Security Event Log Analysis Report

File Name: events_filtered_Security.csv

File Size: 1.37 MB

Collection Date: October 31, 2025

Report Generated: January 17, 2026, 12:13 PM

1. File Overview and Meaning

1.1 What is the Security Event Log?

The Windows Security Event Log (events_filtered_Security.csv) is a comprehensive audit trail of all security-related activities on a Windows system. It is one of the most critical components of Windows security auditing and provides a detailed record of:

- Authentication Events: Who logged in, when, from where, and how
- Authorization Events: What privileges were assigned and used
- Account Management: Creation, deletion, and modification of user accounts and groups
- System Security Events: Security policy changes, object access, and system integrity events
- Audit Events: Tracking of sensitive operations and privilege use

1.2 Purpose and Importance

The Security Event Log serves multiple critical purposes:

1. Security Monitoring: Detect suspicious activities, unauthorized access, and potential security breaches
2. Compliance Auditing: Meet regulatory requirements (SOX, HIPAA, PCI-DSS, GDPR) for access control and audit trails
3. Incident Response: Provide forensic evidence during security investigations
4. Forensic Analysis: Reconstruct security events timeline for investigations
5. Threat Detection: Identify indicators of compromise (IOCs) and attack patterns
6. Accountability: Track user actions and system changes for accountability

1.3 File Format and Structure

File Type: CSV (Comma-Separated Values)

Encoding: UTF-8

Delimiter: Comma (,)

Text Qualifier: Double quotes (")

Header Row: Yes

The file contains structured data where each row represents a single security event, with fields separated by commas. Multiline fields (like event messages) are properly quoted to preserve formatting.

2. Data Types and Structure

2.1 Data Fields

Each security event contains the following standard fields:

Field Name Data Type Description Example

TimeCreated DateTime Timestamp when event

occurred

"31-10-2025 06:50:22

PM"

Id Integer Windows Event ID

(unique identifier)

"4624" (Successful

logon)

LevelDisplayName String Event severity level "Information", "Warning",

"Error"

Message Text (Multiline)

Detailed event

description with

structured data

Contains account info,

IPs, processes, etc.

2.2 Event Message Structure

The Message field contains structured information in a human-readable format, including:

- Subject Information: Account that triggered the event
- Target Information: Account or object affected by the event
- Process Information: Executable path, process ID (PID)
- Network Information: Source IP address, port numbers, workstation names
- Authentication Details: Logon type, authentication package, logon GUID
- Privilege Information: Specific privileges assigned or used
- Group Membership: Security group changes

2.3 Key Data Types Contained

Sensitive Data Categories:

1. User Identifiers:

2. Account names (usernames)

3. Security IDs (SIDs)

Logon IDs (session identifiers)

Network Information:

6. IP addresses (source and destination)

7. Port numbers

8. Workstation names

Network account domains

System Information:

11. Process paths and PIDs

12. File paths accessed

13. Registry keys modified

Service names

Authentication Data:

16. Logon types and methods

17. Authentication packages used

18. Kerberos ticket information

Credential usage patterns

Security Configuration:

21. Privilege assignments
22. Group membership changes
23. Security policy modifications

3. Where This Data Is Used

3.1 Primary Use Cases

A. Security Operations Center (SOC)

- Real-time Monitoring: Continuous monitoring of security events for threats
- Alert Generation: Triggering alerts based on suspicious patterns
- Threat Hunting: Proactively searching for indicators of compromise
- Incident Triage: Prioritizing security events for investigation

B. Compliance and Auditing

- Regulatory Compliance: Meeting requirements for SOX, HIPAA, PCI-DSS, GDPR
- Internal Audits: Regular security audits and assessments
- Access Reviews: Verifying appropriate access controls
- Change Management: Tracking security configuration changes

C. Incident Response

- Timeline Reconstruction: Building chronological event sequences
- Root Cause Analysis: Understanding how security incidents occurred
- Forensic Investigation: Providing evidence for legal proceedings
- Containment Actions: Identifying compromised accounts and systems

D. Security Analytics

- Behavioral Analysis: Establishing normal user behavior baselines
- Anomaly Detection: Identifying deviations from normal patterns
- Attack Pattern Recognition: Detecting known attack techniques
- Risk Assessment: Evaluating security posture and risks

E. System Administration

- Troubleshooting: Diagnosing authentication and access issues

- User Activity Tracking: Understanding user behavior and access patterns
- Policy Enforcement: Verifying security policies are being followed
- Performance Monitoring: Identifying authentication bottlenecks

