Sources

Select all sources

Becoming a Cybersecurity Threat Hunter: A Career Guide

Cybersecurity Mastery: Complete Course in a Single Video | Cybersecurity For Beginners

Every Cybersecurity Job Explained!

Types of cybersecurity - Article | SailPoint

Working in Cybersecurity: A Day in the Life

Chat

🛡️

Cybersecurity: Types, Evolution, and Consolidated Architecture

5 sources

The provided texts collectively offer a comprehensive overview of cybersecurity, detailing **various types of cyber threats and defensive strategies**. They discuss the **importance of understanding threat landscapes, attack surfaces, and threat vectors** in protecting digital assets. A significant portion focuses on **Azure's security features**, including identity and access management, network security, data protection, and compliance with regulations like GDPR and ISO 27001. Finally, the sources touch upon **career opportunities in cybersecurity**, emphasizing the dynamic nature of the field and the continuous need for learning and adaptation.

5 sources

Studio

Audio Overview

Video Overview

Mind Map

Reports

NotebookLM can be inaccurate; please double check its responses.

(Saved responses are view only)

The purpose of this project is to apply threat modeling principles to a single critical component, serving as a proactive exercise to "identify and address security threats to your applications". I will systematically identify potential threats using the STRIDE model, then leverage the DREAD model's numerical values to "rank the threats in terms of severity" based on impact and probability. This focused analysis will enable me to propose high-level countermeasures and mitigation strategies. Ultimately, this project demonstrates my analytical rigor and problem-solving skills, contributing to "reducing the attack surface" and proactively strengthening an organization's security posture.

Understood. So, to confirm, you will have approximately **6 hours per week** for your project, totaling **12 hours over the two-week period**. This is a significant reduction from the previously discussed 24 hours, so we'll need to adjust the project scopes to ensure they are realistically achievable within this tighter timeframe.

Given your enjoyment of riddles and problem-solving, aptitude for math and numbers, boxing-driven discipline and persistence, and your skills in Python and cryptography, here are some revised project ideas that you can complete solo within approximately **12 hours (6 hours per week)**:

Project 1 (Revised): Focused Threat Research & Conceptual Detection

This project will allow you to delve deep into an attacker's methodology and conceptualize how you would detect it, leveraging your analytical skills without requiring extensive lab setup.

- **Total Estimated Time**: ~12 hours (6 hours in Week 1, 6 hours in Week 2)
- **What you'd do**:
  - **Week 1: Deep Dive into a MITRE ATT&CK Technique (6 hours)**
    - Choose **one specific, well-documented adversarial technique** from the **MITRE ATT&CK framework**. For example, "T1059.003 - Command and Scripting Interpreter: Windows Command Shell" or "T1003 - OS Credential Dumping". The MITRE ATT&CK framework is a "globally accessible framework which contains a comprehensive knowledge base that cataloges the tactics techniques and procedures used by threat actors" .
    - Thoroughly research this technique: understand its purpose, common tools attackers use for it, and the typical indicators of compromise (IOCs) or behaviors (IOBs) that it leaves behind. Focus on "understanding what normal looks like" and how to spot deviations for this particular technique.
  - **Week 2: Conceptual Detection Strategy & Documentation (6 hours)**
    - Based on your research, outline a conceptual detection strategy for the chosen technique. What specific logs (e.g., Windows Event Logs, Sysmon, network logs) would you need to monitor to catch this activity?
    - What specific events or sequences of events would definitively indicate the chosen TTP? Draft a pseudo-code or a plain-language hunting query (e.g., for a SIEM like Microsoft Sentinel, if you were using it) that would reliably detect this activity.
    - **Deliverable**: A concise report (e.g., 2-3 pages) summarizing your chosen TTP, the expected indicators, and your conceptual detection logic.
- **Why it suits you:** This project is a pure "riddle" and "problem-solving" exercise at a theoretical level, focused on "understanding the different techniques that attackers can use". It directly leverages your "detail-oriented" and "curiosity-driven" mindset and applies knowledge from coursework on threat landscapes and security tools. Your discipline and persistence will aid in the methodical research and analysis.

Project 2 (Revised): Mini-Threat Model for a Single Critical Component

This condensed project will allow you to apply threat modeling principles to a very focused area, demonstrating your analytical and strategic thinking.

