Behavior Analysis Report (ReportPayload v1)

Meta

Field	Value
Chain ID	`chain-ent-usr123-win24h-1706086400000`
Chain Revision	2
Entity ID	`user-jsmith-prod-01`
Window Start	2024-01-23 00:00:00 UTC (1706000000000)
Window End	2024-01-24 00:00:00 UTC (1706086400000)
Generated At	2024-01-24 01:06:40 UTC (1706090000000)

Policy Versions (inputs_snapshot)

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

Seq 0: BF - ssh_login_attempt (BFL: 3 HIGH)

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

bf_object

Field	Value
bf_id	`bf_0`
action	ssh_login_attempt
bfl	3 (HIGH)
start_ms	1674453600000
end_ms	1674453605000
event_count	6
is_anomalous	true
bf_attack_family	**CREDENTIAL_ACCESS**
bf_attack_stage	**TA0006**
bf_attack_tags	`["bruteforce", "high_fail", "mitre:T1110.001", "external_source"]`

bf_annotations

Field	Value
anomaly_tags	`["anomaly:high_attempt_count", "anomaly:external_ip"]`
anomaly_score	85.0

bpp_events[0]

Field	Value
bpp_id	`bpp-e5f6-7890-1234-567890abcdef`
transition_type	auth_success
anchor_bsp_id	`evt_006`
pti	**0.92**

supporting_stats:

Key	Value
fail_count	5
time_window_seconds	5
unique_source_ips	1
source_ip	203.0.113.50
target_user	root

transition_flags:

Code	Title	Severity	Rule ID
`bpp:pti_high`	High PTI Score	HIGH	pti_threshold_high
`bpp:external_ip`	External IP Source	MEDIUM	external_ip_check

evidence_refs: `["evt_001", "evt_002", "evt_003", "evt_004", "evt_005"]`

node_flags

Code	Title	Severity	Rule ID
`bf:bfl_high`	High Risk Behavior Fragment	HIGH	bfl_threshold
`bf:anomaly_detected`	Anomaly Detected	MEDIUM	anomaly_detection

evidence_refs: `["evt_001", "evt_002", "evt_003", "evt_004", "evt_005", "evt_006"]`

Seq 1: BF - sudo_attempt (BFL: 2 MEDIUM)

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

bf_object

Field	Value
bf_id	`bf_1`
action	sudo_attempt
bfl	2 (MEDIUM)
start_ms	1674453660000
end_ms	1674453663000
event_count	4
is_anomalous	false
bf_attack_family	**PRIVILEGE_ESCALATION**
bf_attack_stage	**TA0004**
bf_attack_tags	`["privilege_escalation", "elevation", "mitre:T1548"]`

bf_annotations

Field	Value
anomaly_tags	`[]`
anomaly_score	0.0

bpp_events[0]

Field	Value
bpp_id	`bpp-f6a7-8901-2345-67890abcdef0`
transition_type	priv_esc_success
anchor_bsp_id	`evt_010`
pti	**0.78**

supporting_stats:

Key	Value
fail_count	3
time_window_seconds	3
is_sudo	true
command	sudo su -

transition_flags:

Code	Title	Severity	Rule ID
`bpp:pti_medium`	Medium PTI Score	MEDIUM	pti_threshold_medium
`bpp:priv_esc`	Privilege Escalation Detected	HIGH	priv_esc_check

evidence_refs: `["evt_007", "evt_008", "evt_009"]`

node_flags

Code	Title	Severity	Rule ID
`bf:bfl_medium`	Medium Risk Behavior Fragment	MEDIUM	bfl_threshold

evidence_refs: `["evt_007", "evt_008", "evt_009", "evt_010"]`

Hotspots

Hotspot 1: BFL_ESCALATION

Field	Value
hotspot_type	BFL_ESCALATION
seq_range	[0, 1]
reason_tags	`["bfl_escalation", "progressive_behavior"]`
evidence_refs	`["bf_0", "bf_1"]`
severity	**HIGH**

Hotspot 2: TRANSITION_CLUSTER

Field	Value
hotspot_type	TRANSITION_CLUSTER
seq_range	[0, 1]
reason_tags	`["transition_cluster", "rapid_transitions"]`
evidence_refs	`["bpp-e5f6-...", "bpp-f6a7-..."]`
severity	**MEDIUM**

Reviews

ai_review

Field	Value
decision	escalate
confidence	0.45 (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

Field	Value
verdict	confirmed_threat
confidence	95
summary	Confirmed brute force attack followed by privilege escalation. Attacker gained root access. Recommend immediate incident response.

Audit Trail

Field	Value
ai_queue_id	`aiq-001-ssh-brute`
human_queue_id	`hq-001-escalated`
reviewers	`["analyst-042"]`

Timestamps

Event	Timestamp
generated_at	1706090000000 (2024-01-24 01:06:40 UTC)
ai_reviewed_at	1706091000000 (2024-01-24 01:23:20 UTC)
human_reviewed_at	1706095000000 (2024-01-24 02:30:00 UTC)

MITRE ATT&CK Mapping Summary

BF	Attack Family	Attack Stage (Tactic)	Technique Tags
bf_0	CREDENTIAL_ACCESS	TA0006 (Credential Access)	T1110.001 (Brute Force: Password Guessing)
bf_1	PRIVILEGE_ESCALATION	TA0004 (Privilege Escalation)	T1548 (Abuse Elevation Control Mechanism)

Report Structure Reference

This report follows the `ReportPayload` structure defined in `internal/contract/report_types.go`:

```
type ReportPayload struct {
    Meta       ReportMeta      `json:"meta"`
    Timeline   []ReportNode    `json:"timeline"`   // BF nodes in sequence
    Hotspots   []ReportHotspot `json:"hotspots"`   // Chain-level
aggregations
    Reviews    ReportReviews   `json:"reviews"`    // AI/Human review
summaries
    AuditTrail ReportAudit     `json:"audit_trail"`
}
```

Key Semantic Constraints

1. **Timeline contains only BF nodes** (not BCP/BSP directly)
2. **BF contains bf_object with attack mapping** (bf_attack_family, bf_attack_stage, bf_attack_tags)
3. **BPP is embedded in BF as bpp_events[]** (not a separate timeline node)
4. **PTI belongs to BPP**, not BF
5. **Flags are generated by Evaluator** based on policy rules

---

Report Generated by: ChainForge Security Analysis System v2.0.3
Report Schema: ReportPayload v1 (report_types.go)
Classification: CONFIDENTIAL - Internal Use Only