Detection, Analysis & Pivoting

Instructor: Thomas “Blue” Blauvelt

So What?

- "No plan of operations extends with certainty beyond the first encounter with the enemy's main strength"
  - Prussian Field Marshal Helmuth von Moltke the Elder
- Using detection (tools/analysis) with data will provide results, and you must be prepared to handle the outcomes
- This lesson will provide a science to survive contact with the enemy and how to use information to move forward

"You need some foundation of science literacy so you can inoculate yourself against those who would exploit your absence of knowledge of how the science works for their own gain... the only point of the scientific method is to make sure you are not fooled into thinking something is true that is not or thinking that something is not true, that is.
- Neil deGrasse Tyson

Academic Objectives

- Define detection
- Define True/False Positive/Negative
- List the goals and categories of high-quality data
- Discuss the factors when developing a collection strategy
- List the products and steps in the detection phase
- Define the 8 analysis methods
- List the 4 stages of the incident response process
- List the key data in a security incident case
- List the suggested workflow steps for case management

Overview

- Detection
  - Collection
  - Identification
  - Classification
- Analysis
- Pivoting

Compromise Assessment Timeline

Detection

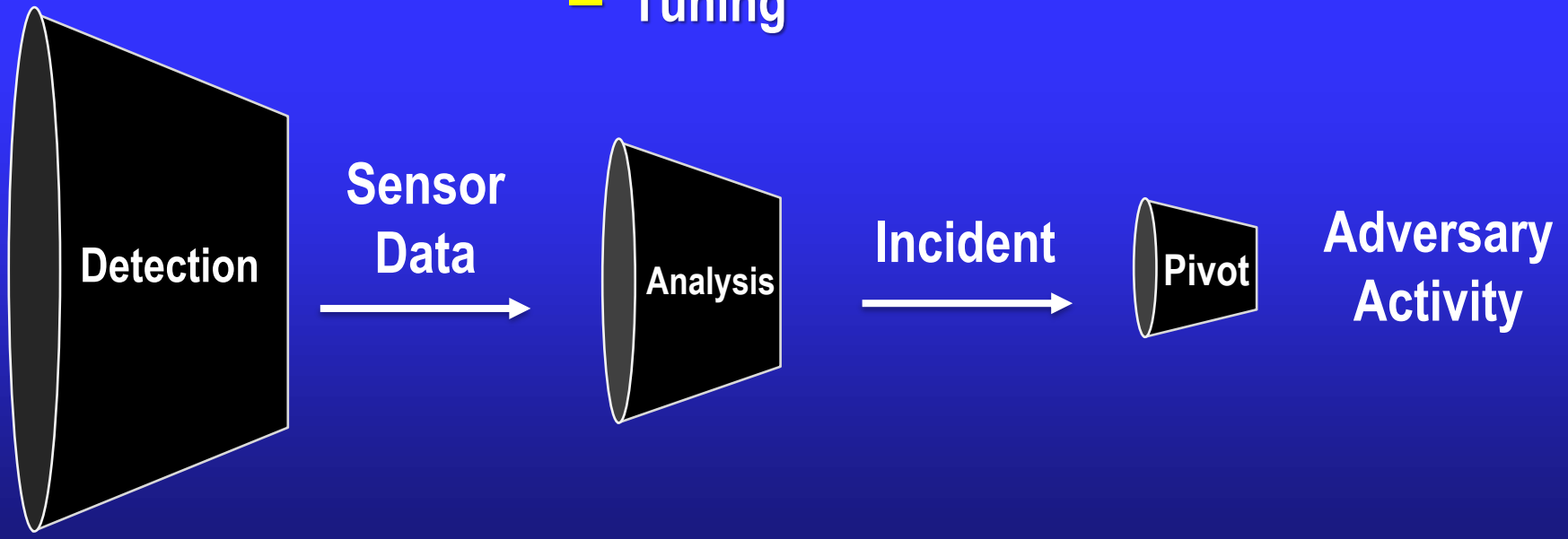
- Sensor Driven
- Automated
- Large amount of FP

Analysis

- Analyst Driven
- Semi-automated/ Playbooks
- Tuning

Pivot

- Adversary/ Hypothesis Driven
- Manual

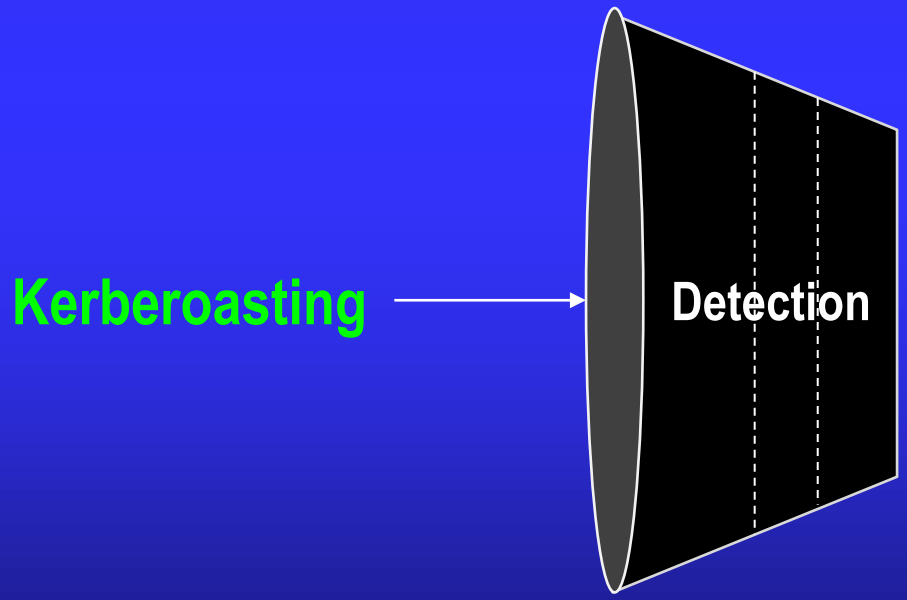


Detection

- Process of identifying security related incidents
- Tool/Sensor: Software or hardware component used for identifying, detecting, protecting, responding and recovering from security threats