3.2 Integration with Security Tools

Security Event Log data is commonly integrated with:

- SIEM Systems: Security Information and Event Management (Splunk, QRadar, ArcSight)
- EDR Solutions: Endpoint Detection and Response tools
- Log Aggregation Platforms: Centralized log management systems
- Threat Intelligence Platforms: Correlation with threat intelligence feeds
- Compliance Tools: Automated compliance monitoring and reporting
- Analytics Platforms: Machine learning and behavioral analytics

3.3 Efficient Data Analysis Techniques

A. Filtering and Querying

- Event ID Filtering: Filter by specific Event IDs (e.g., 4625 for failed logins)
- Time Range Filtering: Analyze specific time periods
- Account Filtering: Focus on specific user accounts
- IP Address Filtering: Identify events from specific IPs
- Logon Type Filtering: Analyze specific authentication types

B. Pattern Recognition

- Failed Login Patterns: Identify brute force attempts (multiple 4625 events)
- Privilege Escalation: Track 4672 events for privilege assignments
- Account Manipulation: Monitor 4720-4733 events for unauthorized changes
- Unusual Access Times: Identify logins outside normal business hours
- Geographic Anomalies: Detect logins from unexpected locations

C. Statistical Analysis

- Frequency Analysis: Count events by type, account, or IP
- Trend Analysis: Identify patterns over time
- Baseline Establishment: Define normal behavior patterns

- Baseline Establishment: Define normal behavior patterns

- Anomaly Detection: Identify deviations from baselines

D. Correlation Analysis

- Event Correlation: Link related events (e.g., failed login followed by success)

- Account Correlation: Track account activities across events

- Time Correlation: Identify events occurring in sequence

- Network Correlation: Link network events with authentication events

3.4 Data Analysis Best Practices

Efficient Processing: 1. n Index Large Files: Use indexed databases for large log files 2. n Chunk Processing: Process files in chunks to manage memory 3. n Selective Loading: Load only required fields for analysis 4. n Parallel Processing: Use multi-threading for large-scale analysis 5. n Caching Results: Cache frequently accessed data

Query Optimization: 1. n Use Specific Filters: Filter early to reduce dataset size 2. n Avoid Full Scans: Use indexed fields for searches 3. n Limit Results: Only retrieve necessary data 4. n Batch Operations: Process multiple queries in batches 5. n Use Aggregations: Prefer aggregated results over raw data

Performance Considerations: - Large Security Event Log files can contain millions of events - CSV format requires full file parsing (consider converting to database) - Message field parsing is computationally expensive - Use appropriate tools for large-scale analysis (databases, SIEM systems)

4. Data Protection and Security Precautions

4.1 Why Security Event Logs Need Protection

Security Event Logs contain highly sensitive information:

- n User Activity Patterns: Reveal user behavior and access patterns

- n Network Topology: IP addresses and network structure

- n System Configuration: Security settings and configurations

- n Account Information: Usernames and account relationships

- n Attack Intelligence: Information about security events and potential vulnerabilities

- n Compliance Data: Contains audit information subject to regulatory requirements

- n Compliance Data: Contains audit information subject to regulatory requirements

Risk if Compromised: - Attackers could use this information to understand system architecture - User behavior patterns could be exploited for social engineering - Network topology information could aid in attack planning - Compliance violations could result from data breaches

4.2 Data Storage Security

A. Encryption Requirements

At Rest: - n Store on encrypted volumes (BitLocker, FileVault, or equivalent) - n Use file-level encryption for additional protection - n Encrypt backups using strong encryption (AES-256 or higher) - n Use password-protected archives when transferring files

In Transit: - n Use encrypted channels (HTTPS, SFTP, VPN) when transferring files - n Never send Security Event Logs via unencrypted email - n Use secure file sharing platforms with encryption - n Verify SSL/TLS certificates when transferring data

B. Access Control

Principle of Least Privilege: - n Grant access only to authorized security analysts and administrators - n Use separate accounts for log analysis (not daily-use accounts) - n Implement role-based access control (RBAC) - n Log all access to Security Event Log files for audit purposes - n Use strong passwords or multi-factor authentication (MFA)

Access Logging: - n Monitor who accesses Security Event Log files - n Track when files are accessed and modified - n Alert on unauthorized access attempts - n Maintain audit trails for compliance

C. Storage Location Security

Physical and Network Security: - n Store files in secure, access-controlled directories - n Use dedicated security analysis workstations when possible - n Avoid storing on shared or public cloud storage without encryption - n Implement proper file permissions (read-only for analysts, restricted access) - n Use isolated network segments for log analysis - n Consider air-gapped systems for highly sensitive analysis

