Behavior Chain Report (ReportV2 - Full Chain Restorability)

Report Metadata

Field	Value
Report ID	`7f8a9b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b0c1d2e3f4a5b6c7d8e9f0a`
Chain ID	`chain-ent-usr123-win24h-1706086400000`
Revision	2
Report Version	**v2** (Full Chain Restorability)
Schema Version	**v2.0.5** (Timeline Structure Fix)

---

v2.0.5 Timeline Structure

> ***IMPORTANT SEMANTIC CHANGE (v2.0.5):***
>
> - *BCP consumed by BF → Appears ONLY in `bf.bcps[]`, NOT as independent timeline node*
> - *BSP consumed by BPP → Appears ONLY in `bpp.anchor_bsp`, NOT as independent timeline node*
> - *This eliminates duplication and provides cleaner chain structure*

Timeline Overview (2 BF Nodes)

Seq	Type	Time Range	Description
0	BF	06:00:00 - 06:00:05	SSH Brute Force (5 BCP embedded, 1 BSP in BPP)
1	BF	06:01:00 - 06:01:03	Privilege Escalation (3 BCP embedded, 1 BSP in BPP)

Phase 1: SSH Brute Force Attack

BF Node (seq: 0)

Field	Value
Type	**BF**
BF ID	`bf-a1b2c3d4-e5f6-7890-1234-567890abcdef`
Time Range	06:00:00 - 06:00:05 UTC (5 seconds)
BFL	**3 (HIGH)**

MITRE ATT&CK Mapping

Field	Value
attack_family	CREDENTIAL_ACCESS
attack_stage	TA0006
attack_tags	`bruteforce`, `high_fail`, `mitre:T1110.001`, `external_source`
technique_id	T1110.001
technique_name	Brute Force: Password Guessing
confidence	0.95

BFL Explain

```
{
  "action_id": "AUTH",
  "base_score": 10,
  "attempt_count": 5,
  "has_external_ip": true,
  "time_window_seconds": 5,
  "final_score": 90
}
```

Embedded BCPs (bf.bcps[])

> *These BCPs are consumed by this BF and do NOT appear as independent timeline nodes.*

Log ID	Event Type	Time	Source IP	Dest IP	User	Action	Result
1001	ssh_login	06:00:00	203.0.113.50	10.0.0.5	root	login	**failure**
1002	ssh_login	06:00:01	203.0.113.50	10.0.0.5	root	login	**failure**
1003	ssh_login	06:00:02	203.0.113.50	10.0.0.5	root	login	**failure**
1004	ssh_login	06:00:03	203.0.113.50	10.0.0.5	root	login	**failure**
1005	ssh_login	06:00:04	203.0.113.50	10.0.0.5	root	login	**failure**

Embedded BPP (bf.bpps[])

Field	Value
BPP ID	`bpp-e5f6-7890-1234-567890abcdef`
PTI	**0.92**
Evidence Log IDs	[1001, 1002, 1003, 1004, 1005]

Anchor BSP (bpp.anchor_bsp)

> *This BSP is consumed by this BPP and does NOT appear as independent timeline node.*

Field	Value
Log ID	1006
Event Type	ssh_login
BSP Type	auth_success
Time	06:00:05
Source IP	203.0.113.50
Dest IP	10.0.0.5
User	root
Action	login
Result	**success**

PTI Explain

```
{
  "base_score": 0.5,
  "failed_attempts_before_success": 5,
  "time_window_seconds": 5,
  "source_ip": "203.0.113.50",
  "target_user": "root",
  "is_external_ip": true,
  "pti_raw": 0.85,
  "source_weight": 1.08,
  "pti_final": 0.92
}
```

Bindings (Chain Restorability)

Binding	Value
member_bcp_log_ids	[1001, 1002, 1003, 1004, 1005]
derived_bpp_id	`bpp-e5f6-7890-1234-567890abcdef`
anchor_bsp_log_id	1006

Phase 2: Privilege Escalation

BF Node (seq: 1)

Field	Value
Type	**BF**
BF ID	`bf-b2c3d4e5-f6a7-8901-2345-67890abcdef0`
Time Range	06:01:00 - 06:01:03 UTC (3 seconds)
BFL	**2 (MEDIUM)**

MITRE ATT&CK Mapping

Field	Value
attack_family	PRIVILEGE_ESCALATION
attack_stage	TA0004
attack_tags	`privilege_escalation`, `elevation`, `mitre:T1548`
technique_id	T1548
technique_name	Abuse Elevation Control Mechanism
confidence	0.88