Detection

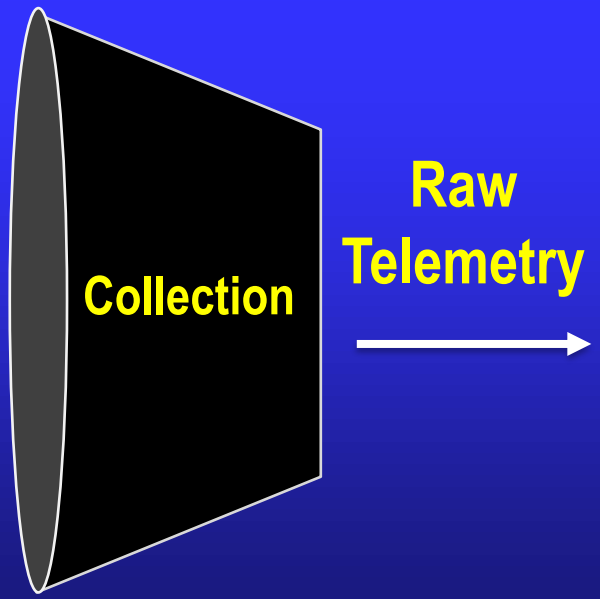
- Collection
- Identification
- Classification



Detection Timeline

Collection

- Sensor Based
- Automated
- Large amount of FP



TP/TN/FP/FN

- True Positive – Identified security related event
- True Negative – Un-identified non-security related event
- False Positive – Identified non-security related event
- False Negative – Un-identified security related event
- Guilty vs. Not Guilty
- FP $\propto$ 1/FN

Tools/Sensors Categories

- Host
  - EDR
  - HIDS
  - SIEM
  - Vuln Scanner
  - Firewalls
  - Forensics
- Network
  - NIDS
  - SIEM
  - Vuln Scanner
  - NIPS
  - Forensics
- Memory
  - SIEM*
  - Forensics
- APT
  - TIPs

Data Quality in Collection

- Goals
  - Reduce time engaging alerts
  - Improve consistency across data sources
  - Enhance automation workflows
- Categories
  - Accuracy
  - Completeness
  - Consistency
  - Timeliness
  - Uniqueness
  - Validity

Collection Strategy

- Collection strategy is tied to collecting relevant data to detect and respond to threats
- The tools and sensors used shape the strategy
- The threats and vulnerable assets focus the strategy
- Leveraging coverage and “analyst units” are key to developing a strategy

Building a Detection

- Credential Access via Kerberoasting
  - Requires TGT
  - Sends TGS-REQ for an account with an SPN with a Kerberos encryption type
  - DC creates a service ticket with the hash of the account requested
  - Attacker extracts encrypted service ticket from the TGS-REP and cracks password offline

Building a Detection

- Collect
  - TGS-REQ requests (Kerberos Service Ticket requests)
    - Windows Event ID 4769
  - All “service”/administrative level accounts with SPN assigned
    - PowerShell, WMIC, LDAP, etc.
  - DC creates a service ticket and replies with TGS-REP
    - Network data

Building a Detection

- Created a hypothesis to identify malicious activity
- Collected data sources to identify the activity
- …now to mark one eye