4.3 Data Handling Procedures

Before Analysis

1. n Verify file integrity (checksums, hashes) before processing
2. n Scan files with antivirus before opening
3. n Work in isolated analysis environment
4. n Create read-only copies for analysis (never modify originals)
5. n Document all analysis activities

During Analysis

1. n Use dedicated analysis tools (not production systems)
2. n Avoid copying sensitive data to clipboard unnecessarily
3. n Use secure analysis platforms (VMware, VirtualBox with isolated networks)
4. n Implement screen lock policies
5. n Monitor analysis activities
6. n Clear analysis tool caches after use

After Analysis

1. n Securely delete temporary analysis files
2. n Clear analysis tool caches
3. n Document findings in secure reports (encrypted if necessary)
4. n Archive original files securely
5. n Maintain chain of custody documentation

4.4 Data Retention and Disposal

Retention Policies

- n Establish retention policies based on legal and compliance requirements
- n Typically retain Security Event Logs for 90 days minimum
- n Some regulations require 1-7 years retention
- n Implement automated retention management
- n Review and update retention policies regularly

Secure Disposal

- n Use secure deletion methods (DoD 5220.22-M standard or equivalent)
- n Overwrite data multiple times when deleting

- n Overwrite data multiple times when deleting
- n Physically destroy storage media when disposing
- n Document disposal activities
- n Maintain disposal certificates
- n Verify successful deletion

4.5 Sharing and Distribution Guidelines

Internal Sharing

- n Share only with authorized team members
- n Use secure internal file sharing systems
- n Implement access logging
- n Use encrypted communication channels
- n Redact sensitive information when possible

External Sharing

- nn Requires Approval: Get management approval before external sharing
- n Redact all sensitive data (IPs, usernames, specific account details)
- n Use secure sharing platforms with encryption
- n Set expiration dates on shared links
- n Monitor access to shared files
- n Use non-disclosure agreements (NDAs) when appropriate
- n Only share what is absolutely necessary

4.6 Compliance Considerations

GDPR (General Data Protection Regulation)

- nn Security Event Logs may contain personal data
- n Implement data minimization (only collect necessary data)
- n Document legal basis for processing
- n Implement data subject rights (access, deletion)
- n Maintain data processing records

Other Regulations

- HIPAA: Healthcare data protection requirements

- HIPAA: Healthcare data protection requirements
- PCI-DSS: Payment card industry data security
- SOX: Financial reporting requirements
- Industry-specific regulations: Varies by industry

4.7 Incident Response Procedures

If Security Event Logs Are Compromised: 1. n Immediately isolate affected systems 2. n Notify security team and management 3. n Document the incident 4. n Assess scope of compromise 5. n Implement containment measures 6. n Notify affected parties if required by law 7. n Conduct post-incident review

Prevention Measures: - n Regular security audits of systems storing logs - n Monitor access to Security Event Log files - n Implement intrusion detection - n Conduct security awareness training - n Perform regular security assessments

5. Executive Summary

This report provides a comprehensive analysis of Windows Security Event Log entries collected from the system. The Security Event Log is one of the most critical sources of security information, recording authentication events, authorization activities, account management, and privilege use.

Key Statistics

- Total Events Analyzed: 1,000
- Failed Login Attempts: 0
- Successful Logins: 0
- Privilege Assignment Events: 0
- Account Management Events: 0

Security Posture Overview

Based on the analysis of Security Event Log data:

- Authentication: 0 successful logins and 0 failed attempts
- Security Events: 0 privilege assignment events requiring review
- Account Changes: 0 account management events to verify
- Data Sensitivity: High - Contains sensitive authentication, network, and system information
- Protection Required: Encryption, access controls, and secure handling

- Protection Required: Encryption, access control, and secure handling mandatory

6. Event Analysis Overview

1.1 Event Distribution by Level

LevelCountPercentage

1.2 Top Event IDs

The following table shows the most frequently occurring Event IDs in the Security log:

Event

IDCountDescription

7. Authentication Analysis

2.1 Successful Logins

Total Successful Logins: 0

Successful logins (Event ID 4624) indicate when accounts successfully authenticated to the system. This is normal system activity but should be monitored for: - Unusual login times - Logins from unexpected locations - Multiple logins in short time periods - Logins to privileged accounts

2.2 Failed Login Attempts

Total Failed Logins: 0

Failed login attempts (Event ID 4625) are critical security indicators. They can indicate: - Brute force attacks - Account enumeration attempts - Credential theft attempts - User errors (typos, forgotten