DeepTempo AI SOC - Overall Report

Report Generated:	2026-01-11 09:42:37
Total Findings:	50
Total Cases:	4

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
case-2026-01-11-5d5c2798	Investigation: c-beaconing-001	new	high	5

Findings Detail

Finding 1: f-20260110-78841ca3

Field	Value
Finding ID	f-20260110-78841ca3
Timestamp	2026-01-10T17:45:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.914
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	57239
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.83), T1573.001 (0.57)

Finding 2: f-20260110-cd2c6b08

Field	Value
Finding ID	f-20260110-cd2c6b08
Timestamp	2026-01-10T17:46:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.796
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.2.33
Entity: query_name	53d00aaa3f8c.api-service.io
Entity: query_type	A
Entity: hostname	server-db-01
MITRE Techniques	T1071.004 (0.82), T1048.003 (0.50)

Finding 3: f-20260110-18782990

Field	Value
Finding ID	f-20260110-18782990
Timestamp	2026-01-10T18:15:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.682

Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.15
Entity: query_name	eef5ecdbb2eb.data-sync.org
Entity: query_type	A
Entity: hostname	server-web-02
MITRE Techniques	T1071.004 (0.76), T1048.003 (0.49)

Finding 4: f-20260110-d8182d42

Field	Value
Finding ID	f-20260110-d8182d42
Timestamp	2026-01-10T18:27:34.465432Z
Severity	low
Data Source	waf
Anomaly Score	0.306
Cluster ID	
Entity: src_ip	10.0.1.45
Entity: dst_ip	198.51.100.25
Entity: hostname	laptop-sales-03
MITRE Techniques	T1048.001 (0.45)

Finding 5: f-20260110-52753eea

Field	Value
Finding ID	f-20260110-52753eea
Timestamp	2026-01-10T18:30:34.465432Z
Severity	low
Data Source	flow
Anomaly Score	0.526
Cluster ID	
Entity: src_ip	10.0.1.45
Entity: dst_ip	203.0.113.50
Entity: hostname	server-db-01
MITRE Techniques	T1071.004 (0.54)

Finding 6: f-20260110-7a2ec4af

Field	Value
Finding ID	f-20260110-7a2ec4af
Timestamp	2026-01-10T18:38:34.465432Z
Severity	high

Data Source	waf
Anomaly Score	0.925
Cluster ID	
Entity: src_ip	198.51.100.25
Entity: dst_ip	10.0.2.10
Entity: method	GET
Entity: uri	/api/upload
Entity: status_code	200
MITRE Techniques	T1190 (0.91), T1059.001 (0.55)

Finding 7: f-20260110-430f9447

Field	Value
Finding ID	f-20260110-430f9447
Timestamp	2026-01-10T18:40:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.767
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	59669
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.82), T1573.001 (0.56)

Finding 8: f-20260110-31601022

Field	Value
Finding ID	f-20260110-31601022
Timestamp	2026-01-10T18:43:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.687
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.22
Entity: query_name	842d677086b8.api-service.io
Entity: query_type	A
Entity: hostname	server-web-02
MITRE Techniques	T1071.004 (0.89), T1048.003 (0.58)

Finding 9: f-20260110-dbea12d6

Field	Value
Finding ID	f-20260110-dbea12d6
Timestamp	2026-01-10T19:20:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.749
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.22
Entity: query_name	9f74609000bb.cdn-update.net
Entity: query_type	A
Entity: hostname	server-web-02
MITRE Techniques	T1071.004 (0.79), T1048.003 (0.41)

Finding 10: f-20260110-eb6de471

Field	Value
Finding ID	f-20260110-eb6de471
Timestamp	2026-01-10T19:44:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.813
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	55628
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.82), T1573.001 (0.61)

Finding 11: f-20260110-1f31c9f0

Field	Value
Finding ID	f-20260110-1f31c9f0
Timestamp	2026-01-10T19:49:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.758
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.22
Entity: query_name	a0a8e221d542.cdn-update.net
Entity: query_type	A
Entity: hostname	workstation-055
MITRE Techniques	T1071.004 (0.77), T1048.003 (0.50)

Finding 12: f-20260110-45b9626c

Field	Value
Finding ID	f-20260110-45b9626c
Timestamp	2026-01-10T20:17:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.767
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.2.10
Entity: query_name	f3e0c5288024.api-service.io
Entity: query_type	TXT
Entity: hostname	laptop-sales-03
MITRE Techniques	T1071.004 (0.83), T1048.003 (0.64)

Finding 13: f-20260110-769abc4f

Field	Value
Finding ID	f-20260110-769abc4f
Timestamp	2026-01-10T20:44:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.946
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15