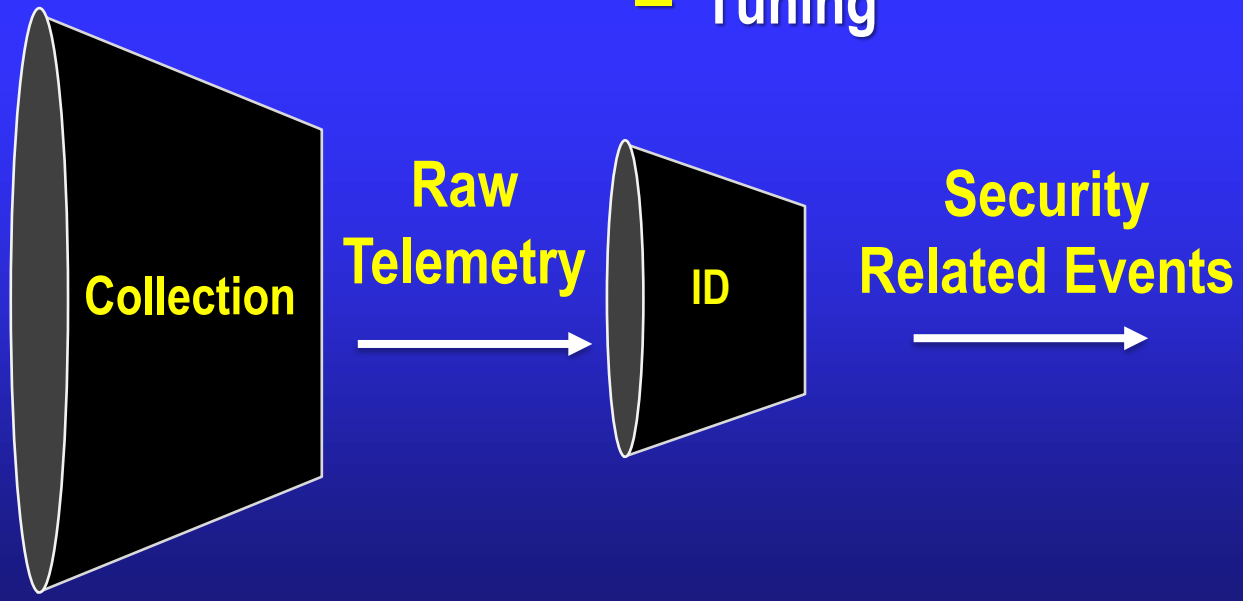
Detection Timeline

Collection

- Sensor Based
- Automated
- Large amount of FP

Identification

- Alert/Definition Based
- Semi-automated
- Tuning

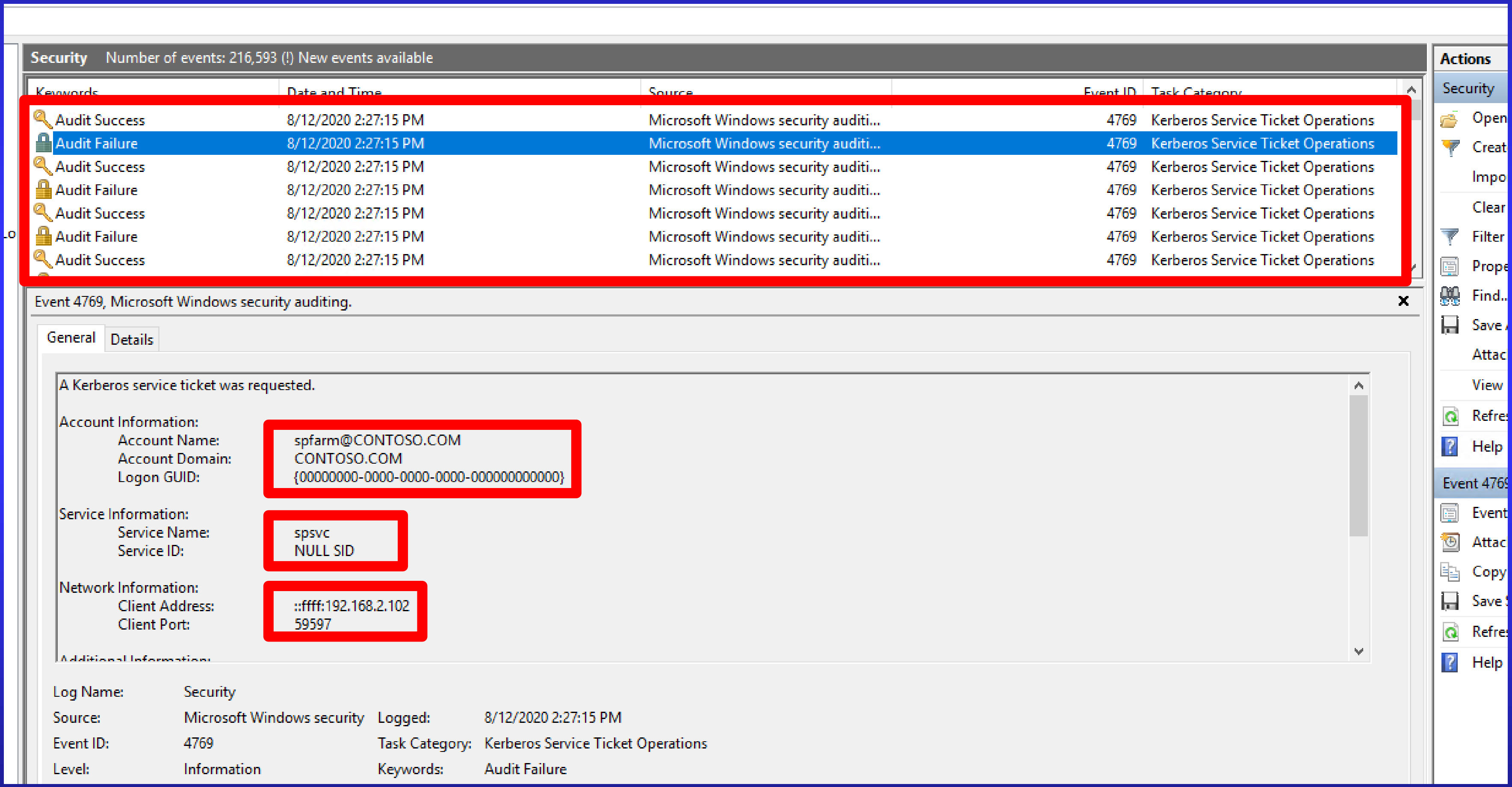


Building a Detection

- Identify
  - All service tickets requested
  - Accounts that are requesting service tickets
  - Accounts that are being requested as service tickets
  - Devices that are requesting service tickets
  - The encryption type used to transmit the service ticket

This is a significant process to identify all the data sources in any given technique. You'll learn about the ADS framework a bit more in the next lesson which will provide techniques for deciding which data source is the most efficient.

Is This Malicious?



