StealthWard Endpoint Detection and Response

Security Threat Report

Generated: 2025-05-12 19:21:42

Executive Summary

510
TOTAL SYSTEM THREATS

100
NETWORK ALERTS

58626
TOTAL ATTACK ATTEMPTS

This report covers security events detected on the admin system and network between 2025-05-11 19:21:43 and 2025-05-12 19:21:42. Key findings include:

- **113 critical threats** detected on the admin system
- **100 critical network alerts** detected
- Most active threat source: **unknown** (510 events)
- Most active network attacker: **192.168.100.24** (100 alerts)

Network Status

Interface	Incoming Traffic	Outgoing Traffic	Total In	Total Out
wlp2s0	0.00 B/s	0.00 B/s	371.18 MB	35.35 MB

System Threat Analysis

Threat Overview

Severity	Count	Percentage
MEDIUM	397	77.8%
HIGH	105	20.6%
CRITICAL	8	1.6%

Top Threat Sources

Source IP	Count
unknown	510

Critical Threat Details

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.293539

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.293714

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.293983

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.294125

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.295075

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.295192

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.295520

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.295692

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.296092

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.296278

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.296849
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.297249
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.298615
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.299066
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.299675
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.300063
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.301387
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.301901
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.302263
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.302445
Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.309489

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.309881

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.310533

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.310867

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.311353

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.311679

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.327469

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.327664

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.327935

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.328118

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.336441

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.336766

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.337282

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.337615

Description: Execution of suspicious binaries

Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T18:23:58.402108

Description: Multiple successful logins from single source (possible lateral movement)

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.402381

Description: Execution of suspicious binaries

Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T18:23:58.403740

Description: Multiple successful logins from single source (possible lateral movement)

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.404034

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.404250

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.404464

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.404683

Description: Execution of suspicious binaries

Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T18:23:58.406708

Description: Multiple successful logins from single source (possible lateral movement)

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.406978

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.407209

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.407423

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.407638

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.407850

Description: Execution of suspicious binaries

Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T18:23:58.412420

Description: Multiple successful logins from single source (possible lateral movement)

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.412875

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.413178

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.413662

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.413944

Description: Execution of suspicious binaries

Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T18:23:58.414857

Description: Multiple successful logins from single source (possible lateral movement)

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.415285

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.415539

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.415766

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.416023

Description: Execution of suspicious binaries

Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T18:23:58.416423

Description: Multiple successful logins from single source (possible lateral movement)

Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T18:23:58.436293

Description: Multiple successful logins from single source (possible lateral movement)

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.436620

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.436838

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.437089

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.437346

Description: Execution of suspicious binaries

Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T18:23:58.437996

Description: Multiple successful logins from single source (possible lateral movement)

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.438285

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.438506

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.438722

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.438949

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.439193

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.439442

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.439724

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.439963

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.441749

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.442162

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.442393

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.482872

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.491322

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:58.491563

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:23:59.586715

Description: Execution of suspicious binaries

Log File: syslog

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:24:00.020754

Description: Execution of suspicious binaries

Log File: syslog

SQL injection attempt CRITICAL

Timestamp: 2025-05-12T18:24:00.504347
Description: SQL injection attempt
Log File: syslog

SSH brute force with multiple usernames CRITICAL

Timestamp: 2025-05-12T18:26:10.294891
Description: SSH brute force with multiple usernames
Log File: auth.log

SSH brute force with multiple usernames CRITICAL

Timestamp: 2025-05-12T18:26:10.294962
Description: SSH brute force with multiple usernames
Log File: auth.log

SSH brute force with multiple usernames CRITICAL

Timestamp: 2025-05-12T18:26:10.295052
Description: SSH brute force with multiple usernames
Log File: auth.log

SSH brute force with multiple usernames CRITICAL

Timestamp: 2025-05-12T18:26:10.295123
Description: SSH brute force with multiple usernames
Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T18:26:10.295193
Description: Multiple successful logins from single source (possible lateral movement)
Log File: auth.log

SSH brute force with multiple usernames CRITICAL

Timestamp: 2025-05-12T18:26:10.295525
Description: SSH brute force with multiple usernames
Log File: auth.log

SSH brute force with multiple usernames CRITICAL

Timestamp: 2025-05-12T18:26:10.295592
Description: SSH brute force with multiple usernames
Log File: auth.log

SSH brute force with multiple usernames CRITICAL

Timestamp: 2025-05-12T18:26:10.295659
Description: SSH brute force with multiple usernames
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:36:53.924251
Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:36:53.924419

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:36:53.924682

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:36:53.924849

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:36:53.925113

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T18:36:53.925280

Description: Execution of suspicious binaries

Log File: auth.log

Multiple successful logins from single source (possible lateral movement) HIGH

Timestamp: 2025-05-12T19:09:06.620622

Description: Multiple successful logins from single source (possible lateral movement)