- **Total Estimated Time**: ~12 hours (6 hours in Week 1, 6 hours in Week 2)
- **What you'd do**:
  - **Week 1: Component Identification & Decomposition (6 hours)**
    - Choose a **very small, specific component** within a hypothetical system. Examples could include:
      - The authentication module of a simple web application.
      - A single data storage unit (e.g., a specific database table containing sensitive customer data) for a small business.
    - Briefly describe the component's function, its direct inputs, outputs, and any trust boundaries it interacts with.
  - **Week 2: STRIDE-based Threat Identification & High-Level Mitigations (6 hours)**
    - Apply the **STRIDE model** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) to identify potential threats *specifically for that chosen component*.
    - For each identified threat, propose **one or two high-level countermeasures** (e.g., "Implement Multi-Factor Authentication for authentication module" or "Encrypt sensitive data in storage").
    - **Deliverable**: A short document (e.g., 1-2 pages) describing the component, listing the STRIDE-identified threats, and proposing high-level mitigations.
- **Why it suits you:** This is a core "riddle" and "problem-solving" task, focusing on "identifying and addressing security threats to your applications". It requires creative thinking and the methodical application of security frameworks like STRIDE, aligning with your interests and persistence.

Project 3 (Revised): Basic Python Script for Log Keyword Search

This project directly uses your Python skills and aptitude for data, providing a tangible output for your portfolio with a manageable scope.

- **Total Estimated Time**: ~12 hours (6 hours in Week 1, 6 hours in Week 2)
- **What you'd do**:
  - **Week 1: Data Acquisition & Python Setup (6 hours)**
    - Find a **very small, publicly available, simplified log file** (e.g., a few hundred lines of web server access logs, or authentication logs) from a platform like Kaggle.
    - Ensure you have Python installed and any basic libraries (e.g., `re` for regular expressions, or standard `csv` module if applicable to your chosen log format) are ready.
  - **Week 2: Script for Key Information Extraction & Simple Counting (6 hours)**
    - Develop a Python script that:
      - Reads the chosen log file line by line.
      - Searches for a specific keyword or pattern (e.g., "login failed", "error", or a specific IP address).
      - Counts the total occurrences of this keyword/pattern.

        - Prints out each line where the keyword is found and the total count. This leverages your "math or numbers" aptitude.
    - **Deliverable**: A functional Python script and a brief accompanying document (e.g., 1 page) explaining the script's purpose, the log data used, and the findings.
- **Why it suits you:** This directly applies your "Python" skills and "math or numbers" aptitude to a cybersecurity context. It's a tangible piece of code that demonstrates your ability to "manage multiple pieces of evidence and information" and perform initial log analysis, which is foundational for SOC analysts and threat hunters.

These revised projects are more compact and specifically designed to fit your **12-hour total project time**. They provide excellent opportunities to demonstrate key cybersecurity skills and can serve as valuable additions to your portfolio. Remember that consistent, focused effort during your 3-hour sessions will be key to successfully completing these projects within the two-week deadline.

NotebookLM can be inaccurate; please double check its responses.

That's a great question! With the additional source, we can further strengthen the reasoning behind the recommended courses for a Threat Hunter and highlight how they align with the real-world demands and expert advice in the field. The new source strongly validates the previously suggested curriculum, especially by providing explicit definitions for key cybersecurity concepts and underscoring the importance of continuous learning and adaptability.

To become a **Threat Hunter**, leveraging your enjoyment of riddles and problem-solving, your aptitude for math and numbers, your boxing-driven discipline and persistence, and your new skills in Python and cryptography, a comprehensive set of courses focusing on deep investigation, understanding attacker methodologies, and data analysis would be highly beneficial. Threat hunting involves proactively searching for adversaries within a network, assuming they are already present, rather than waiting for alerts. This requires a deep understanding of "normal" network behavior and the different techniques attackers can use.

While the provided sources don't outline a specific "Threat Hunter" certification path, the **Microsoft Cybersecurity Analyst Professional Certificate** program offers a robust curriculum that aligns directly with the skills and knowledge required for this role.

