*File Name**: `events_filtered_Security.csv`

Report Generated: January 16, 2026

System: DESKOFSKYCRAWLE

Collection Date: October 31, 2025, 18:50:32 UTC

---

1. File Overview

1.1 Basic Information

- **File Path**: `logs/events_filtered_Security.csv`
- **File Type**: CSV (Comma-Separated Values)
- **Encoding**: UTF-8
- **File Size**: 1,436,860 bytes (~1.4 MB)
- **Record Count**: 1,000 events (analyzed)
- **Time Range**: Last 30 days from collection date
- **Source**: Windows Security Event Log (Event Viewer)

1.2 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

1.3 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

---

2. Data Structure

2.1 CSV Format

- **Encoding**: UTF-8

- **Delimiter**: Comma (`,`)

- **Text Qualifier**: Double quotes (`"`)

- **Header Row**: Yes

- **Multiline Fields**: Yes (Message field contains multiline text)

2.2 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.

2.3 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

---

3. Executive Summary

3.1 Key Statistics

Based on analysis of **1,000 events** from the Security Event Log:

- **Total Events Analyzed**: 1,000
- **Failed Login Attempts**: 0
- **Successful Logins**: 500 (Event ID 4624)
- **Privilege Assignment Events**: 473 (Event ID 4672)
- **Logon with Explicit Credentials**: 27 (Event ID 4648)
- **Event Levels**: 100% Information (no warnings or errors)

3.2 Security Posture Overview

Overall Assessment: ✅ **GOOD SECURITY POSTURE**

- ✅ **No Failed Login Attempts**: Excellent - No brute force attacks or authentication failures detected
- ✅ **Normal Authentication Activity**: 500 successful logins indicate normal system usage
- ✅ **Privilege Events**: 473 privilege assignment events require review to ensure they are legitimate
- ✅ **No Account Management Events**: No unauthorized account creation, deletion, or modification detected
- ✅ **All Events are Information Level**: No critical errors or warnings in the analyzed period

3.3 Top Event IDs

Event ID	Count	Percentage	Description
4624	500	50.0%	Successful logon
4672	473	47.3%	Special privileges assigned to new logon
4648	27	2.7%	Logon with explicit credentials

---

4. Detailed Event Analysis

4.1 Authentication Events

Successful Logins (Event ID 4624)

Total: 500 events (50% of all events)

Successful logins 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

Security Assessment: ✅ **NORMAL** - High number of successful logins is expected for an active system.

Failed Login Attempts (Event ID 4625)

Total: 0 events

Failed login attempts are critical security indicators. They can indicate:

- Brute force attacks
- Account enumeration attempts
- Credential theft attempts

- User errors (typos, forgotten passwords)

Security Assessment: ✅ **EXCELLENT** - No failed login attempts detected in the analyzed period. This is a very positive security indicator.

Logon with Explicit Credentials (Event ID 4648)

Total: 27 events (2.7% of all events)

Event ID 4648 indicates a logon using explicit credentials (RunAs or similar). This can be:

- Normal administrative activity (RunAs for elevated privileges)

- Scheduled tasks running with specific credentials

- Service accounts authenticating

- Potentially suspicious if unexpected

Security Assessment: ⚠ **REVIEW RECOMMENDED** - 27 events should be reviewed to ensure they are legitimate administrative activities.

4.2 Privilege and Authorization Events

Privilege Assignment Events (Event ID 4672)

Total: 473 events (47.3% of all events)

Event ID 4672 indicates when special privileges are assigned to a logon session. These privileges include:

- SeAssignPrimaryTokenPrivilege

- SeTcbPrivilege (Trusted Computing Base)

- SeSecurityPrivilege

- SeTakeOwnershipPrivilege

- SeLoadDriverPrivilege

- SeBackupPrivilege

- SeRestorePrivilege

- SeDebugPrivilege

- SeAuditPrivilege

- SeSystemEnvironmentPrivilege

- SeImpersonatePrivilege

Security Assessment: ⚠ **REVIEW REQUIRED** - 473 privilege assignment events detected. Review to ensure:

- Privileges are assigned to legitimate system processes

- No unauthorized privilege escalation

- Privileges are used appropriately

- Most should be SYSTEM account (S-1-5-18) which is normal

Note: Many of these events are likely from the SYSTEM account during normal system operations, which is expected behavior.