Detection Timeline

Collection

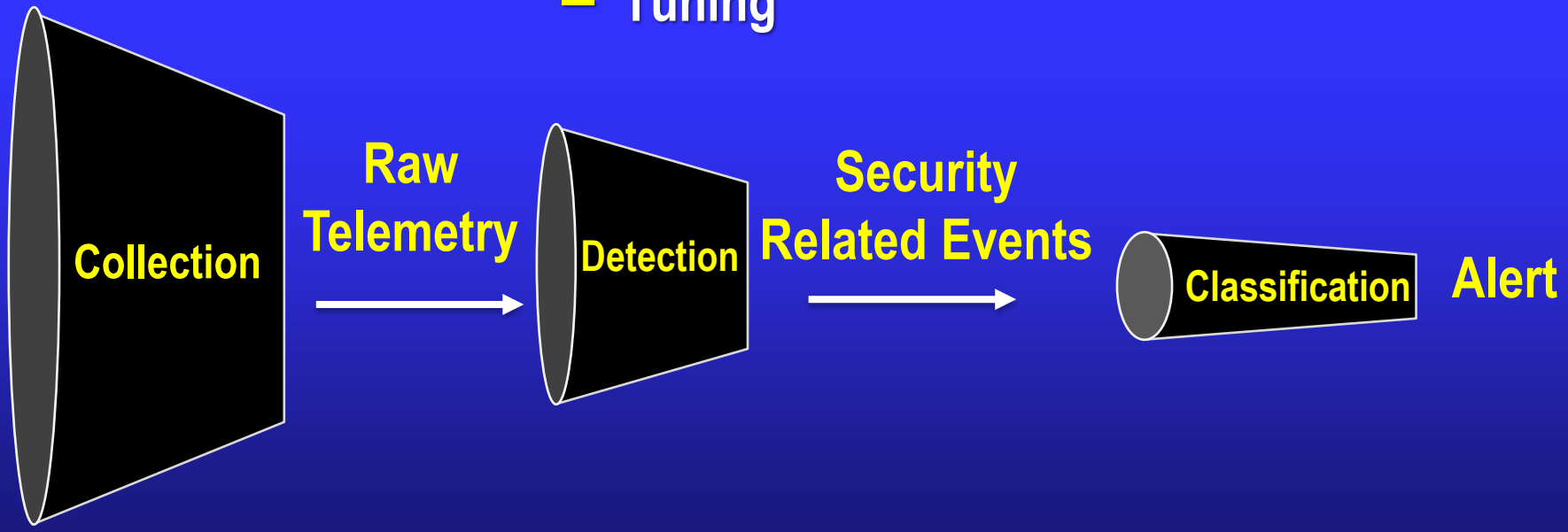
- Sensor Based
- Automated
- Large amount of FP

Detection

- Alert/Definition Based
- Semi-automated
- Tuning

Classification

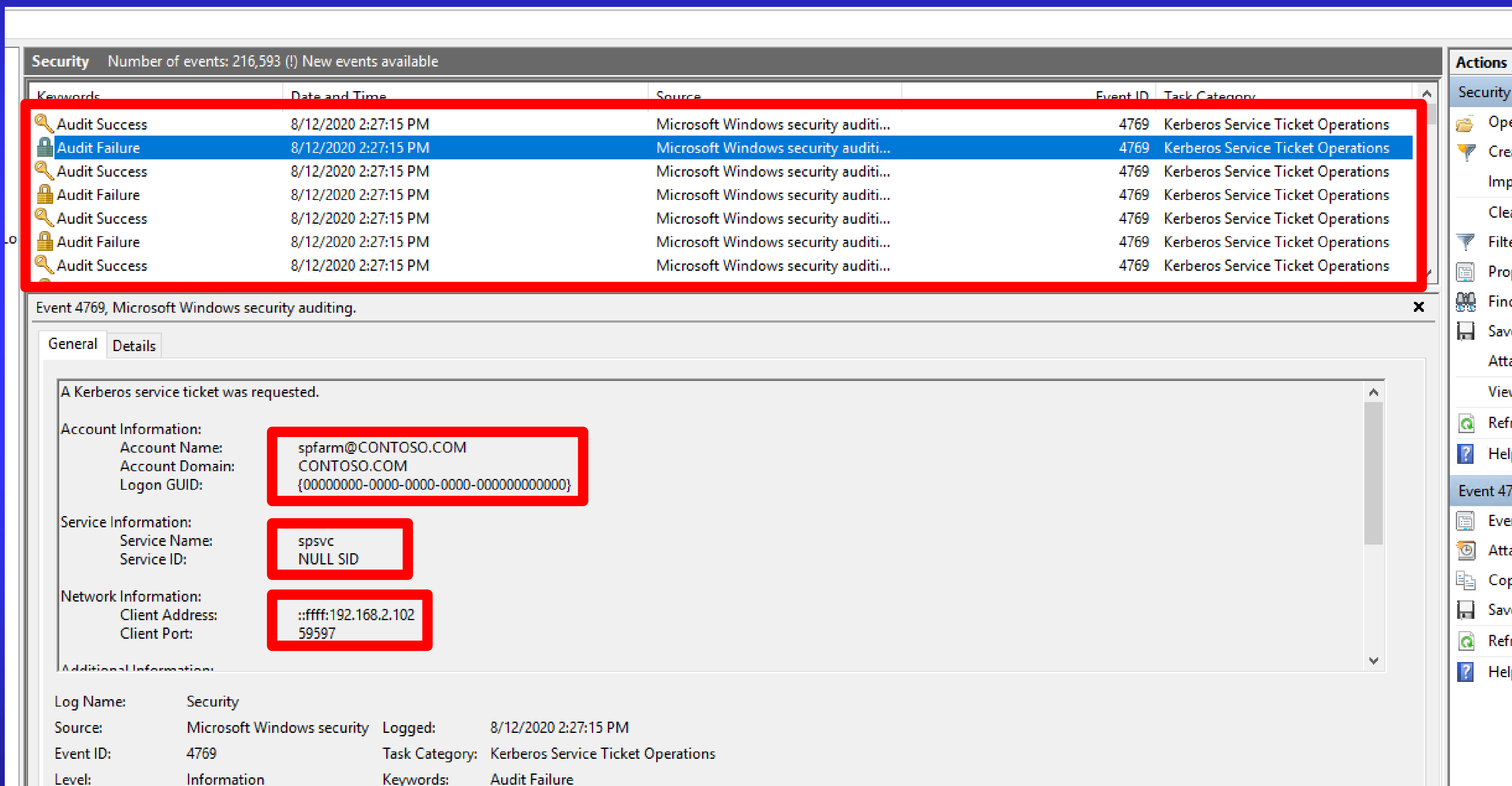
- Criteria Based
- Semi-automated



Building a Detection

- Classify
  - All service tickets requested from *compromised account*
  - All service tickets requested from *compromised device*
  - All service tickets requested with RC4 encryption

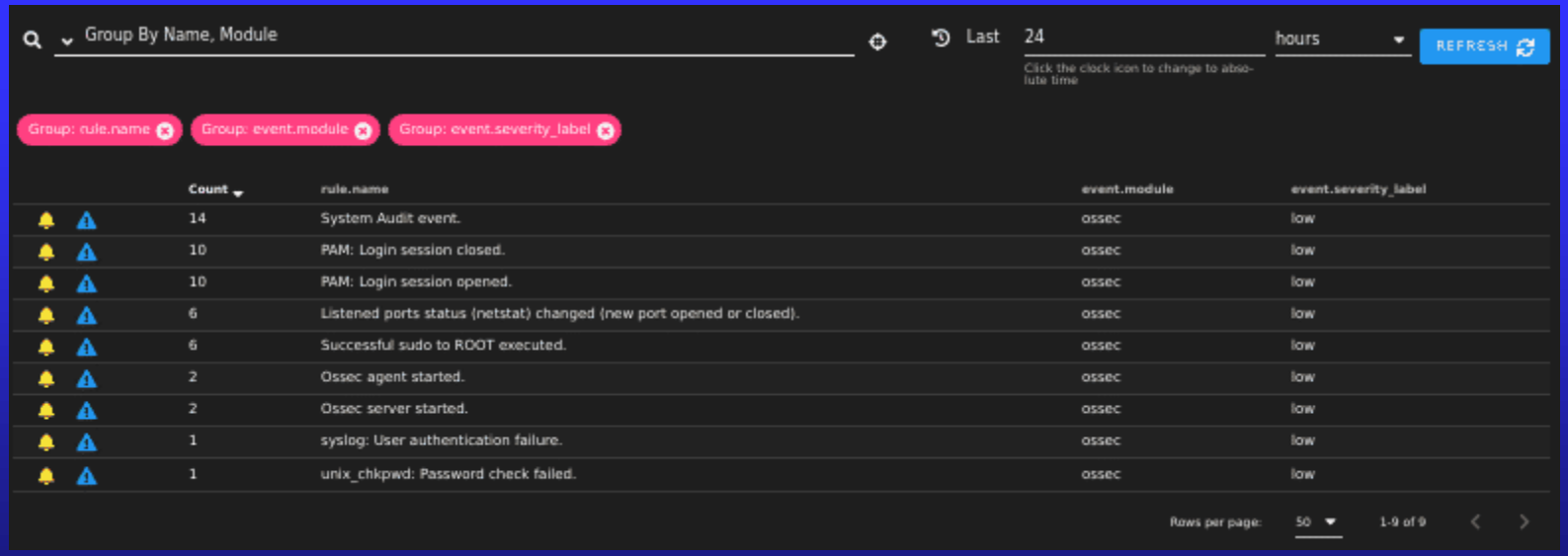
Is This Malicious?