Here are the courses you would need to complete within that program, with reinforced justifications from all sources:

1. **Introduction to Computers and Operating Systems and Security**
    - **Relevance**: This foundational course introduces how computers work, including hardware, software, and operating systems, and explores the cyber threat landscape and common attack types. Understanding these basics is crucial for a threat hunter to discern "normal" system behavior from anomalies and to recognize various attack patterns. The importance of understanding the threat landscape as "an all-encompassing term that refers to three major areas which are all potential vulnerabilities of an application, the attackers that may be targeting this area, and the attacks that are used" is highlighted.
2. **Introduction to Networking and Cloud Computing**
    - **Relevance**: This course provides a solid understanding of network types, topologies, devices, protocols, and cloud computing concepts. A threat hunter relies heavily on network monitoring, log analysis, and understanding data transmission to identify suspicious activities.

Knowledge of cloud environments, including Azure, is increasingly important for hunting threats in modern infrastructures.

3. **Threat Vectors and Mitigation**
    - **Relevance**: This course directly addresses the "active threat landscape," various attack vectors (such as phishing, malware, zero-day exploits, and Advanced Persistent Threats), and strategies to mitigate them. Crucially, it also introduces **cryptography**, building on your existing knowledge of Caesar's Cipher, which is vital for understanding how attackers might conceal their activities or how data is protected. The new source reinforces the persistence of phishing attacks, including new approaches like QR codes and multi-stage attacks to bypass MFA, as well as the evolution of malware. A threat hunter must deeply understand attacker techniques to proactively search for them.
4. **Cybersecurity Identity and Access Solutions Using Azure AD**
    - **Relevance**: This course focuses on **identity and access management (IAM)**, including authentication methods like multi-factor authentication (MFA) and conditional access. It covers **Azure AD Identity Protection**, which uses machine learning to analyze user behavior and sign-in patterns to detect suspicious activities and compromised accounts. This is highly relevant to threat hunting, as identity-based attacks are a common vector, and detecting deviations from normal user behavior is a core hunting technique. The new source mentions "identity protection" as a core capability in data security.
5. **Microsoft Security Solutions and Microsoft Defender**
    - **Relevance**: This course is exceptionally valuable for a threat hunter. It covers Azure's basic security capabilities, Azure security management, and **Microsoft 365 Defender threat protection**. It specifically delves into **Microsoft Sentinel**, a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution. **Sentinel leverages advanced analytics and machine learning to detect and investigate threats across the entire organization's infrastructure and helps in hunting for suspicious activities at scale by tapping into years of cybersecurity experience at Microsoft**. The new source explicitly defines **SIEM** as solutions that "combine security event data from logs and then apply rules and statistical correlations to identify threats" and **SOAR** as systems that "integrate separate security tools" to "efficiently coordinate and automate repetitive tasks as well as streamline incident and threat response workflows". This strongly validates the centrality of Sentinel in threat hunting. Furthermore, it covers **Microsoft Defender for Endpoint**, which includes "Microsoft threat experts [who] bring deep knowledge and **proactive threat hunting** to your security operations center". Understanding these integrated tools is essential for gathering and analyzing data for threat hunting.
6. **Cybersecurity Tools and Technologies**
    - **Relevance**: This course introduces penetration testing concepts and tools, which helps a threat hunter **think like an adversary** and understand their methods. It also covers the **MITRE ATT&CK framework**, which is an indispensable knowledge base of adversarial tactics, techniques, and common knowledge, explicitly recommended for threat hunters. Your Python skills would be beneficial here for scripting and automating analysis tasks. The importance of understanding how attackers operate is also reinforced by experts who were "fascinated by not only the technology but also the people coming up with all these techniques" and were interested in the "dark side of technology".

7. **Cybersecurity Management and Compliance**
    - **Relevance**: This course covers security planning, disaster recovery, data management, and risk management. While more governance-focused, understanding an organization's risk posture and compliance requirements helps a threat hunter prioritize efforts to protect critical assets and data that are subject to regulations.
8. **Advanced Cybersecurity Concepts and Capstone Project**
    - **Relevance**: This course delves into **threat modeling**, **advanced threats and mitigation** (including IoT and common attacks on infrastructure), and **security-conscious modeling** (threat landscapes, attack surfaces, threat vectors). These are direct and advanced topics critical for a threat hunter to proactively identify and understand complex threats. The Capstone project allows you to integrate all learned knowledge into a practical security mitigation plan, simulating real-world scenarios. The new source highlights that "Traditional cyber attack methods continue to be widely used... These are being joined by evolving versions that take advantage of machine learning (ML) and artificial intelligence (AI) to increase their reach and efficacy".
9. **Microsoft SC-900 Exam Preparation and Practice Course**
    - **Relevance**: This course prepares you for the SC-900 Microsoft Security, Compliance, and Identity Fundamentals exam. While primarily an exam preparation course, earning this certification provides industry-endorsed evidence of your foundational skills and knowledge in security concepts, Microsoft Security Solutions, and identity management, which are all underlying components of a threat hunter's toolkit.