4.3 Account Management Events

Total: 0 events

Account management events track changes to user accounts and group memberships:

- Event ID 4720: User account was created

- Event ID 4722: User account was enabled

- Event ID 4724: Attempt to reset account password

- Event ID 4726: User account was deleted

- Event ID 4732: Member was added to a security-enabled local group

- Event ID 4733: Member was removed from a security-enabled local group

Security Assessment: ✅ **GOOD** - No account management events detected. This indicates:

- No unauthorized account creation

- No account deletions

- No group membership changes

- No password resets

---

5. Event Distribution Analysis

5.1 Event Distribution by Level

| Level | Count | Percentage |

|-------|-------|------------|

| Information | 1,000 | 100.0% |

| Warning | 0 | 0.0% |

| Error | 0 | 0.0% |

| Critical | 0 | 0.0% |

Analysis: All events are at the Information level, which indicates:

- ✅ No critical security errors

- ✅ No warnings that require immediate attention

- ✅ Normal system operation

5.2 Event ID Distribution

| Event ID | Count | Percentage | Description |

|--------|-------|-----------|------------|

| 4624 | 500 | 50.0% | Successful logon |

| 4672 | 473 | 47.3% | Special privileges assigned to new logon |

| 4648 | 27 | 2.7% | Logon with explicit credentials |

Analysis:

- Authentication events (4624, 4648) represent 52.7% of all events

- Privilege events (4672) represent 47.3% of all events

- This distribution is typical for a Windows system with active logging

---

6. Security Assessment

6.1 Overall Security Posture

Risk Level: ✅ **LOW RISK**

The Security Event Log analysis shows normal activity with no significant security concerns:

1. ✅ **No Failed Login Attempts**: Excellent security indicator

2. ✅ **Normal Authentication Patterns**: Expected number of successful logins

3. ✅ **Privilege Events**: High number but likely normal system operations

4. ✅ **No Account Management Events**: No unauthorized changes detected

5. ✅ **No Critical Errors**: All events are Information level

6.2 Security Strengths

1. **Strong Authentication Security**: Zero failed login attempts indicates:
   - No brute force attacks
   - No account enumeration attempts
   - Strong password policies likely in place
   - Good account security

2. **Stable Account Management**: No account management events indicates:
   - No unauthorized account creation
   - No account deletions
   - Stable user base
   - No suspicious group changes

3. **Clean Event Log**: All Information-level events indicate:
   - No critical security errors
   - System operating normally
   - No immediate security concerns

6.3 Areas for Review

1. **Privilege Assignment Events (4672)**: 473 events should be reviewed to ensure:
   - Most are from SYSTEM account (expected)
   - No unexpected privilege escalations
   - Legitimate administrative activities

2. **Logon with Explicit Credentials (4648)**: 27 events should be verified:
   - Legitimate RunAs usage

- Expected scheduled task authentications

- No unauthorized credential usage

---

7. Security Recommendations

7.1 Immediate Actions

1. ✅ **No Immediate Actions Required**: The analysis shows good security posture with no critical issues.

2. ✅ **Review Privilege Events**: Review the 473 privilege assignment events (Event ID 4672) to ensure:

- They are from legitimate system processes

- No unexpected privilege escalations

- Most are from SYSTEM account (S-1-5-18)

3. ✅ **Verify Explicit Credential Logons**: Review the 27 Event ID 4648 events to ensure:

- Legitimate administrative RunAs usage

- Expected scheduled task authentications

- No unauthorized credential usage

7.2 Ongoing Monitoring

1. **Regular Review**: Review Security Event Logs regularly (daily or weekly)

2. **Alert Configuration**: Set up alerts for:

