DeepTempo AI SOC - Overall Report

Report Generated:	2026-01-10 14:29:27
Total Findings:	50
Total Cases:	3

Executive Summary

Severity	Count	Percentage
Critical	0	0.0%
High	20	40.0%
Medium	23	46.0%
Low	7	14.0%

Cases Summary

Case ID	Title	Status	Priority	Findings
case-2026-01-10-38c5453	Investigation: c-beaconing-001	new	high	5
case-2026-01-10-a662bd02	Investigation: c-beaconing-001	new	high	5
case-2026-01-10-1f8d8961	Investigation: c-beaconing-001	new	high	5

Findings Detail

Finding 1: f-20260109-40d9379b

Field	Value
Finding ID	f-20260109-40d9379b
Timestamp	2026-01-09T19:17:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.823
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	55014
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.87), T1573.001 (0.57)

Finding 2: f-20260109-4a6c1b8b

Field	Value
Finding ID	f-20260109-4a6c1b8b
Timestamp	2026-01-09T19:24:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.642
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.2.10
Entity: query_name	af942af07dea.suspicious-domain.com
Entity: query_type	A
Entity: hostname	server-db-01
MITRE Techniques	T1071.004 (0.90), T1048.003 (0.62)

Finding 3: f-20260109-137ca4a8

Field	Value
Finding ID	f-20260109-137ca4a8
Timestamp	2026-01-09T19:33:55.046656Z
Severity	medium
Data Source	waf
Anomaly Score	0.938

Cluster ID	
Entity: src_ip	203.0.113.50
Entity: dst_ip	10.0.2.10
Entity: method	PUT
Entity: uri	/data/export
Entity: status_code	403
MITRE Techniques	T1190 (0.89), T1059.001 (0.51)

Finding 4: f-20260109-0963afc2

Field	Value
Finding ID	f-20260109-0963afc2
Timestamp	2026-01-09T19:54:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.614
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.15
Entity: query_name	634b12607569.suspicious-domain.com
Entity: query_type	A
Entity: hostname	server-db-01
MITRE Techniques	T1071.004 (0.89), T1048.003 (0.41)

Finding 5: f-20260109-02e111cb

Field	Value
Finding ID	f-20260109-02e111cb
Timestamp	2026-01-09T20:14:55.046656Z
Severity	high
Data Source	waf
Anomaly Score	0.895
Cluster ID	
Entity: src_ip	198.51.100.25
Entity: dst_ip	10.0.2.33
Entity: method	POST
Entity: uri	/api/upload
Entity: status_code	403
MITRE Techniques	T1190 (0.92), T1059.001 (0.49)

Finding 6: f-20260109-f6136639

Field	Value
Finding ID	f-20260109-f6136639
Timestamp	2026-01-09T20:15:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.851
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	50485
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.93), T1573.001 (0.52)

Finding 7: f-20260109-0aac1189

Field	Value
Finding ID	f-20260109-0aac1189
Timestamp	2026-01-09T20:19:55.046656Z
Severity	low
Data Source	flow
Anomaly Score	0.392
Cluster ID	
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.100
Entity: hostname	server-web-02
MITRE Techniques	T1041 (0.38)

Finding 8: f-20260109-cec39aee

Field	Value
Finding ID	f-20260109-cec39aee
Timestamp	2026-01-09T20:24:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.809
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.2.10
Entity: query_name	84dfd30ab31b.suspicious-domain.com
Entity: query_type	A

Entity: hostname	workstation-042
MITRE Techniques	T1071.004 (0.88), T1048.003 (0.57)

Finding 9: f-20260109-8c6ba7bb

Field	Value
Finding ID	f-20260109-8c6ba7bb
Timestamp	2026-01-09T20:52:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.798
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.15
Entity: query_name	1cc44c13d62a.api-service.io
Entity: query_type	A
Entity: hostname	laptop-sales-03
MITRE Techniques	T1071.004 (0.76), T1048.003 (0.64)

