Behavior Analysis Report

Summary

- **Report ID**: `rpt-sha256-7f8a9b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f0a`
- **Chain ID**: `chain-ent-usr123-win24h-1706086400000`
- **Revision**: 2
- **Entity**: `user-jsmith-prod-01`
- **Time Window**: 2024-01-23 00:00:00 - 2024-01-24 00:00:00 UTC
- **Generated**: 2024-01-24 01:06:40 UTC
- **Report Version**: v2

Policy Versions

Policy	Version
Priority Policy	1.2.0
BPP Policy	2.1.0
Report Policy	1.0.0
AI Policy	1.5.0
Human Policy	1.0.0

Timeline

Node 0: BCP (Behavior Coordinate Point)

- **Type**: BCP

- **Time**: 2023-01-23 06:00:00 UTC
- **Log ID**: 1001
- **Event**: SSH Login Attempt (FAILURE)

Node 1: BCP (Behavior Coordinate Point)

- **Type**: BCP
- **Time**: 2023-01-23 06:00:01 UTC
- **Log ID**: 1002
- **Event**: SSH Login Attempt (FAILURE)

Node 2: BCP (Behavior Coordinate Point)

- **Type**: BCP
- **Time**: 2023-01-23 06:00:02 UTC
- **Log ID**: 1003
- **Event**: SSH Login Attempt (FAILURE)

Node 3: BCP (Behavior Coordinate Point)

- **Type**: BCP
- **Time**: 2023-01-23 06:00:03 UTC
- **Log ID**: 1004
- **Event**: SSH Login Attempt (FAILURE)

Node 4: BCP (Behavior Coordinate Point)

- **Type**: BCP
- **Time**: 2023-01-23 06:00:04 UTC
- **Log ID**: 1005
- **Event**: SSH Login Attempt (FAILURE)

Node 5: BSP (Behavior Success Point)

- **Type**: BSP
- **Time**: 2023-01-23 06:00:05 UTC
- **Log ID**: 1006
- **Event**: SSH Login Attempt (SUCCESS)

Node 6: BF (Behavior Fragment) - ssh_login_attempt (BFL: 3)

Time Range: 2023-01-23 06:00:00 - 2023-01-23 06:00:05 UTC

- **BF ID**: `bf-a1b2c3d4-e5f6-7890-1234-567890abcdef`
- **Action**: ssh_login_attempt
- **BFL**: 3 (HIGH)

BFL Explain:

Feature	Value	Weight	Type
action_id	AUTH	-	base
base_score	10	-	-
attempt_count	5	10	multiplicative
has_external_ip	true	20	additive
time_window_seconds	5	5	additive
final_score	**90**	-	-

Bindings:

- Member BCP Log IDs: [1001, 1002, 1003, 1004, 1005]
- Derived BPP ID: `bpp-e5f6-7890-1234-567890abcdef`
- Anchor BSP Log ID: 1006

BPP Event: bpp-e5f6-7890-1234-567890abcdef

- **Transition Type**: auth_success (SSH Brute Force → Success)
- **Anchor BSP**: Log ID 1006
- **PTI**: 0.92 (Very High)

PTI Explain:

Multiplier	Value
base_score	0.5
failed_attempts_before_success	5
time_window_seconds	5
unique_source_ips	1

Evidence Log IDs: [1001, 1002, 1003, 1004, 1005]

Node 7: BCP (Behavior Coordinate Point)

- **Type**: BCP
- **Time**: 2023-01-23 06:01:00 UTC
- **Log ID**: 2001
- **Event**: Sudo Attempt (FAILURE)

Node 8: BCP (Behavior Coordinate Point)

- **Type**: BCP
- **Time**: 2023-01-23 06:01:01 UTC
- **Log ID**: 2002
- **Event**: Sudo Attempt (FAILURE)

Node 9: BCP (Behavior Coordinate Point)

- **Type**: BCP
- **Time**: 2023-01-23 06:01:02 UTC
- **Log ID**: 2003
- **Event**: Sudo Attempt (FAILURE)

Node 10: BSP (Behavior Success Point)

- **Type**: BSP
- **Time**: 2023-01-23 06:01:03 UTC
- **Log ID**: 2004
- **Event**: Sudo Attempt (SUCCESS)