- Multiple failed login attempts (Event ID 4625) - Currently none, which is good

- Account management events (Event IDs 4720-4733) - Currently none
- Privilege assignment events (Event ID 4672) - Review patterns
- Unusual login times or locations
- Privilege escalation attempts
- Account creation/deletion
- Group membership changes

3. **Baseline Establishment**: Establish normal patterns for:
- Login times
- Account usage
- Network logins
- Authentication methods
- Privilege assignments

4. **Incident Response**: Maintain procedures for investigating security events

7.3 Best Practices

1. **Log Retention**:
- Maintain Security Event Logs for at least 90 days (compliance may require longer)
- Some regulations require 1-7 years retention
- Implement automated retention policies

2. **Centralized Logging**:
- Consider implementing centralized log collection (SIEM)
- Use log aggregation platforms
- Implement real-time log forwarding

3. **Regular Audits**:

- Conduct regular security audits using Event Logs

- Perform monthly security reviews

- Quarterly comprehensive audits

4. **Access Control**:

- Limit access to Security Event Logs to authorized security personnel

- Implement role-based access control

- Monitor access to log files

5. **Monitoring Tools**:

- Implement automated monitoring and alerting tools

- Use SIEM systems for correlation and analysis

- Configure real-time alerts for critical events

---

8. Important Event IDs Reference

8.1 Authentication Events

| Event ID | Description | Security Relevance | Count in Analysis |

|---|---|---|---|

| 4624 | Successful logon | Monitor for unusual logins | 500 |

| 4625 | Failed logon attempt | **HIGH** - Brute force indicator | 0 |

| 4634 | Account was logged off | Normal activity | 0 |

| 4647 | User initiated logoff | Normal activity | 0 |

| 4648 | Logon with explicit credentials | **MEDIUM** - Review RunAs usage | 27 |

8.2 Privilege and Authorization

Event ID	Description	Security Relevance	Count in Analysis
4672	Special privileges assigned	**HIGH** - Privilege escalation indicator	473
4673	Sensitive privilege use	**HIGH** - Privilege abuse indicator	0
4674	Operation attempted on privileged object	**MEDIUM** - Access to sensitive objects	0

8.3 Account Management

Event ID	Description	Security Relevance	Count in Analysis
4720	User account was created	**HIGH** - Unauthorized account creation	0
4722	User account was enabled	**MEDIUM** - Account activation	0
4724	Attempt to reset account password	**HIGH** - Password reset activity	0
4726	User account was deleted	**HIGH** - Account deletion	0
4732	Member added to security group	**HIGH** - Privilege escalation	0
4733	Member removed from security group	**MEDIUM** - Group membership change	0

---

9. Sample Event Analysis

9.1 Sample Event: Privilege Assignment (Event ID 4672)

```
TimeCreated: "31-10-2025 06:50:22 PM"
```

Id: "4672"

LevelDisplayName: "Information"

Message: "Special privileges assigned to new logon.

Subject:

Security ID: S-1-5-18

Account Name: SYSTEM

Account Domain: NT AUTHORITY

Logon ID: 0x3E7

Privileges: SeAssignPrimaryTokenPrivilege

SeTcbPrivilege

SeSecurityPrivilege

SeTakeOwnershipPrivilege

SeLoadDriverPrivilege

SeBackupPrivilege

SeRestorePrivilege

SeDebugPrivilege

SeAuditPrivilege

SeSystemEnvironmentPrivilege

SeImpersonatePrivilege

SeDelegateSessionUserImpersonatePrivilege"

```

**Analysis**:

- **Event ID 4672**: Special privileges assigned to new logon

- **Subject**: SYSTEM account (S-1-5-18) - This is the Windows Local System account

- **Privileges**: Multiple high-level privileges assigned including:
```

- SeTcbPrivilege (Act as part of the operating system)

- SeDebugPrivilege (Debug programs)

- SeSecurityPrivilege (Manage auditing and security log)

- SeBackupPrivilege / SeRestorePrivilege

Security Relevance: This is a normal system event when services or system processes start. However, if seen with unexpected accounts, it could indicate privilege escalation.