Finding 10: f-20260109-95865c6d

Field	Value
Finding ID	f-20260109-95865c6d
Timestamp	2026-01-09T21:16:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.640
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.15
Entity: query_name	c19d7ee2bad8.suspicious-domain.com
Entity: query_type	A
Entity: hostname	server-db-01
MITRE Techniques	T1071.004 (0.79), T1048.003 (0.61)

Finding 11: f-20260109-60968929

Field	Value
Finding ID	f-20260109-60968929
Timestamp	2026-01-09T21:17:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.918
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	55544
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.93), T1573.001 (0.55)

Finding 12: f-20260109-445da0ed

Field	Value
Finding ID	f-20260109-445da0ed
Timestamp	2026-01-09T21:54:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.802
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.22
Entity: query_name	13946a41625b.data-sync.org
Entity: query_type	A
Entity: hostname	server-db-01
MITRE Techniques	T1071.004 (0.74), T1048.003 (0.47)

Finding 13: f-20260109-198c6b99

Field	Value
Finding ID	f-20260109-198c6b99
Timestamp	2026-01-09T22:17:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.868
Cluster ID	c-beaconing-001

Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	50596
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.93), T1573.001 (0.59)

Finding 14: f-20260109-7dafeb89

Field	Value
Finding ID	f-20260109-7dafeb89
Timestamp	2026-01-09T22:21:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.705
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.15
Entity: query_name	152fe0dafd3b.data-sync.org
Entity: query_type	A
Entity: hostname	workstation-042
MITRE Techniques	T1071.004 (0.74), T1048.003 (0.58)

Finding 15: f-20260109-8a4f8f7e

Field	Value
Finding ID	f-20260109-8a4f8f7e
Timestamp	2026-01-09T22:53:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.678
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.2.33
Entity: query_name	8bc77866d9bf.data-sync.org
Entity: query_type	TXT
Entity: hostname	laptop-sales-03
MITRE Techniques	T1071.004 (0.73), T1048.003 (0.62)

Finding 16: f-20260109-287b98ca

Field	Value
Finding ID	f-20260109-287b98ca

Timestamp	2026-01-09T23:14:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.849
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.2.33
Entity: query_name	068be65663d6.cdn-update.net
Entity: query_type	TXT
Entity: hostname	server-db-01
MITRE Techniques	T1071.004 (0.73), T1048.003 (0.63)

Finding 17: f-20260109-65b5976d

Field	Value
Finding ID	f-20260109-65b5976d
Timestamp	2026-01-09T23:17:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.852
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	52069
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.90), T1573.001 (0.69)

Finding 18: f-20260109-125e8ed4

Field	Value
Finding ID	f-20260109-125e8ed4
Timestamp	2026-01-09T23:44:55.046656Z
Severity	medium
Data Source	dns
Anomaly Score	0.719
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.2.33
Entity: query_name	f2033e0fccdf.cdn-update.net
Entity: query_type	A
Entity: hostname	server-web-02

MITRE Techniques	T1071.004 (0.76), T1048.003 (0.40)

Finding 19: f-20260109-2b1ebefe

Field	Value
Finding ID	f-20260109-2b1ebefe
Timestamp	2026-01-09T23:44:55.046656Z
Severity	low
Data Source	dns
Anomaly Score	0.328
Cluster ID	
Entity: src_ip	10.0.1.15
Entity: dst_ip	None
Entity: hostname	workstation-042
MITRE Techniques	T1018 (0.37)

Finding 20: f-20260110-02f2f632

Field	Value
Finding ID	f-20260110-02f2f632
Timestamp	2026-01-10T00:14:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.878
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	57428
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.89), T1573.001 (0.60)