BFL Explain

```json
{
  "action_id": "PRIV_ESC",
  "base_score": 30,
  "attempt_count": 3,
  "is_sudo": true,
  "final_score": 65
}
```

Embedded BCPs (bf.bcps[])

> *These BCPs are consumed by this BF and do NOT appear as independent timeline nodes.*

Log ID	Event Type	Time	Source IP	Dest IP	User	Action	Result
2001	sudo	06:01:00	10.0.0.5	10.0.0.5	root	sudo_exec	**failure**
2002	sudo	06:01:01	10.0.0.5	10.0.0.5	root	sudo_exec	**failure**
2003	sudo	06:01:02	10.0.0.5	10.0.0.5	root	sudo_exec	**failure**

Embedded BPP (bf.bpps[])

Field	Value
BPP ID	`bpp-f6a7-8901-2345-67890abcdef0`
PTI	**0.78**
Evidence Log IDs	[2001, 2002, 2003]

Anchor BSP (bpp.anchor_bsp)

> *This BSP is consumed by this BPP and does NOT appear as independent timeline node.*

Field	Value
Log ID	2004
Event Type	sudo
BSP Type	privilege_success
Time	06:01:03
Source IP	10.0.0.5
Dest IP	10.0.0.5
User	root
Action	sudo_exec
Result	**success**

PTI Explain

```json
{
  "base_score": 0.4,
  "failed_attempts_before_success": 3,
  "time_window_seconds": 3,
  "is_sudo": true,
  "command": "sudo su -",
  "is_privilege_escalation": true,
  "pti_raw": 0.72,
  "source_weight": 1.08,
  "pti_final": 0.78
}
```

Bindings (Chain Restorability)

Binding	Value
member_bcp_log_ids	[2001, 2002, 2003]
derived_bpp_id	`bpp-f6a7-8901-2345-67890abcdef0`
anchor_bsp_log_id	2004

MITRE ATT&CK Mapping Summary

BF	Attack Family	Tactic	Technique
bf-a1b2…	CREDENTIAL_ACCESS	TA0006 (Credential Access)	T1110.001 (Brute Force: Password Guessing)
bf-b2c3…	PRIVILEGE_ESCALATION	TA0004 (Privilege Escalation)	T1548 (Abuse Elevation Control Mechanism)

---

v2.0.5 Report Structure Reference

Key Semantic Constraints

1. **Chain nodes are ONLY: BCP, BSP, BF** - But consumed BCP/BSP are embedded, not independent
2. **BCP consumed by BF** → `bf.bcps[]` (full detail, not just log_id)
3. **BSP consumed by BPP** → `bpp.anchor_bsp` (full detail, not just log_id)
4. **BPP is NOT a chain node** - Embedded in BF as explanation
5. **PTI only exists in BPP**, never in BF
6. **Attack mapping belongs to BF** - attack_family, attack_stage, attack_tags, attack_explain

Type Definitions (v2.0.5)

```go
// BCPViewV2 represents BCP details embedded in BF
type BCPViewV2 struct {
    LogID     int64  `json:"log_id"`
    EventType string `json:"event_type"`
    TMs       int64  `json:"t_ms"`
    SrcIP     string `json:"src_ip,omitempty"`
    DstIP     string `json:"dst_ip,omitempty"`
    UserName  string `json:"user_name,omitempty"`
    Action    string `json:"action,omitempty"`
    Result    string `json:"result"` // "failure" for BCP
}

// BSPViewV2 represents BSP details embedded in BPP
type BSPViewV2 struct {
    LogID     int64  `json:"log_id"`
    EventType string `json:"event_type"`
    BSPType   string `json:"bsp_type,omitempty"`
    TMs       int64  `json:"t_ms"`
    SrcIP     string `json:"src_ip,omitempty"`
    DstIP     string `json:"dst_ip,omitempty"`
    UserName  string `json:"user_name,omitempty"`
    Action    string `json:"action,omitempty"`
    Result    string `json:"result"` // "success" for BSP
}

// BFViewV2 now includes bcps[] for embedded BCP details
type BFViewV2 struct {
    // ... existing fields ...
    BCPs []BCPViewV2 `json:"bcps,omitempty"` // v2.0.5: Embedded BCP details
}

// BPPViewV2 now includes anchor_bsp for embedded BSP details
type BPPViewV2 struct {
    // ... existing fields ...
    AnchorBSP *BSPViewV2 `json:"anchor_bsp,omitempty"` // v2.0.5: Embedded BSP details
}
```

Report Generated by: ChainForge Security Analysis System v2.0.5
Report Schema: ReportV2 (Full Chain Restorability + Timeline Structure Fix)
Classification: CONFIDENTIAL - Internal Use Only