9.2 Sample Event: Successful Logon (Event ID 4624)

```

TimeCreated: "31-10-2025 06:50:22 PM"

Id: "4624"

LevelDisplayName: "Information"

Message: "An account was successfully logged on.

Subject:

 Security ID:  S-1-5-18

 Account Name:  DESKOFSKYCRAWLE$

 Account Domain:  WORKGROUP

 Logon ID:  0x3E7

Logon Information:

 Logon Type:  5

 Restricted Admin Mode:  -

 Remote Credential Guard:  -

 Virtual Account:  No

 Elevated Token:  Yes
```

New Logon:

Security ID: S-1-5-18

Account Name: SYSTEM

Account Domain: NT AUTHORITY

Logon ID: 0x3E7

...

```

**Analysis**:

- **Event ID 4624**: Successful logon

- **Logon Type**: 5 (Service logon)

- **Account**: SYSTEM account (S-1-5-18)

- **Elevated Token**: Yes

**Security Relevance**: This is a normal service logon. Logon Type 5 indicates a service account authentication, which is expected system behavior.

---

## 10. Data Protection and Security Precautions

### 10.1 Why Security Event Logs Need Protection

Security Event Logs contain highly sensitive information:

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

- **Network Topology**: IP addresses and network structure

- **System Configuration**: Security settings and configurations
```

- □ **Account Information**: Usernames and account relationships
- □ **Attack Intelligence**: Information about security events and potential vulnerabilities
- □ **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

10.2 Data Storage Security

Encryption Requirements

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

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

Access Control

Principle of Least Privilege:

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

10.3 Data Handling Procedures

Before Analysis

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

During Analysis

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

After Analysis

1. ☐ Securely delete temporary analysis files
2. ☐ Clear analysis tool caches
3. ☐ Document findings in secure reports (encrypted if necessary)

4. ☐ Archive original files securely

5. ☐ Maintain chain of custody documentation

---

11. Where This Data Is Used

11.1 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

11.2 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

---

12. Conclusion

12.1 Summary

This analysis of the Security Event Log provides valuable insights into system security activities. The log contains **1,000 events** covering authentication, authorization, account management, and system security.

12.2 Key Findings

1. **Failed Logins**: 0 failed login attempts detected
2. **Successful Logins**: 500 successful logins recorded
3. **Privilege Events**: 473 privilege assignment events (Review recommended)
4. **Account Management**: 0 account management events
5. **Event Levels**: 100% Information level (no errors or warnings)

12.3 Overall Security Assessment

 LOW RISK: Security Event Log analysis shows normal activity with no significant security concerns.

The analysis indicates:

- Strong authentication security (no failed logins)
- Stable account management (no unauthorized changes)
- Normal system operations (all Information-level events)
- Some privilege events require review but are likely normal

12.4 Next Steps

1. Continue monitoring for failed login attempts
2. Review the 473 privilege assignment events to ensure legitimacy
3. Verify the 27 explicit credential logons are authorized
4. Maintain current security monitoring practices

5. □ Continue regular log reviews

---

13. Related Files

- `events_filtered_System.csv` - System-level events
- `events_filtered_Application.csv` - Application-level events
- `risk_signals/failed_logins.csv` - Extracted failed login attempts
- `risk_signals/successful_logins_interactive.csv` - Successful interactive logons
- `Security_Events_Report.pdf` - Comprehensive PDF report with detailed analysis

---

14. Notes

- CSV format requires careful parsing due to multiline messages
- Event messages contain structured data that may need specialized parsing
- Timezone: Events are recorded in system local time
- File size suggests comprehensive logging is enabled
- This analysis covers 1,000 events from the Security Event Log
- For complete analysis, refer to the full Security_Events_Report.pdf

---

Report Generated: January 16, 2026

Analysis Tool: Security Event Log Analyzer

System: DESKOFSKYCRAWLE

Collection Date: October 31, 2025, 18:50:32 UTC

This report is generated from Windows Security Event Log data. For detailed event information, refer to the original CSV file or the comprehensive PDF report.