Windows Event Log Forensic Report

=== Windows Event Log Analysis Report ===

Total Events Analyzed: 23

Failed Login Attempts (Event ID 4625):

	timestamp	AccountName	SourceIP	Details
1	2025-05-14 08:16:45	admin	192.168.1.15	Failed login attempt
4	2025-05-14 10:22:56	root	10.0.0.20	Failed login attempt
6	2025-05-15 03:14:27	admin	192.168.1.15	Failed login attempt
7	2025-05-15 03:14:30	admin	192.168.1.15	Failed login attempt
8	2025-05-15 03:14:35	admin	192.168.1.15	Failed login attempt

Total failed logins: 9

Successful Logins (Event ID 4624):

	timestamp	AccountName	SourceIP	Details
0	2025-05-14 08:15:23	user1	192.168.1.10	Successful login
5	2025-05-14 12:30:01	guest	172.16.0.10	Successful login
9	2025-05-15 07:45:12	user3	10.0.0.25	Successful login
11	2025-05-15 11:20:45	user1	192.168.1.10	Successful login
14	2025-05-16 02:15:00	admin	192.168.1.15	Successful login after multiple failures

Total successful logins: 7

Process Creation Events (Event ID 4688):

	timestamp	AccountName	Details
2	2025-05-14 09:00:12	user2	Process creation: cmd.exe
10	2025-05-15 09:00:00	system	Process creation: powershell.exe
15	2025-05-16 06:30:55	user3	Process creation: notepad.exe
21	2025-05-17 08:00:00	admin	Process creation: suspicious.exe

Total process creations: 4

Privilege Assignment Events (Event ID 4672):

	timestamp	AccountName	Details
3	2025-05-14 09:05:34	admin	Privilege assigned: SeSystemtimePrivilege
12	2025-05-15 14:33:22	user2	Privilege assigned: SeBackupPrivilege
18	2025-05-16 15:45:33	system	Privilege assigned: SeDebugPrivilege

Total privilege assignments: 3

Top 5 Source IPs by Event Count:

SourceIP	
192.168.1.15	8
192.168.1.10	3
172.16.0.5	3
10.0.0.20	3
172.16.0.10	2

Name: count, dtype: int64

Suspicious Account Activity (admin/root):

	timestamp	EventID	AccountName	SourceIP
1	2025-05-14 08:16:45	4625	admin	192.168.1.15
4	2025-05-14 10:22:56	4625	root	10.0.0.20
6	2025-05-15 03:14:27	4625	admin	192.168.1.15
7	2025-05-15 03:14:30	4625	admin	192.168.1.15
8	2025-05-15 03:14:35	4625	admin	192.168.1.15

Detailed results saved to forensic_event_analysis.csv
Visualizations saved in 'forensic_plots' directory as 'windows_event_plots.png'.
Analysis Visualizations: