Introduction to Log Analysis

- Course Incharge: Yahya Batla
- Course Instructor: Umar Bilal

WHAT IS A LOG

In computing, a log is a record of events, actions, or transactions that occur within a system, application, or network. Logs provide a chronological history of activities and serve various purposes, including troubleshooting, auditing, security monitoring, and performance analysis.

```
The system time was changed.

Subject:
  Security ID: LB\administrator
  Account Name: administrator
  Account Domain: LB
  Logon ID: 0x3DE02

Process Information:
  Process ID: 0x1034
  Name: C:\Windows\System32\rundll32.exe

Previous Time: 2013-10-14T14:14:35.026274800Z
New Time: 2013-10-14T14:14:35.000000000Z
```

```
"A user account was unlocked.

Subject:
        Security ID:            S-1-5-21-4088076005
        Account Name:
        Account Domain:         SIT
        Logon ID:               0x16138C00

Target Account:
        Security ID:            S-1-5-21-4088076005-3353233225-
        Account Name:           lar
        Account Domain:         SIT"
```

WHAT INFORMATION DOES A LOG CONTAIN?

Logs typically contain a variety of information depending on the type of log and the specific event or activity being recorded. However, some common elements found in most logs include:

Timestamp: The date and time when the event occurred. This helps in establishing a chronological sequence of events.

Event Type/Severity Level: Indicates the nature or severity of the event, such as informational, warning, error, or critical.

Event Source/Component: Identifies the source or component within the system or application that generated the event. It could be the name of an application, system process, or device.

Outcome/Result: Indicates the outcome or result of the event, such as success, failure, completion, or termination.

IP Address/Host: Specifies the IP address, hostname, or network identifier associated with the event, especially relevant for network-related events.

Event Description/Message: Provides a brief description or message explaining the event, including relevant details such as error codes, status messages, or actions taken.

User/Actor: Specifies the user or entity associated with the event, such as a username, user ID, or system service account.

Resource/Target: Identifies the resource, object, or system component affected by the event, such as a file, database record, network device, or application module.

Session/Transaction ID: Provides a unique identifier for the session or transaction associated with the event, facilitating correlation and tracking across multiple logs.

Additional Contextual Data: May include additional contextual information relevant to the event, such as location, device type, operating system, browser version, or error stack trace.

TYPES OF LOG

- System Logs
- Security Logs
- Application Logs
- Database Logs
- Network Logs

SYSTEM LOG

System logs track the operation of the operating system and hardware components. They include information about system startups, shutdowns,and hardware issues.

Example:

```
System audit policy was changed.

Subject:

   Security ID:  S-1-5-21-3108364787-189202583-342365621-500
   Account Name:  Administrator
   Account Domain:  WIN-R9H529RIO4Y
   Logon ID:  0x169e9

Audit Policy Change:

   Category:  Logon/Logoff
   Subcategory:  Special Logon
   Subcategory GUID: {0CCE921B-69AE-11D9-BED3-505054503030}
   Changes:  Failure added
```

Security LOGS

Security logs focus on recording security related events, such as login attempts, account changes, and other activities that may pose a security risk.

Example:

```
Special privileges assigned to new logon.

Subject:

     Security ID:  WIN-R9H529RIO4Y\Administrator
     Account Name:  Administrator
     Account Domain:  WIN-R9H529RIO4Y
     Logon ID:  0x4b842

Privileges:

     SeSecurityPrivilege
     SeTakeOwnershipPrivilege
     SeLoadDriverPrivilege
     SeBackupPrivilege
     SeRestorePrivilege
     SeDebugPrivilege
     SeSystemEnvironmentPrivilege
     SeImpersonatePrivilege
```

Application LOGS

Application logs track events and errors related to specific software applications. These logs can help developers and administrators identify issues within an application.

Example:

[2024-02-09T12:34:56.789Z] ERROR: Failed to process order
Order ID: 5678
Error: Insufficient inventory for product 'ABC123'

Database LOGS

Database logs are chronological records of changes made to a database. These logs capture various activities such as insertions, updates, and deletions of data, as well as structural changes like creating or dropping tables or indexes.

Example:

```
2024-02-09T12:34:56.789Z [INFO] Query executed: SELECT *
FROM users WHERE user_id = '1234'
```

Network LOGS

Network logs track communication activities within a network, including network traffic, firewall events, DNS requests, and network device configurations.