Entity: dst_ip	203.0.113.50
Entity: src_port	50659
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.93), T1573.001 (0.67)

Finding 14: f-20260110-2da7b8e7

Field	Value
Finding ID	f-20260110-2da7b8e7
Timestamp	2026-01-10T20:44:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.815
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.45
Entity: query_name	624040f35be4.api-service.io
Entity: query_type	TXT
Entity: hostname	laptop-sales-03
MITRE Techniques	T1071.004 (0.84), T1048.003 (0.61)

Finding 15: f-20260110-e1d69ac6

Field	Value
Finding ID	f-20260110-e1d69ac6
Timestamp	2026-01-10T21:11:34.465432Z
Severity	high
Data Source	waf
Anomaly Score	0.911
Cluster ID	
Entity: src_ip	203.0.113.100
Entity: dst_ip	10.0.2.10
Entity: method	GET
Entity: uri	/data/export
Entity: status_code	200
MITRE Techniques	T1190 (0.86), T1059.001 (0.35)

Finding 16: f-20260110-9977d78f

Field	Value
Finding ID	f-20260110-9977d78f

Timestamp	2026-01-10T21:14:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.750
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.15
Entity: query_name	98f15e5d2d76.cdn-update.net
Entity: query_type	TXT
Entity: hostname	laptop-sales-03
MITRE Techniques	T1071.004 (0.78), T1048.003 (0.57)

Finding 17: f-20260110-0f75a485

Field	Value
Finding ID	f-20260110-0f75a485
Timestamp	2026-01-10T21:41:34.465432Z
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	55465
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.82), T1573.001 (0.67)

Finding 18: f-20260110-18fd9d90

Field	Value
Finding ID	f-20260110-18fd9d90
Timestamp	2026-01-10T21:50:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.674
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.22
Entity: query_name	d2135a5640c8.api-service.io
Entity: query_type	TXT
Entity: hostname	workstation-042

MITRE Techniques	T1071.004 (0.87), T1048.003 (0.52)

Finding 19: f-20260110-f9e85046

Field	Value
Finding ID	f-20260110-f9e85046
Timestamp	2026-01-10T22:14:34.465432Z
Severity	medium
Data Source	dns
Anomaly Score	0.701
Cluster ID	c-dns-tunnel-001
Entity: src_ip	10.0.1.22
Entity: query_name	b2b93605e9ee.cdn-update.net
Entity: query_type	TXT
Entity: hostname	workstation-042
MITRE Techniques	T1071.004 (0.89), T1048.003 (0.53)

Finding 20: f-20260110-30aa3dec

Field	Value
Finding ID	f-20260110-30aa3dec
Timestamp	2026-01-10T22:43:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.768
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	56234
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.93), T1573.001 (0.66)

Finding 21: f-20260110-35bff064

Field	Value
Finding ID	f-20260110-35bff064
Timestamp	2026-01-10T23:40:34.465432Z
Severity	low
Data Source	waf
Anomaly Score	0.467
Cluster ID	
Entity: src_ip	10.0.1.22
Entity: dst_ip	203.0.113.100
Entity: hostname	workstation-042
MITRE Techniques	T1133 (0.31)

Finding 22: f-20260110-8d4c5769

Field	Value
Finding ID	f-20260110-8d4c5769
Timestamp	2026-01-10T23:42:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.817
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	56639
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.85), T1573.001 (0.56)

Finding 23: f-20260111-b30f9734

Field	Value
Finding ID	f-20260111-b30f9734
Timestamp	2026-01-11T00:44:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.935
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15

Entity: dst_ip	203.0.113.50
Entity: src_port	55050
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.81), T1573.001 (0.60)

Finding 24: f-20260111-85937ad2

Field	Value
Finding ID	f-20260111-85937ad2
Timestamp	2026-01-11T01:40:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.777
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	55722
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.89), T1573.001 (0.54)

Finding 25: f-20260111-bc3ce038

Field	Value
Finding ID	f-20260111-bc3ce038
Timestamp	2026-01-11T02:25:34.465432Z
Severity	medium
Data Source	waf
Anomaly Score	0.740
Cluster ID	
Entity: src_ip	198.51.100.10
Entity: dst_ip	10.0.2.10
Entity: method	PUT
Entity: uri	/admin/config
Entity: status_code	500
MITRE Techniques	T1190 (0.77), T1059.001 (0.32)

Finding 26: f-20260111-1bdeb67b

Field	Value

Finding ID	f-20260111-1bdeb67b
Timestamp	2026-01-11T02:43:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.814
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	50445
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.90), T1573.001 (0.66)