Why these courses suit you as a Threat Hunter, further reinforced by the new source:

- **Riddles and Problem-Solving**: Threat hunting is essentially a complex riddle, requiring you to piece together disparate clues and data points to uncover hidden threats. The investigative nature of many of these courses, particularly those on advanced threats and security tools, aligns perfectly with this interest.
- **Math and Numbers**: Courses involving log analysis, data processing in SIEM tools like Microsoft Sentinel, and understanding attack metrics or scoring (like CVSS mentioned in relation to other roles but a common concept) will leverage your numerical aptitude.
- **Boxing Discipline and Persistence**: Threat hunting is not about "quick wins" and often involves dealing with "uncertainty or obscurity". Your resilience and persistence, even with a "cloudy memory that eventually remembers," are ideal for the long hours of analytical work, research, and troubleshooting required to uncover sophisticated threats. The discipline from boxing translates directly to the sustained focus needed for deep investigations. This is strongly supported by expert advice emphasizing **perseverance and persistence to solve problems** [Security Engineer description in the initial comprehensive overview] and being "addict to information: learning how computer viruses worked... and was fascinated by not only the technology but also the people coming up with all these techniques".
- **Python and Cryptography**: Your Python skills will be invaluable for scripting and automating data analysis, parsing logs, and interacting with security tools, enhancing your efficiency as a threat hunter. Your basic understanding of cryptography will be expanded upon, which is essential for analyzing encrypted communications or understanding how threats might be hidden.

Finally, the new source reinforces the critical importance of **continuous learning** and **adaptability** in cybersecurity. Experts consistently advise "constantly looking for resources of information" through "blogs and videos and podcasts to expand my knowledge base", and the need to "be willing to adapt to change and be willing to always be learning". This emphasizes that formal courses are a strong foundation, but a threat hunter's journey also requires ongoing self-study and engagement with the evolving threat landscape.

(Saved responses are view only)

To become a **Threat Hunter**, leveraging your enjoyment of riddles and problem-solving, your aptitude for math and numbers, your boxing-driven discipline and persistence, and your new skills in Python and cryptography, a comprehensive set of courses focusing on deep investigation, understanding attacker methodologies, and data analysis would be highly beneficial.

While the provided sources don't outline a specific "Threat Hunter" certification path, the **Microsoft Cybersecurity Analyst Professional Certificate** program offers a robust curriculum that aligns directly with the skills and knowledge required for this role. Threat hunting involves proactively searching for adversaries within a network, assuming they are already present, rather than waiting for alerts. This requires a deep understanding of what "normal" network behavior looks like and the different techniques attackers can use.

Here are the courses you would need to complete within that program, and how they would contribute to your goal of becoming a Threat Hunter:

1. **Introduction to Computers and Operating Systems and Security**
    - **Relevance**: This foundational course introduces how computers work, including hardware, software, and operating systems, and explores the cyber threat landscape and common attack types. Understanding these basics is crucial for a threat hunter to discern "normal" system behavior from anomalies and to recognize various attack patterns.
2. **Introduction to Networking and Cloud Computing**
    - **Relevance**: This course provides a solid understanding of network types, topologies, devices, protocols, and cloud computing concepts. A threat hunter relies heavily on network monitoring, log analysis, and understanding data transmission to identify suspicious activities. Knowledge of cloud environments, including Azure, is increasingly important for hunting threats in modern infrastructures.
3. **Threat Vectors and Mitigation**
    - **Relevance**: This course directly addresses the "active threat landscape," various attack vectors (such as phishing, malware, zero-day exploits, and Advanced Persistent Threats), and strategies to mitigate them. Crucially, it also introduces **cryptography**, building on your existing knowledge of Caesar's Cipher, which is vital for understanding how attackers might conceal their activities or how data is protected. A threat hunter must understand attacker techniques to proactively search for them.
4. **Cybersecurity Identity and Access Solutions Using Azure AD**
    - **Relevance**: This course focuses on identity and access management (IAM), including authentication methods like multi-factor authentication (MFA) and conditional access. It covers **Azure AD Identity Protection**, which uses machine learning to analyze user behavior and

sign-in patterns to detect suspicious activities and compromised accounts. This is highly relevant to threat hunting, as identity-based attacks are a common vector, and detecting deviations from normal user behavior is a core hunting technique.

5. **Microsoft Security Solutions and Microsoft Defender**
   - **Relevance**: This course is exceptionally valuable for a threat hunter. It covers Azure's basic security capabilities, Azure security management, and **Microsoft 365 Defender threat protection**. It delves into **Microsoft Sentinel**, a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution, which uses advanced analytics and machine learning to detect and investigate threats across an organization's infrastructure and helps in **hunting for suspicious activities at scale**. Furthermore, it covers **Microsoft Defender for Endpoint**, which includes "Microsoft threat experts [who] bring deep knowledge and **proactive threat hunting** to your security operations center". Understanding these tools is essential for gathering and analyzing data for threat hunting.
6. **Cybersecurity Tools and Technologies**
   - **Relevance**: This course introduces penetration testing concepts and tools, which helps a threat hunter **think like an adversary**and understand their methods. It also covers the **MITRE ATT&CK framework**, which is an indispensable knowledge base of adversarial tactics, techniques, and common knowledge, explicitly recommended for threat hunters. Your Python skills would be beneficial here for scripting and automating analysis tasks.
7. **Cybersecurity Management and Compliance**
   - **Relevance**: This course covers security planning, disaster recovery, data management, and risk management. While more governance-focused, understanding an organization's risk posture and compliance requirements helps a threat hunter prioritize efforts to protect critical assets and data that are subject to regulations.
8. **Advanced Cybersecurity Concepts and Capstone Project**
   - **Relevance**: This course delves into **threat modeling**, **advanced threats and mitigation** (including IoT and common attacks on infrastructure), and **security-conscious modeling** (threat landscapes, attack surfaces, threat vectors). These are direct and advanced topics critical for a threat hunter to proactively identify and understand complex threats. The Capstone project allows you to integrate all learned knowledge into a practical security mitigation plan, simulating real-world scenarios.
9. **Microsoft SC-900 Exam Preparation and Practice Course**
   - **Relevance**: This course prepares you for the SC-900 Microsoft Security, Compliance, and Identity Fundamentals exam. While primarily an exam preparation course, earning this certification provides industry-endorsed evidence of your foundational skills and knowledge in security concepts, Microsoft Security Solutions, and identity management, which are all underlying components of a threat hunter's toolkit.

Why these courses suit you as a Threat Hunter:

- **Riddles and Problem-Solving**: Threat hunting is essentially a complex riddle, requiring you to piece together disparate clues and data points to uncover hidden threats. The investigative nature of many of these courses, particularly those on advanced threats and security tools, aligns perfectly with this interest.

- **Math and Numbers**: Courses involving log analysis, data processing in SIEM tools like Microsoft Sentinel, and understanding attack metrics or scoring (like CVSS mentioned in relation to other roles but a common concept) will leverage your numerical aptitude.
- **Boxing Discipline and Persistence**: Threat hunting is not about "quick wins" and often involves dealing with "uncertainty or obscurity". Your resilience and persistence, even with a "cloudy memory that eventually remembers," are ideal for the long hours of analytical work, research, and troubleshooting required to uncover sophisticated threats. The discipline from boxing translates directly to the sustained focus needed for deep investigations.
- **Python and Caesar's Cipher**: Your Python skills will be invaluable for scripting and automating data analysis, parsing logs, and interacting with security tools, enhancing your efficiency as a threat hunter. Your basic understanding of cryptography will be expanded upon in the "Threat Vectors and Mitigation" course, which is essential for analyzing encrypted communications or understanding how threats might be hidden.