Example:

[2024-02-09T12:34:56.789Z] Flow Analysis: TCP connection established
Source IP: 192.168.1.200
Destination IP: 203.0.113.50
Source Port: 12345
Destination Port: 80
Bytes Sent: 1234
Bytes Received: 5678

Practice:

https://tryhackme.com/room/introtologs

Students are advised to complete this room from thier own THM account

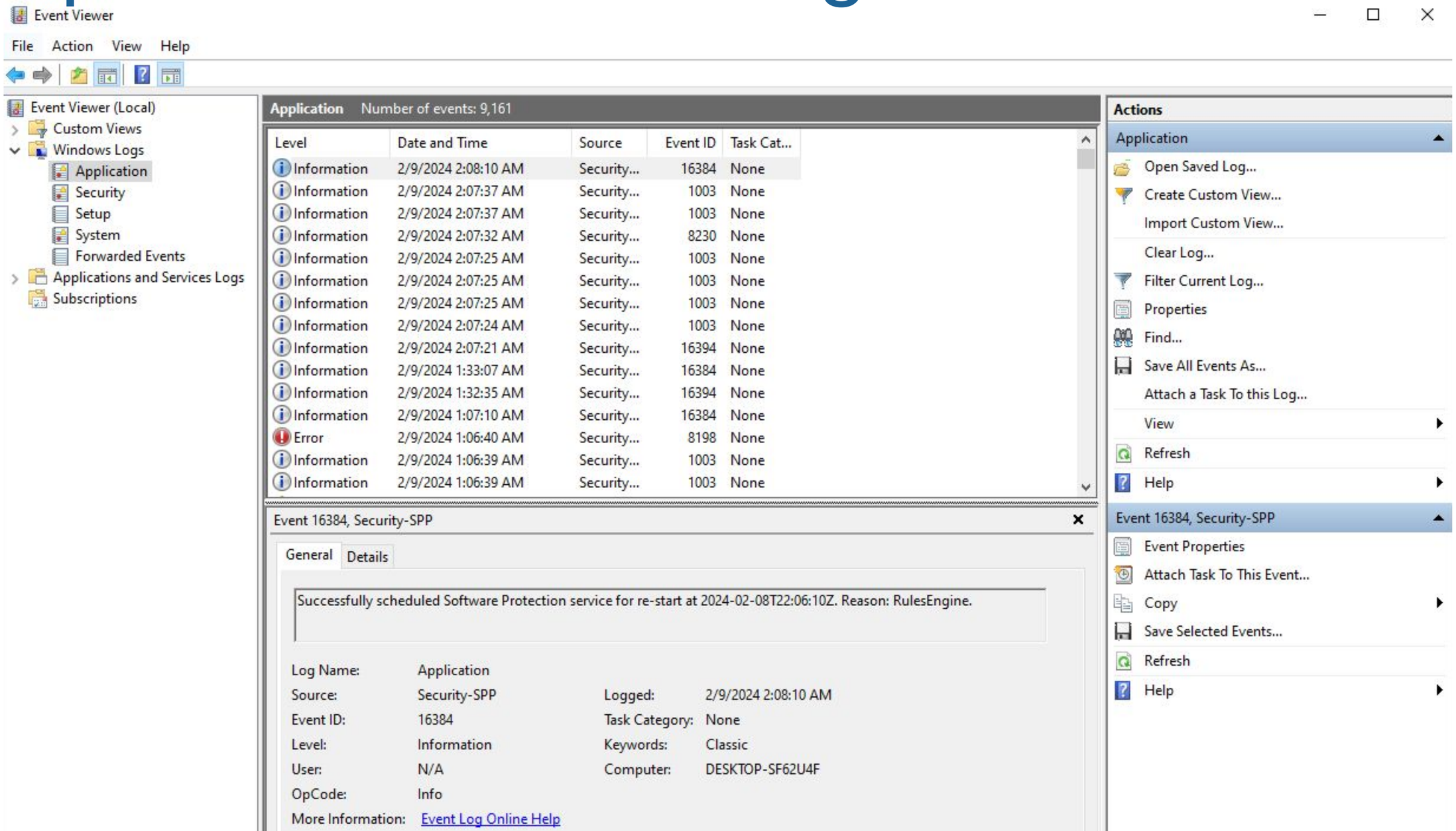
Understanding Event IDs

- Event IDs: Unique identifiers assigned to specific types of system or network events.
- Role in Cybersecurity: Crucial for identifying specific security incidents, system changes, or operational issues.
- Monitoring Event IDs:
- - Windows Security Event IDs: Key IDs such as 4625 (Failed login attempt), 4740 (Account lockout), etc.

Understanding Event IDs(cont.)

- Importance of Context: Understanding the relevance of an Event ID within the specific environment.
- Interpreting Event IDs:
- - Tools and Resources: Utilize event log management tools and online databases for interpretation.
- - Correlation: Combine insights from various Event IDs for a comprehensive understanding of events.

Example of Event ID & Logs



Introduction to MITRE ATT&CK Framework

- Definition: A knowledge base of adversary tactics and techniques based on real-world observations.
- Components: Detailed enumeration of tactics (goals of the attackers) and techniques (methods to achieve goals).
- Application in Cybersecurity:

- Threat Modeling: Understanding attacker methodologies to strengthen defenses.
- Security Assessments: Identifying gaps in current security posture.
- Enhancing Incident Response: Developing more informed response strategies.