*spfarm & sppvc are default SharePoint accounts and AES256 is used

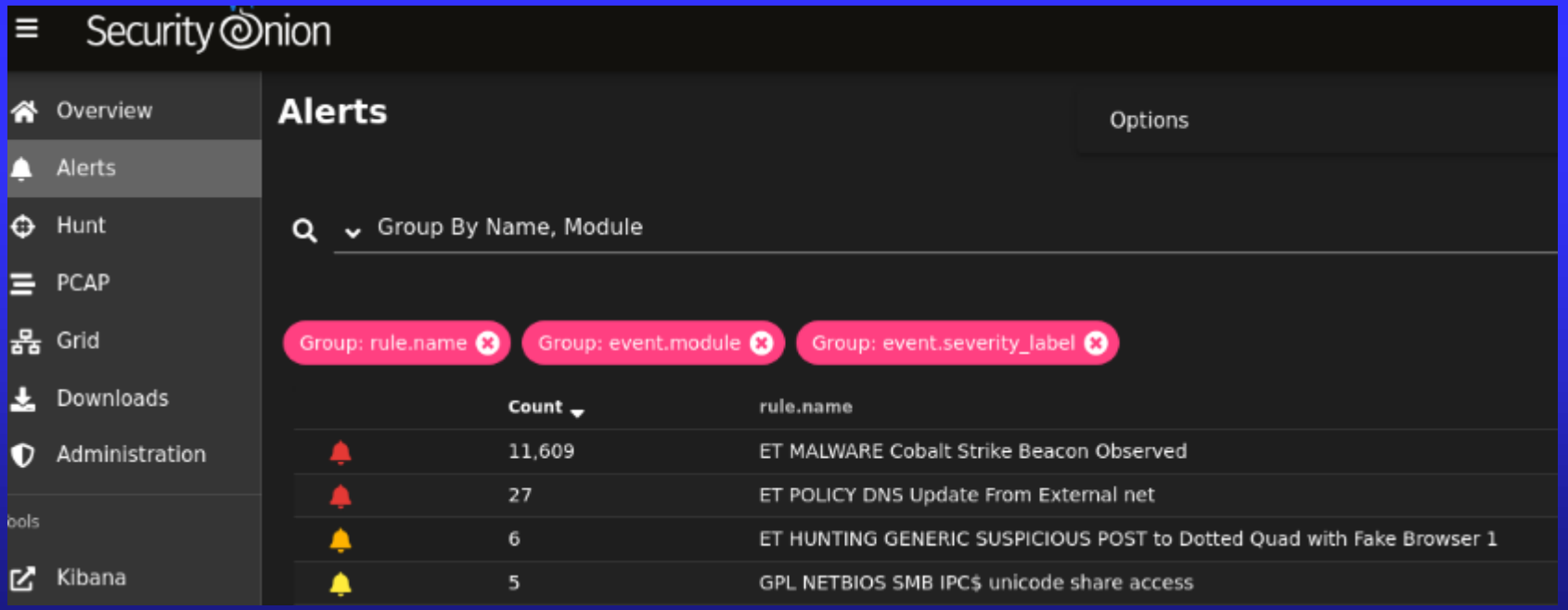
Alerts

- Alerts are an identified detection, with an associated classification
- Alert/Not-Alert/High/Medium/Low buckets
- Signal to Noise Ratio



Execute a Plan

- Ambiguous vs Unambiguous in hunting
- Confidence levels in reporting



Query/Filter

- Alerts are a specific telemetry meeting a condition
- Queries/Filters are essentially the same thing, but in practice used differently
- Queries/Filters bridge the gap between detection and analysis
- Can you think of any queries you would use to detect Kerberoasting that wouldn't meet the criteria of an alert?

Overview

- Detection
- Analysis
  - Analysis methods
  - Detection vs. Analysis
- Pivoting

Analysis Methods

- Temporal
- Causal
- Frequency
- Correlation
- Cluster
- Anomaly
- User and Entity Behavior Analytics (UEBA)
- Kill Chain

Temporal Analysis

- A method of problem-solving that involves examining data over time to detect trends.
- Requirements:
  - Access to historical data logs
  - Tools for time-series analysis
  - Ability to normalize data for time-based comparison
- Examples:
  - Identifying patterns in user logon activity
  - Detecting an increase in external traffic to sensitive devices at unusual hours

Causal Analysis

- A method of problem-solving that involves identifying cause and effect relationships
- Requirements:
  - Detailed cases, incident reports or logs
  - Expertise in systems and network architecture
- Examples:
  - Tracing the source of initial access to a phishing email
  - Linking system failure to malware executing

Frequency Analysis

- A method of studying how often certain events occur to identify patterns or anomalies
- Requirements:
  - Access to historical data logs
  - Statistical tools to display frequency distribution
- Examples:
  - Identifying a spike in failed login attempts indicating a brute force attack
  - Observing frequent access to rarely used ports

Correlation Analysis

- A statistical technique used to determine the interdependence or statistical relationship between two or more variables or datasets
- Requirements:
  - Datasets from multiple tools, sources, and organizations (IDS, OS logs, firewalls)
  - Statistical tools to display correlation
- Examples:
  - Correlating increases in data exfiltration attempts with employee exit dates
  - Correlating software update lapses and malware infections

Cluster Analysis

- A method of grouping a set of objects in such a way that objects in the same group (called a cluster) are more similar to each other than to those in other groups
- Requirements:
  - Large dataset for meaningful clustering
  - Expertise in identifying relevant data features
- Examples:
  - Grouping network traffic by type and origin to identify anomalous activities
  - *Clustering user behavior to identify potential insider threats*

Anomaly Analysis

- A technique used to identify unusual patterns that do not conform to expected behavior
- Requirements:
  - Baseline data to define “normal” behavior
  - Analytical tools for pattern recognition
- Examples:
  - Detecting surge in network traffic from a device hosting a database
  - Detecting unusual login times or locations for sensitive accounts

UEBA Analysis

- A technique using defined user behavior to identify security threats
- Requirements:
  - Detailed logs of user activities and behaviors
  - *UEBA software with machine learning capabilities*
- Examples:
  - Identifying a user accessing files irrelevant to their role

Kill Chain Analysis

- A technique using the phases of a cyber attack to predict previous or future activity
- Requirements:
  - Understanding of the Cyber Kill Chain framework (MITRE/LM)
  - Detailed incident data and threat intelligence
- Examples:
  - Analyzing a ransomware attack to identify the delivery method and exploited vulnerability
  - Identifying an initial access method via phishing from malware execution

Overview

- Detection
- Analysis
- Pivoting
  - Incident Response
  - Case Management (theory)

Pivoting (Threat Hunting)

- The Hypothesized Red Scheme of Manuever (HRSoM) validity and update process
- The role of ambiguous and unambiguous signals in investigations
- Transitioning from identifying activities to a comprehensive RSoM
- Using data gathered from Detection/Analysis to investigate and respond to incidents