Finding 21: f-20260110-9753aff9

Field	Value
Finding ID	f-20260110-9753aff9
Timestamp	2026-01-10T00:43:55.046656Z
Severity	high
Data Source	waf
Anomaly Score	0.761
Cluster ID	
Entity: src_ip	198.51.100.25
Entity: dst_ip	10.0.2.33
Entity: method	POST
Entity: uri	/admin/config
Entity: status_code	500
MITRE Techniques	T1190 (0.82), T1059.001 (0.53)

Finding 22: f-20260110-9bcbd0d6

Field	Value
Finding ID	f-20260110-9bcbd0d6
Timestamp	2026-01-10T01:09:55.046656Z
Severity	medium
Data Source	waf
Anomaly Score	0.862
Cluster ID	
Entity: src_ip	198.51.100.25
Entity: dst_ip	10.0.2.33
Entity: method	POST
Entity: uri	/api/upload
Entity: status_code	403
MITRE Techniques	T1190 (0.93), T1059.001 (0.42)

Finding 23: f-20260110-277d6f70

Field	Value
Finding ID	f-20260110-277d6f70
Timestamp	2026-01-10T01:14:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.892

Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	59003
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.91), T1573.001 (0.57)

Finding 24: f-20260110-8aa19816

Field	Value
Finding ID	f-20260110-8aa19816
Timestamp	2026-01-10T02:19:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.833
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	51725
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.84), T1573.001 (0.67)

Finding 25: f-20260110-a0b1b3ec

Field	Value
Finding ID	f-20260110-a0b1b3ec
Timestamp	2026-01-10T03:17:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.892
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	53984
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.84), T1573.001 (0.57)

Finding 26: f-20260110-8f22bfc9

Field	Value
Finding ID	f-20260110-8f22bfc9
Timestamp	2026-01-10T03:59:55.046656Z
Severity	low
Data Source	waf
Anomaly Score	0.528
Cluster ID	
Entity: src_ip	10.0.1.45
Entity: dst_ip	198.51.100.25
Entity: hostname	laptop-sales-03
MITRE Techniques	T1048.003 (0.40)

Finding 27: f-20260110-81131297

Field	Value
Finding ID	f-20260110-81131297
Timestamp	2026-01-10T04:18:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.910
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	59017
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.94), T1573.001 (0.64)

Finding 28: f-20260110-d5380ad1

Field	Value
Finding ID	f-20260110-d5380ad1
Timestamp	2026-01-10T05:16:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.841
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15

Entity: dst_ip	203.0.113.50
Entity: src_port	54327
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.95), T1573.001 (0.65)

Finding 29: f-20260110-f10e080a

Field	Value
Finding ID	f-20260110-f10e080a
Timestamp	2026-01-10T06:03:55.046656Z
Severity	low
Data Source	waf
Anomaly Score	0.476
Cluster ID	
Entity: src_ip	10.0.2.33
Entity: dst_ip	203.0.113.50
Entity: hostname	workstation-042
MITRE Techniques	T1048.003 (0.51)

Finding 30: f-20260110-5bf88b52

Field	Value
Finding ID	f-20260110-5bf88b52
Timestamp	2026-01-10T06:18:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.858
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	50225
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.84), T1573.001 (0.58)

Finding 31: f-20260110-8d98d5f9

Field	Value
Finding ID	f-20260110-8d98d5f9
Timestamp	2026-01-10T07:06:55.046656Z
Severity	medium
Data Source	flow
Anomaly Score	0.792
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	10.0.2.10
Entity: src_port	54056
Entity: dst_port	5985
Entity: hostname	workstation-042
MITRE Techniques	T1021.002 (0.79), T1018 (0.60)

Finding 32: f-20260110-0a5ec3fb

Field	Value
Finding ID	f-20260110-0a5ec3fb
Timestamp	2026-01-10T07:14:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.892
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	59935
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.81), T1573.001 (0.53)