Node 11: BF (Behavior Fragment) - sudo_attempt (BFL: 2)

Time Range: 2023-01-23 06:01:00 - 2023-01-23 06:01:03 UTC

- **BF ID**: `bf-b2c3d4e5-f6a7-8901-2345-67890abcdef0`
- **Action**: sudo_attempt
- **BFL**: 2 (MEDIUM)

BFL Explain:

Feature	Value	Weight	Type
action_id	PRIV_ESC	-	base
base_score	30	-	-
attempt_count	3	5	multiplicative
is_sudo	true	20	additive
final_score	**65**	-	-

Bindings:

- Member BCP Log IDs: [2001, 2002, 2003]
- Derived BPP ID: `bpp-f6a7-8901-2345-67890abcdef0`
- Anchor BSP Log ID: 2004

BPP Event: bpp-f6a7-8901-2345-67890abcdef0

- **Transition Type**: priv_esc_success (Sudo Attempt → Success)
- **Anchor BSP**: Log ID 2004
- **PTI**: 0.78 (High)

PTI Explain:

Multiplier	Value
base_score	0.4
failed_attempts_before_success	3
time_window_seconds	3
is_privilege_escalation	true

Evidence Log IDs: [2001, 2002, 2003]

Hotspots

Hotspot 1: BFL_ESCALATION (HIGH)

- **Sequence Range**: [0, 6]
- **Reason Tags**: high_pti, external_ip, brute_force
- **Evidence**: bf-a1b2c3d4-e5f6-7890-1234-567890abcdef
- **Severity**: HIGH

Hotspot 2: TRANSITION_CLUSTER (MEDIUM)

- **Sequence Range**: [7, 11]

- **Reason Tags**: privilege_escalation, sudo_abuse
- **Evidence**: bf-b2c3d4e5-f6a7-8901-2345-67890abcdef0
- **Severity**: MEDIUM

Reviews

AI Review

- **Decision**: ESCALATE
- **Confidence**: 45%
- **Summary**: Detected SSH brute force attack from external IP followed by successful login and privilege escalation attempt. Escalating due to confirmed post-compromise activity.

Human Review

- **Verdict**: CONFIRMED_THREAT
- **Confidence**: 95%
- **Reviewer**: analyst-042
- **Summary**: Confirmed brute force attack followed by privilege escalation. Attacker gained root access. Recommend immediate incident response.

Audit Trail

Event	Timestamp
Chain Created	2024-01-24 00:00:00 UTC
Report Generated	2024-01-24 01:06:40 UTC
AI Reviewed	2024-01-24 01:23:20 UTC
Human Reviewed	2024-01-24 02:30:00 UTC

- **AI Queue ID**: aiq-001-ssh-brute
- **Human Queue ID**: hq-001-escalated
- **Reviewers**: analyst-042

Statistics Summary

Metric	Count
Total Timeline Nodes	12
BCP (Behavior Coordinate Points)	8
BSP (Behavior Success Points)	2
BF (Behavior Fragments)	2
BPP (Behavior Pivot Points)	2
Hotspots	2

Terminology Reference

Term	Full Name	Definition
BCP	Behavior Coordinate Point	The smallest semantic unit in a behavior chain. Marks the position of a failed behavior event.
BSP	Behavior Success Point	Marks that a specific behavior succeeded. A pure success marker.
BPP	Behavior Pivot Point	A special type of BSP representing the success point after consecutive failures. **All BPPs are BSPs, but not all BSPs are BPPs.** BPP is NOT a chain node - it is a BF derivation/explanation.
BF	Behavior Fragment	An aggregated behavioral pattern containing BCPs, BSP, and anchored by a BPP. BF is a chain node.
BFL	Behavior Fragment Level	Risk scoring (1=Low, 2=Medium, 3=High) mapped to ATT&CK tactics.
PTI	Phase Transition Intensity	Measures the strength of the pivot point (0-1 scale). Higher = stronger attack evidence. PTI only exists in BPP, never in BF.

Report Generated by: ChainForge Security Analysis System v2.0.3
Classification: CONFIDENTIAL - Internal Use Only