Incident Response Process

- Preparation *(outside of scope)*
- Detection/Analysis
- Eradication
- Recovery

- Defined by NIST 800-61

Detection

- The detection process is cyclical as information is uncovered
- Indicators of Incident for Kerberoasting:
  - Abnormal service ticket requests
  - Unusual spikes in TGS requests

Eradication

- Steps for removing the effects of the incident
- Importance of identifying and mitigating vulnerabilities that caused the incident
- Eradicate Kerberoasting:
  - Isolating affected systems
  - Resetting compromised accounts
  - Patching any application related vulnerabilities
  - Updating Kerberos configurations

Recovery

- Process for restoring systems and services
- Monitoring for signs of incident recurrence
- Recovery from Kerberoasting:
  - Monitoring for future attacks/updating detections
  - Reinstating network access to devices/accounts

Investigation Planning

- Do you use previous information to continue an investigation?
- Focused on considerations for students to make decisions
- Tactical Pause
- Revising HRSoM

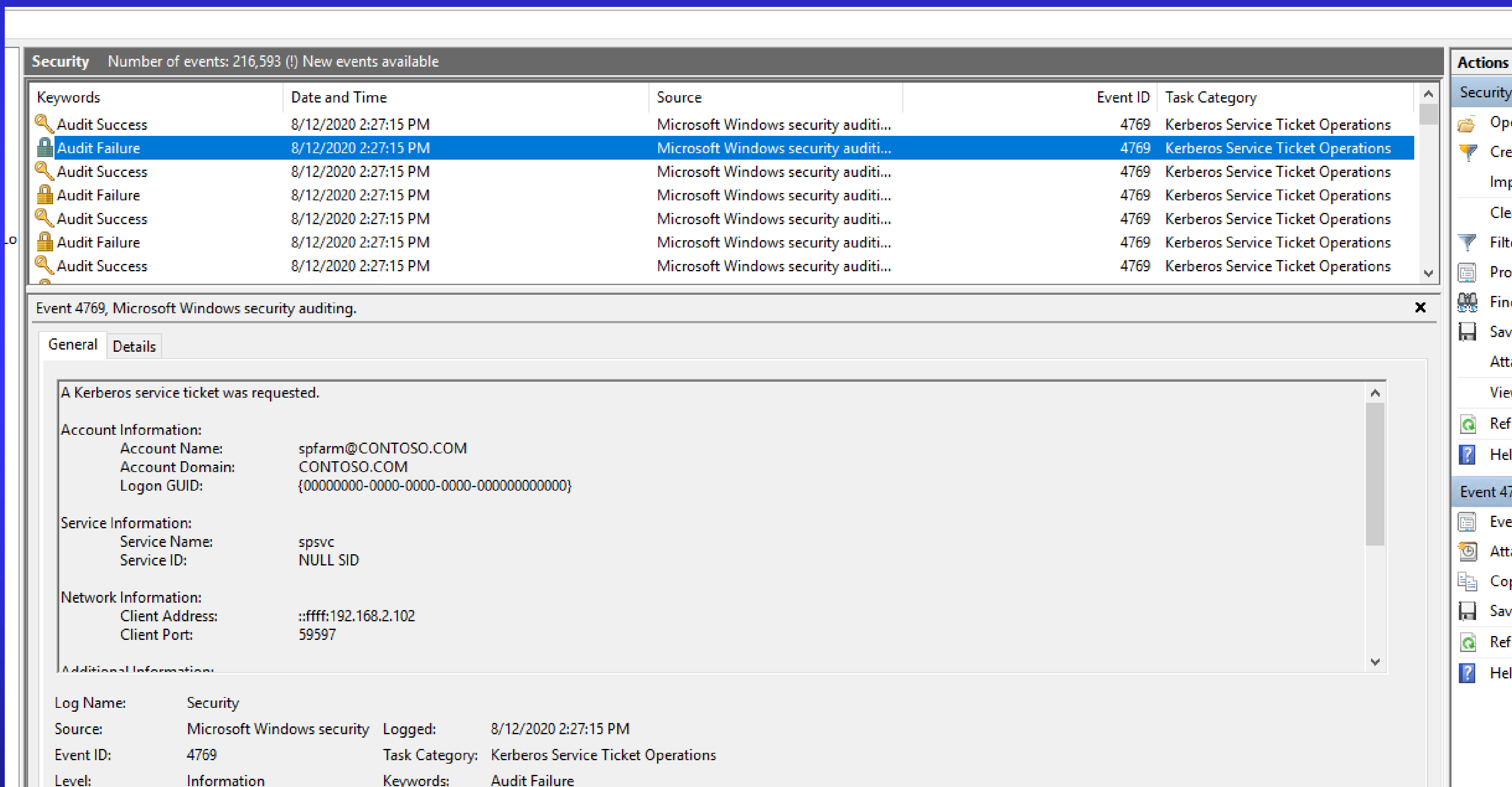
Anatomy of a Case

- Key Data
  - Incident identification data: time/date, categorization, detection method
  - Incident description: summary of incident, assets/systems, potential impact
  - Evidence and artifacts: logs, network captures, screenshots, emails, etc.
  - Response actions: steps taken to contain, eradicate, and recover
  - Communications: external communications related to the incident