Finding 33: f-20260110-355903d5

Field	Value
Finding ID	f-20260110-355903d5
Timestamp	2026-01-10T08:02:55.046656Z
Severity	medium
Data Source	flow
Anomaly Score	0.733

Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.45
Entity: dst_ip	10.0.2.10
Entity: src_port	55773
Entity: dst_port	3389
Entity: hostname	server-db-01
MITRE Techniques	T1018 (0.75), T1021.002 (0.67)

Finding 34: f-20260110-5eeb60f6

Field	Value
Finding ID	f-20260110-5eeb60f6
Timestamp	2026-01-10T08:19:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.942
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	54585
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.85), T1573.001 (0.65)

Finding 35: f-20260110-ba05be55

Field	Value
Finding ID	f-20260110-ba05be55
Timestamp	2026-01-10T08:46:55.046656Z
Severity	medium
Data Source	waf
Anomaly Score	0.890
Cluster ID	
Entity: src_ip	203.0.113.100
Entity: dst_ip	10.0.2.33
Entity: method	POST
Entity: uri	/api/execute
Entity: status_code	200
MITRE Techniques	T1190 (0.86), T1059.001 (0.56)

Finding 36: f-20260110-3e0306b0

Field	Value
Finding ID	f-20260110-3e0306b0
Timestamp	2026-01-10T09:13:55.046656Z
Severity	medium
Data Source	flow
Anomaly Score	0.600
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	10.0.2.10
Entity: src_port	59545
Entity: dst_port	445
Entity: hostname	workstation-055
MITRE Techniques	T1021.002 (0.74), T1018 (0.59)

Finding 37: f-20260110-45414e82

Field	Value
Finding ID	f-20260110-45414e82
Timestamp	2026-01-10T09:19:55.046656Z
Severity	high
Data Source	flow
Anomaly Score	0.839
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	54030
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.93), T1573.001 (0.58)

Finding 38: f-20260110-4dc87459

Field	Value
Finding ID	f-20260110-4dc87459
Timestamp	2026-01-10T09:41:55.046656Z
Severity	high
Data Source	waf
Anomaly Score	0.860

Cluster ID	
Entity: src_ip	198.51.100.10
Entity: dst_ip	10.0.2.33
Entity: method	GET
Entity: uri	/api/upload
Entity: status_code	500
MITRE Techniques	T1190 (0.87), T1059.001 (0.37)

Finding 39: f-20260110-8bcdb33a

Field	Value
Finding ID	f-20260110-8bcdb33a
Timestamp	2026-01-10T09:49:55.046656Z
Severity	low
Data Source	flow
Anomaly Score	0.307
Cluster ID	
Entity: src_ip	10.0.2.10
Entity: dst_ip	198.51.100.10
Entity: hostname	server-db-01
MITRE Techniques	T1190 (0.36)

Finding 40: f-20260110-1d88684b

Field	Value
Finding ID	f-20260110-1d88684b
Timestamp	2026-01-10T09:56:55.046656Z
Severity	medium
Data Source	flow
Anomaly Score	0.693
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	10.0.2.10
Entity: src_port	59667
Entity: dst_port	5985
Entity: hostname	workstation-042
MITRE Techniques	T1018 (0.75), T1021.002 (0.70)

Finding 41: f-20260110-4d2fe86d

Field	Value
Finding ID	f-20260110-4d2fe86d
Timestamp	2026-01-10T10:04:55.046656Z
Severity	medium
Data Source	waf
Anomaly Score	0.742
Cluster ID	
Entity: src_ip	198.51.100.10
Entity: dst_ip	10.0.2.33
Entity: method	PUT
Entity: uri	/data/export
Entity: status_code	500
MITRE Techniques	T1190 (0.93), T1059.001 (0.54)