Implementing MITRE ATT&CK in Cybersecurity

- Practical Uses:
- - Incident Response: Mapping attack patterns to MITRE ATT&CK to inform response actions.
- - Threat Hunting: Proactively searching for malicious activities aligned with known tactics and techniques.
- Case Studies:
- - Example 1: Utilization in identifying and responding to an APT (Advanced Persistent Threat) attack.
- - Example 2: Application in a SOC (Security Operations Center) for enhancing monitoring and alerting processes.

The Cyber Kill Chain Framework

- Cyber Kill Chain Overview:
- - Origin: Developed by Lockheed Martin as a model to identify and prevent cyber intrusions.
- - Stages: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Actions on Objectives.
- Utilization in Cyber Defense:
- - Identifying Weak Points: Analyzing each stage to identify where attacks can be prevented.
- - Disrupting Attacks: Implementing countermeasures at different stages to interrupt the attack chain.

THE CYBER KILL CHAIN

MITRE ATT&CK vs. Cyber Kill Chain

- Comparative Analysis:
  - Structure: MITRE ATT&CK focuses on specific tactics and techniques, while CKC outlines the stages of an attack lifecycle.
  - Approach: ATT&CK provides a more granular view of attacker behavior; CKC offers a linear progression of an attack.
- Complementary Use:
  - Integration: Using CKC to understand the attack lifecycle and MITRE ATT&CK to delve into detailed attacker tactics and techniques.
  - Situational Application: Depending on the organization's needs, one may be more applicable than the other, or both can be used in tandem for comprehensive defense.

CYBER KILL CHAIN vs. MITRE ATT&CK

CYBER KILL CHAIN

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives

MITRE ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact

Benefits of Integrating Frameworks

- Integrating MITRE ATT&CK and CKC:
  - Synergy: Utilizing both frameworks for a comprehensive security strategy.
  - Enhanced Threat Intelligence: Combining MITRE's detailed techniques with CKC's attack progression for richer insights.
- Operational Benefits:
  - Improved Detection and Response: A more nuanced understanding of threats leads to quicker and more effective responses.
  - Strategic Planning: Informing cybersecurity roadmaps with insights from both frameworks.

Challenges in Log Analysis and Event ID Interpretation

- Common Challenges:
  - Volume of Data: Managing and analyzing large quantities of log data.
  - False Positives: Differentiating between actual threats and benign anomalies.
  - Contextual Understanding: Interpreting logs and Event IDs within the context of your specific environment.
- Overcoming Challenges:
  - Effective Tools: Leveraging advanced log analysis tools for better data management and analysis.
  - Skilled Personnel: Employing or training staff with the expertise to accurately interpret log data and Event IDs.

Case Studies in Log Analysis and Event Monitoring

- Real-World Applications: Case Studies in Log Analysis and Event Monitoring
- - Case Study 1:

- Scenario: Detection of an insider threat through anomaly detection in log data.
- Outcome: Early identification and mitigation of data exfiltration attempt.

- - Case Study 2:

- Scenario: Identifying and responding to a network breach using Event ID analysis.
- Outcome: Quick containment of the breach and prevention of data loss.

Future Trends in Log Analysis and Threat Detection Frameworks

- Emerging Trends:
  - AI and Machine Learning: Enhancing log analysis with automated pattern recognition and anomaly detection.
  - Integration of Cloud-based Analytics: Increased use of cloud platforms for scalable and efficient log management.
- Adapting to Future Threats:
  - Staying Informed: Keeping up-to-date with the latest developments in cybersecurity.
  - Continual Learning: Emphasizing the need for ongoing education and training in new technologies and methodologies.

Advanced Techniques in Log Analysis

- Deep Dive into Techniques:
  - Behavioral Analysis: Understanding normal patterns to identify anomalies.
  - Predictive Analytics: Using historical data to predict and prevent future incidents.
  - Root Cause Analysis: Tracing back events to identify the source of security incidents.
- Utilizing Advanced Tools:
  - Advanced SIEM solutions and machine learning-based analytics tools.
  - Enhanced Detection: Improved ability to spot sophisticated threats.
  - Proactive Security Posture: Moving from reactive to predictive threat management.

Event ID Management Best Practices

- Key Practices:

- Regular Auditing: Frequently review and analyze Event IDs for unusual activities.
- Contextual Analysis: Understanding the relevance of Event IDs in your specific environment.
- Correlation: Linking Event IDs with other security data for a comprehensive view.

- Tools and Solutions:

- Event management software and correlation engines.

- Importance:

- Reduces the risk of missed threats.
- Enhances the overall security posture of the organization.

THANK YOU