Finding 27: f-20260111-c068967b

Field	Value
Finding ID	f-20260111-c068967b
Timestamp	2026-01-11T02:51:34.465432Z
Severity	medium
Data Source	waf
Anomaly Score	0.916
Cluster ID	
Entity: src_ip	203.0.113.100
Entity: dst_ip	10.0.2.10
Entity: method	PUT
Entity: uri	/admin/config
Entity: status_code	403
MITRE Techniques	T1190 (0.88), T1059.001 (0.46)

Finding 28: f-20260111-0d634949

Field	Value
Finding ID	f-20260111-0d634949
Timestamp	2026-01-11T03:31:34.465432Z
Severity	low
Data Source	flow
Anomaly Score	0.488
Cluster ID	
Entity: src_ip	10.0.1.22
Entity: dst_ip	198.51.100.10

Entity: hostname	laptop-sales-03
MITRE Techniques	T1571 (0.48)

Finding 29: f-20260111-2274d27a

Field	Value
Finding ID	f-20260111-2274d27a
Timestamp	2026-01-11T03:32:34.465432Z
Severity	medium
Data Source	waf
Anomaly Score	0.783
Cluster ID	
Entity: src_ip	203.0.113.100
Entity: dst_ip	10.0.2.33
Entity: method	POST
Entity: uri	/data/export
Entity: status_code	403
MITRE Techniques	T1190 (0.87), T1059.001 (0.59)

Finding 30: f-20260111-be47c8d6

Field	Value
Finding ID	f-20260111-be47c8d6
Timestamp	2026-01-11T03:32:34.465432Z
Severity	medium
Data Source	flow
Anomaly Score	0.716
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.45
Entity: dst_ip	10.0.2.10
Entity: src_port	50833
Entity: dst_port	445
Entity: hostname	server-db-01
MITRE Techniques	T1021.002 (0.80), T1018 (0.71)

Finding 31: f-20260111-1392cfed

Field	Value
Finding ID	f-20260111-1392cfed
Timestamp	2026-01-11T03:34:34.465432Z
Severity	medium
Data Source	flow
Anomaly Score	0.668
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	10.0.2.10
Entity: src_port	52017
Entity: dst_port	5985
Entity: hostname	workstation-042
MITRE Techniques	T1021.002 (0.69), T1018 (0.69)

Finding 32: f-20260111-b013d2fa

Field	Value
Finding ID	f-20260111-b013d2fa
Timestamp	2026-01-11T03:43:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.822
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	52208
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.83), T1573.001 (0.70)

Finding 33: f-20260111-0a4f2677

Field	Value
Finding ID	f-20260111-0a4f2677
Timestamp	2026-01-11T04:18:34.465432Z
Severity	high
Data Source	waf
Anomaly Score	0.767

Cluster ID	
Entity: src_ip	203.0.113.100
Entity: dst_ip	10.0.2.33
Entity: method	PUT
Entity: uri	/api/upload
Entity: status_code	403
MITRE Techniques	T1190 (0.89), T1059.001 (0.51)

Finding 34: f-20260111-b185b979

Field	Value
Finding ID	f-20260111-b185b979
Timestamp	2026-01-11T04:43:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.845
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	59807
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.91), T1573.001 (0.55)

Finding 35: f-20260111-cb5962b4

Field	Value
Finding ID	f-20260111-cb5962b4
Timestamp	2026-01-11T05:42:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.844
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	53448
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.85), T1573.001 (0.58)

Finding 36: f-20260111-27b21171

Field	Value
Finding ID	f-20260111-27b21171
Timestamp	2026-01-11T05:53:34.465432Z
Severity	medium
Data Source	flow
Anomaly Score	0.731
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.22
Entity: dst_ip	10.0.2.10
Entity: src_port	54605
Entity: dst_port	5985
Entity: hostname	server-db-01
MITRE Techniques	T1021.002 (0.77), T1018 (0.64)

Finding 37: f-20260111-352e6b7a

Field	Value
Finding ID	f-20260111-352e6b7a
Timestamp	2026-01-11T06:11:34.465432Z
Severity	low
Data Source	flow
Anomaly Score	0.329
Cluster ID	
Entity: src_ip	10.0.1.15
Entity: dst_ip	198.51.100.10
Entity: hostname	laptop-sales-03
MITRE Techniques	T1048.003 (0.37)

Finding 38: f-20260111-e1a7b41a

Field	Value
Finding ID	f-20260111-e1a7b41a
Timestamp	2026-01-11T06:37:34.465432Z
Severity	high
Data Source	waf
Anomaly Score	0.801
Cluster ID	
Entity: src_ip	198.51.100.25