Finding 42: f-20260110-ca7143fd

Field	Value
Finding ID	f-20260110-ca7143fd
Timestamp	2026-01-10T10:24:55.046656Z
Severity	high
Data Source	waf
Anomaly Score	0.948
Cluster ID	
Entity: src_ip	198.51.100.25
Entity: dst_ip	10.0.2.10
Entity: method	PUT
Entity: uri	/data/export
Entity: status_code	200
MITRE Techniques	T1190 (0.91), T1059.001 (0.57)

Finding 43: f-20260110-4a9a956d

Field	Value
Finding ID	f-20260110-4a9a956d
Timestamp	2026-01-10T10:38:55.046656Z
Severity	low
Data Source	waf
Anomaly Score	0.503

Cluster ID	
Entity: src_ip	10.0.1.15
Entity: dst_ip	198.51.100.25
Entity: hostname	laptop-sales-03
MITRE Techniques	T1572 (0.36)

Finding 44: f-20260110-ad533d01

Field	Value
Finding ID	f-20260110-ad533d01
Timestamp	2026-01-10T11:56:55.046656Z
Severity	medium
Data Source	flow
Anomaly Score	0.833
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	10.0.2.10
Entity: src_port	53305
Entity: dst_port	3389
Entity: hostname	workstation-055
MITRE Techniques	T1021.002 (0.71), T1018 (0.55)

Finding 45: f-20260110-83ddd090

Field	Value
Finding ID	f-20260110-83ddd090
Timestamp	2026-01-10T12:25:55.046656Z
Severity	medium
Data Source	flow
Anomaly Score	0.761
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.45
Entity: dst_ip	10.0.2.10
Entity: src_port	53923
Entity: dst_port	3389
Entity: hostname	workstation-055
MITRE Techniques	T1021.002 (0.81), T1018 (0.49)

Finding 46: f-20260110-6fc7af44

Field	Value

Finding ID	f-20260110-6fc7af44
Timestamp	2026-01-10T12:41:55.046656Z
Severity	medium
Data Source	flow
Anomaly Score	0.741
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.45
Entity: dst_ip	10.0.2.33
Entity: src_port	51376
Entity: dst_port	445
Entity: hostname	workstation-042
MITRE Techniques	T1021.002 (0.87), T1018 (0.65)

Finding 47: f-20260110-202be353

Field	Value
Finding ID	f-20260110-202be353
Timestamp	2026-01-10T13:58:55.046656Z
Severity	medium
Data Source	flow
Anomaly Score	0.610
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	10.0.2.10
Entity: src_port	52339
Entity: dst_port	3389
Entity: hostname	workstation-055
MITRE Techniques	T1021.002 (0.82), T1018 (0.66)

Finding 48: f-20260110-4274d137

Field	Value
Finding ID	f-20260110-4274d137
Timestamp	2026-01-10T14:23:55.046656Z
Severity	high
Data Source	waf
Anomaly Score	0.884
Cluster ID	
Entity: src_ip	198.51.100.25
Entity: dst_ip	10.0.2.33

Entity: method	GET
Entity: uri	/api/execute
Entity: status_code	403
MITRE Techniques	T1190 (0.82), T1059.001 (0.44)

Finding 49: f-20260110-6db4f039

Field	Value
Finding ID	f-20260110-6db4f039
Timestamp	2026-01-10T14:33:55.046656Z
Severity	low
Data Source	dns
Anomaly Score	0.432
Cluster ID	
Entity: src_ip	10.0.1.45
Entity: dst_ip	None
Entity: hostname	server-db-01
MITRE Techniques	T1059.003 (0.54)

Finding 50: f-20260110-75d01137

Field	Value
Finding ID	f-20260110-75d01137
Timestamp	2026-01-10T15:49:55.046656Z
Severity	medium
Data Source	waf
Anomaly Score	0.856
Cluster ID	
Entity: src_ip	198.51.100.25
Entity: dst_ip	10.0.2.10
Entity: method	PUT
Entity: uri	/api/execute
Entity: status_code	403
MITRE Techniques	T1190 (0.82), T1059.001 (0.39)