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.620883

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.621091

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.621295

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.621509

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.621722

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.621926

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.622136

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.622340

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.622545

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.622750

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:09:06.622955

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:10:10.966651

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:10:10.966856

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:10:10.967063

Description: Execution of suspicious binaries

Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:10:10.967268
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:10:10.967472
Description: Execution of suspicious binaries
Log File: auth.log

Execution of suspicious binaries HIGH

Timestamp: 2025-05-12T19:10:10.967675
Description: Execution of suspicious binaries
Log File: auth.log

Network Threat Analysis

Alert Overview

Severity	Count	Percentage
HIGH	100	100.0%

Top Attack Sources

Source IP	Alerts	Attempts
192.168.100.24	100	58626

Targeted Services

Service	Alerts
SSH	100

Critical Alert Details

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.774039
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 551
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.785142
Source IP: 192.168.100.24

Target IP: unknown
Service: SSH
Attempts: 552
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.792712
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 553
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.807767
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 554
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.825770
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 555
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.829127
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 556
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.832236
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 557
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.835887

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 558

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.841486

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 559

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.843876

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 560

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.846032

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 561

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.848127

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 562

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.850237

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 563

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.852352
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 564
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.854539
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 565
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.857016
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 566
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.859260
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 567
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.861405
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 568
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.896566
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 569

Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:45.911786
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 570
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:45.914062
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 571
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:45.916418
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 572
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:45.927126
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 573
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:45.929338
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 574
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:45.931451
Source IP: 192.168.100.24
Target IP: unknown

Service: SSH

Attempts: 575

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.933539

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 576

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.936719

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 577

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.938946

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 578

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.941072

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 579

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.943295

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 580

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.945391

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 581

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.947493

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 582

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.949586

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 583

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.951921

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 584

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.954284

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 585

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.956428

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 586

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.958555
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 587
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.960651
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 588
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.980443
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 589
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.982723
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 590
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.984850
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 591
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.987208
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 592

Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.990131
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 593
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.992242
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 594
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.994346
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 595
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.996687
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 596
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:45.998801
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 597
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.001048
Source IP: 192.168.100.24
Target IP: unknown

Service: SSH

Attempts: 598

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.003526

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 599

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.005757

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 600

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.008978

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 601

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.011139

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 602

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.013243

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 603

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.015350

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 604

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.017466

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 605

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.019798

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 606

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.021997

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 606

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.024401

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 607

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.026528

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 608

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.028630

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 609

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.030732

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 610

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.032836

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 611

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.034968

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 612

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.037621

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 613

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.039877

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 614

Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:46.042040
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 615
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:46.044188
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 616
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:46.046329
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 617
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:46.048447
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 618
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:46.093594
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 619
Protocol: unknown
Category: bruteforce

SSH brute-force attempt **HIGH**

Timestamp: 2025-05-12T19:09:46.095852
Source IP: 192.168.100.24
Target IP: unknown

Service: SSH
Attempts: 620
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.098326
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 621
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.102406
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 622
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.111349
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 623
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.188130
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 624
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.229271
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 625
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.231963

Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 626
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.238532
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 627
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.260411
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 627
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.366252
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 626
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.368685
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 627
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.373534
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 628
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.376298

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 629

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.447137

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 630

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.449834

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 631

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.455933

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 632

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.460034

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 633

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.476466

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 634

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.479880

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 635

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.482140

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 636

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.840363

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 632

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.876235

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 633

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.878627

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH

Attempts: 634

Protocol: unknown

Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.885239

Source IP: 192.168.100.24

Target IP: unknown

Service: SSH
Attempts: 635
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.894189
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 636
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.952664
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 635
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.962501
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 636
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:09:46.966706
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 637
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:10:48.885955
Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 10
Protocol: unknown
Category: bruteforce

SSH brute-force attempt HIGH

Timestamp: 2025-05-12T19:10:52.405536

Source IP: 192.168.100.24
Target IP: unknown
Service: SSH
Attempts: 11
Protocol: unknown
Category: bruteforce

Recommendations

Immediate Actions

- **Block malicious IPs:** Consider blocking the top attacking IPs (192.168.100.24) at the firewall level
- **Harden vulnerable services:** The most targeted service was SSH - review its configuration and access controls
- **Review authentication logs:** Check for any successful unauthorized access attempts

Long-term Improvements

- **Implement rate limiting:** For services like SSH to prevent brute force attacks
- **Update and patch:** Ensure all systems and services are up-to-date with security patches
- **Review monitoring rules:** Fine-tune alert thresholds to reduce false positives