By completing this comprehensive program, you would gain the theoretical knowledge and practical experience with tools and frameworks highly relevant to a Threat Hunter role, positioning you well to pursue this engaging and critical field. Don't forget the advice from professionals to continuously seek information from blogs, videos, and podcasts, and to participate in Capture-the-Flag (CTF) competitions and online challenges to further develop your technical, puzzle-solving, and creative skills.

(Saved responses are view only)

Given your dedication to boxing and training approximately 24 hours per week, it's important to consider how the demands of cybersecurity roles, particularly SOC Analyst and Threat Hunter, would align with such a rigorous schedule.

Here's an assessment based on the sources:

SOC Analyst (Security Operations Center Analyst)

- **Work Schedule and Demands**: The sources explicitly state that working as a SOC Analyst **often involves shift work**, and it requires **sustained focus for long periods of time** and the ability to **work well under pressure** [689, Initial comprehensive overview]. A typical day involves triaging alerts, escalating legitimate threats, and writing shift or handover reports. The schedule can be "flexible" due to the unpredictable nature of security incidents, but this often means being "at the mercy of cybersecurity incidents".
- **Alignment with your traits**: Your boxing background suggests discipline, resilience, and the ability to perform under pressure. Your detail-oriented nature and enjoyment of investigation are also strong fits. However, the requirement for shift work and sustained focus for long, potentially irregular hours could pose a significant challenge in balancing with a 24-hour weekly boxing/training schedule. If your training schedule is highly flexible and can adapt to varied shifts and unexpected incident response, then these aspects might be manageable.

Threat Hunter

- **Work Schedule and Demands**: Threat hunting involves proactively searching for adversaries within a network, rather than waiting for alerts. This role is described as **detail-oriented work** and suitable for someone **driven by curiosity**. It requires understanding "what normal looks like" on a network and the different techniques attackers use. Unlike the SOC Analyst role, the sources do not explicitly mention "shift work" for Threat Hunters. However, it does note that if you "like quick wins and you're not okay dealing with uncertainty or obscurity then maybe you should be looking elsewhere".

- **Alignment with your traits**: Your enjoyment of riddles and problem-solving, along with your persistence (even with a "cloudy memory" that eventually remembers), aligns well with the investigative and detail-oriented nature of threat hunting. The discipline and strategic thinking from boxing would also be highly beneficial for proactively anticipating and uncovering hidden threats. Since shift work is not explicitly mentioned as a core component, this role *might* offer more predictable hours compared to a SOC Analyst, potentially making it easier to integrate with your training schedule, provided you can maintain the high level of mental engagement and sustained focus required for deep analysis.

Conclusion

Both roles demand **high levels of sustained focus and attention to detail**. The primary difference that impacts your extensive training schedule is the **shift work** often associated with a SOC Analyst position.

- If your boxing/training schedule can accommodate **flexible or irregular shifts**, a **SOC Analyst** role might still be suitable, leveraging your ability to work under pressure and your detail-oriented approach.
- A **Threat Hunter** role, while equally demanding in terms of focus and detail, **might be a better fit if it offers more consistent, non-shift-based hours**, allowing you to better plan around your 24 hours of weekly training. This role would strongly leverage your problem-solving skills, persistence, and strategic mindset.

Ultimately, your capacity to manage mental and physical energy, and the flexibility of both your training and potential work schedule, would be key determinants.

- **Data Analysis**: The ability to process and analyze large datasets is crucial in roles like **SOC Analyst** and **Threat Hunter**, where you're sifting through logs and network traffic for anomalies. Python's libraries make it a powerful tool for this.
- **SOC Analyst (Security Operations Center Analyst)** SOC analysts are responsible for detecting and responding to threats, which includes **triaging alerts** and investigating security incidents. This role is ideal if you are **detail-oriented** and enjoy understanding various protocols and technologies. SOC analysts may also be involved in deploying sensors or **writing rules to pass logs into a central system**, requiring the analysis of numerical or categorical log data to identify patterns.
- **Threat Hunter** As a threat hunter, you proactively search for adversaries believed to be already inside the network, rather than waiting for alerts. This requires a deep understanding of what "normal" network behavior looks like, to then **detect deviations or anomalies** that could indicate an intrusion. This role is driven by curiosity and a detail-oriented approach to recognizing patterns, often involving statistical analysis of network data.