Aggregation of data from multiple sources.
- Detailed analysis and reporting.
- Integration with security platforms.

Notable Content/Services: The bot provides continuous monitoring and alerts, helping organizations stay ahead of potential threats.

Cost: Information not provided; likely varies based on usage and integration.

Cyber Security Ninja (Cyber Security Ninja)

Description: Cyber Security Ninja is an AI-based tool designed to enhance cybersecurity measures within an organization. It offers a range of features, including threat detection, vulnerability assessment, and automated response actions.

Key Features:

- Threat detection and response.
- Vulnerability assessment and management.
- Automated security operations.
- Integration with existing security infrastructure.

Notable Content/Services: Cyber Security Ninja provides comprehensive security coverage, helping organizations proactively manage and mitigate risks.

Cost: Information not provided; likely varies based on usage and integration.

ATT&CK Mate (ATT&CK Mate)

Description: ATT&CK Mate is a tool designed to work with the MITRE ATT&CK framework, providing detailed insights and mapping of threats to the ATT&CK matrix. It helps organizations understand and implement effective defence strategies.

Key Features:

- Mapping of threats to MITRE ATT&CK framework.
- Detailed threat analysis and reporting.
- Integration with security tools.
- Visualization of attack patterns and techniques.

Notable Content/Services: ATT&CK Mate enhances the usability of the MITRE ATT&CK framework, making it easier for organizations to apply its principles in their security operations.

Cost: Information not provided; likely varies based on usage and integration.

HackTricksGPT (HackTricksGPT)

Description: HackTricksGPT is an AI-powered tool that provides hacking tricks, tips, and techniques for ethical hacking and penetration testing. It offers guidance and resources for cybersecurity professionals to enhance their skills.

Key Features:

- Tips and techniques for ethical hacking.
- Comprehensive guides and tutorials.
- Real-time assistance and support.
- Integration with penetration testing tools.

Notable Content/Services: HackTricksGPT is a valuable resource for ethical hackers and penetration testers looking to stay updated with the latest methods and practices.

Cost: Information not provided; likely varies based on usage and integration.

MagicUnprotect (MagicUnprotect)

Description: MagicUnprotect is a specialized tool designed to remove protections and obfuscations from malicious software, making it easier to analyse. It helps malware analysts quickly understand the true nature of malware.

Key Features:

- Removal of protections and obfuscations from malware.
- Detailed analysis and reporting.
- Integration with malware analysis tools.
- Automated and manual deobfuscation options.

Notable Content/Services: MagicUnprotect simplifies the malware analysis process by stripping away layers of protection used by malicious software to evade detection.

Cost: Information not provided; likely varies based on usage and integration.

SOC Analyst GPT (chat.openai.com/g/g-IjjVSZeUV-cyber-guardian)

Description: SOC Analyst GPT is an AI-driven tool designed to assist Security Operations Centre (SOC) analysts in identifying, analysing, and responding to security incidents. It provides real-time insights and recommendations to improve security operations.

Key Features:

- Real-time incident analysis and response recommendations.
- Integration with SOC tools and platforms.
- Automated threat detection and reporting.

- Continuous learning and improvement from analyst feedback.

Notable Content/Services: SOC Analyst GPT enhances the efficiency and effectiveness of SOC teams by providing AI-driven support and insights for security operations.

Cost: Information not provided; likely varies based on usage and integration.

18. Search and Analysis Platforms

18.1 Threat Intelligence and Analysis

URLScan.io (urlscan.io)

Description: URLScan.io is an online service that allows users to scan and analyse websites. It provides detailed information on the content, connections, and behaviours of URLs, helping to identify malicious or suspicious activities.

Key Features:

- Real-time website scanning and analysis.
- Detailed reports on website content, connections, and scripts.
- Visualization of network requests and external links.
- API access for integration with other security tools.

Notable Content/Services: URLScan.io is widely used by cybersecurity professionals for threat hunting, incident response, and research purposes.

Cost: Free tier available; subscription plans for advanced features and higher usage limits.

19. Learning Platforms

19.1 Cybersecurity Education and Training

CYBER THREAT INTELLIGENCE 101 (arcX) (arcx.io/courses/cyber-threat-intelligence-101)

Description: CYBER THREAT INTELLIGENCE 101 by arcX is an introductory course that provides foundational knowledge in cyber threat intelligence. It covers essential concepts, methodologies, and tools used in the field of threat intelligence.

Key Features:

- Comprehensive introduction to cyber threat intelligence.
- Interactive modules and video lectures.
- Practical exercises and case studies.
- Certification upon completion.

Notable Content/Services: The course is designed for beginners and professionals looking to enhance their understanding of threat intelligence.

Cost: Subscription-based access; pricing details available on the website.

Betrayal (Kase Scenarios) (kasescenarios.com/betrayal)

Description: Betrayal by Kase Scenarios is an interactive learning platform that offers realistic cybersecurity scenarios to train individuals in handling security incidents. It focuses on improving decision-making and response skills in simulated environments.

Key Features:

- Realistic cybersecurity scenarios and simulations.
- Interactive and immersive training environment.
- Focus on decision-making and incident response.
- Feedback and performance analysis.

Notable Content/Services: Betrayal provides a hands-on learning experience, helping users develop practical skills in managing and responding to cybersecurity incidents.

Cost: Subscription-based access; pricing details available on the website.