Anatomy of a Case

- Suggested Workflow
  - **Initial Assessment**: Determine severity and scope
  - **Assignment and Tracking**: Assign the case to appropriate team members and track progress
  - **Evidence Collection**: Gather evidence and document findings
  - **Response Coordination**: Coordinate containment, eradication and recovery actions
  - **Reporting and Documentation**: Continuously update with new findings, actions and resolutions
  - **Review and Closure**: Final review of the case to ensure completeness followed by closure

Build a Case


Security
Number of events: 216,593 (!) New events available
Keywords
Date and Time
Source
Event ID
Task Category
Audit Success 8/12/2020 2:27:15 PM Microsoft Windows security auditi... 4769 Kerberos Service Ticket Operations
Audit Failure 8/12/2020 2:27:15 PM Microsoft Windows security auditi... 4769 Kerberos Service Ticket Operations
Audit Success 8/12/2020 2:27:15 PM Microsoft Windows security auditi... 4769 Kerberos Service Ticket Operations
Audit Failure 8/12/2020 2:27:15 PM Microsoft Windows security auditi... 4769 Kerberos Service Ticket Operations
Audit Success 8/12/2020 2:27:15 PM Microsoft Windows security auditi... 4769 Kerberos Service Ticket Operations
Audit Failure 8/12/2020 2:27:15 PM Microsoft Windows security auditi... 4769 Kerberos Service Ticket Operations
Audit Success 8/12/2020 2:27:15 PM Microsoft Windows security auditi... 4769 Kerberos Service Ticket Operations
Event 4769, Microsoft Windows security auditing.
General
Details
A Kerberos service ticket was requested.
Account Information:
Account Name: spfarm@CONTOSO.COM
Account Domain: CONTOSO.COM
Logon GUID: {00000000-0000-0000-0000-000000000000}
Service Information:
Service Name: spsvc
Service ID: NULL SID
Network Information:
Client Address: ::ffff:192.168.2.102
Client Port: 59597
Log Name: Security
Source: Microsoft Windows security
Logged: 8/12/2020 2:27:15 PM
Event ID: 4769
Task Category: Kerberos Service Ticket Operations
Level: Information
Keywords: Audit Failure
Actions
Security
Open
Creat
Impo
Clear
Filter
Prope
Find...
Save
Attac
View
Refre
Help
Event 4769
Event
Attac
Copy
Save
Refre
Help

Build a Case

- Case Title: Suspected Kerberoasting Attempt
- Key Data from the Event Log:
  - Date and Time: 8/12/2020 2:27:15 PM
  - Source: Microsoft Windows security auditing.
  - Event ID: 4769
  - Task Category: Kerberos Service Ticket Operations
  - Account Information:
    - Account Name: spfarm@CONTOSO.COM
    - Account Domain: CONTOSO.COM
    - Service Information:
    - Service Name: spsvc
    - Service ID: NULL SID
  - Network Information:
    - Client Address: ::ffff:192.168.2.102
    - Client Port: 59597
    - Keywords: Audit Failure

Build a Case

- Initial Assessment:
  - Review the log entry to confirm the abnormality.
  - Note the audit failure indicating a possible compromised service account or abnormal service ticket request.
- Assignment and Tracking:
  - Assign the incident to a security analyst for investigation.
  - Track the incident in the incident management system with a unique identifier.

Build a Case

- Evidence Collection and Analysis:
  - Collect relevant logs around the time frame of the detected event.
  - Analyze the service ticket requests from the account "spfarm" to determine if there was an unusual volume or pattern indicating Kerberoasting.
- Response Coordination:
  - If Kerberoasting is confirmed, implement immediate containment measures such as disabling the suspected account or changing its credentials.
  - Coordinate with the network team to monitor traffic from the client address associated with the suspicious activity.

Build a Case

- Reporting and Documentation:
  - Document all findings and actions taken in response to the suspected Kerberoasting attempt.
  - Ensure all evidence is preserved in a forensically sound manner.
- Review and Closure:
  - Once the threat is neutralized, and systems are secure, review the case details to confirm that all aspects of the incident have been addressed.
  - Conduct a post-incident review to update procedures and policies as necessary to prevent similar incidents.

Overview

- Detection
  - Collection
  - Identification
  - Classification
- Analysis
  - Analysis methods
  - Detection vs. Analysis
- Pivoting
  - Incident Response
  - Case Management (theory)

Academic Objectives

- Define detection
- Define True/False Positive/Negative
- List the goals and categories of high-quality data
- Discuss the factors when developing a collection strategy
- List the products and steps in the detection phase
- Define the 8 analysis methods
- List the 4 stages of the incident response process

Questions?

- Instructor's name: Thomas "Blue" Blauvelt
- Instructor's e-mail: tcblauvelt@gmail.com

References

- *Department of Defense Dictionary of Military and Associated Terms,* Jan 19
- http://ndupress.ndu.edu/Media/News/NewsArticleView/ tabid/7849/Article/607722/jfq-78-three-approaches-to-center-of-gravity-analysis-the-islamic-state-of-iraq.aspx
- https://www.youtube.com/watch?v=zKFiYStExK4
- http://usacac.army.mil/CAC2/Repository/Planning-for-Action-Kem-August-2012.pdf
- Joint Publication 2-0, *Joint Intelligence*, 22 Oct 13
- Joint Publication 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, 21 May 14
- Joint Publication 5-0, *Joint Planning*, 16 Jun 17
- JOPPA Handbook for Air, 4 Nov 16
- Marine Corps Doctrinal Publication 1, *Warfighting*, 20 Jun 97

Detection, Analysis & Pivoting

Instructor: Thomas “Blue” Blauvelt