Entity: dst_ip	10.0.2.33
Entity: method	PUT
Entity: uri	/data/export
Entity: status_code	403
MITRE Techniques	T1190 (0.83), T1059.001 (0.47)

Finding 39: f-20260111-9cb57614

Field	Value
Finding ID	f-20260111-9cb57614
Timestamp	2026-01-11T06:42:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.889
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	59023
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.93), T1573.001 (0.63)

Finding 40: f-20260111-8ff4ae62

Field	Value
Finding ID	f-20260111-8ff4ae62
Timestamp	2026-01-11T07:09:34.465432Z
Severity	medium
Data Source	flow
Anomaly Score	0.788
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.45
Entity: dst_ip	10.0.2.10
Entity: src_port	57056
Entity: dst_port	3389
Entity: hostname	workstation-055
MITRE Techniques	T1021.002 (0.67), T1018 (0.60)

Finding 41: f-20260111-2e1903ee

Field	Value
Finding ID	f-20260111-2e1903ee
Timestamp	2026-01-11T07:43:34.465432Z
Severity	high
Data Source	flow
Anomaly Score	0.846
Cluster ID	c-beaconing-001
Entity: src_ip	10.0.1.15
Entity: dst_ip	203.0.113.50
Entity: src_port	55715
Entity: dst_port	443
Entity: hostname	workstation-042
MITRE Techniques	T1071.001 (0.88), T1573.001 (0.66)

Finding 42: f-20260111-34c3af46

Field	Value
Finding ID	f-20260111-34c3af46
Timestamp	2026-01-11T10:52:34.465432Z
Severity	low
Data Source	waf
Anomaly Score	0.400
Cluster ID	
Entity: src_ip	10.0.2.33
Entity: dst_ip	198.51.100.10
Entity: hostname	server-db-01
MITRE Techniques	T1133 (0.53)

Finding 43: f-20260111-3d33a64f

Field	Value
Finding ID	f-20260111-3d33a64f
Timestamp	2026-01-11T11:15:34.465432Z
Severity	medium
Data Source	flow
Anomaly Score	0.712
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.15

Entity: dst_ip	10.0.2.33
Entity: src_port	58377
Entity: dst_port	3389
Entity: hostname	server-db-01
MITRE Techniques	T1021.002 (0.79), T1018 (0.72)

Finding 44: f-20260111-4d7a26e5

Field	Value
Finding ID	f-20260111-4d7a26e5
Timestamp	2026-01-11T11:19:34.465432Z
Severity	low
Data Source	dns
Anomaly Score	0.500
Cluster ID	
Entity: src_ip	10.0.1.22
Entity: dst_ip	None
Entity: hostname	server-web-02
MITRE Techniques	T1059.003 (0.44)

Finding 45: f-20260111-014c6477

Field	Value
Finding ID	f-20260111-014c6477
Timestamp	2026-01-11T11:39:34.465432Z
Severity	medium
Data Source	flow
Anomaly Score	0.739
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.45
Entity: dst_ip	10.0.2.10
Entity: src_port	50779
Entity: dst_port	445
Entity: hostname	workstation-055
MITRE Techniques	T1021.002 (0.86), T1018 (0.52)

Finding 46: f-20260111-6d10ee4a

Field	Value
Finding ID	f-20260111-6d10ee4a
Timestamp	2026-01-11T12:13:34.465432Z

Severity	medium
Data Source	flow
Anomaly Score	0.823
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.22
Entity: dst_ip	10.0.2.10
Entity: src_port	58665
Entity: dst_port	5985
Entity: hostname	workstation-055
MITRE Techniques	T1021.002 (0.75), T1018 (0.56)

Finding 47: f-20260111-071f3b11

Field	Value
Finding ID	f-20260111-071f3b11
Timestamp	2026-01-11T12:14:34.465432Z
Severity	medium
Data Source	flow
Anomaly Score	0.752
Cluster ID	c-lateral-001
Entity: src_ip	10.0.1.22
Entity: dst_ip	10.0.2.33
Entity: src_port	53343
Entity: dst_port	3389
Entity: hostname	workstation-055
MITRE Techniques	T1021.002 (0.66), T1018 (0.46)

Finding 48: f-20260111-e06b5a30

Field	Value
Finding ID	f-20260111-e06b5a30
Timestamp	2026-01-11T12:40:34.465432Z
Severity	medium
Data Source	waf
Anomaly Score	0.815
Cluster ID	
Entity: src_ip	203.0.113.100
Entity: dst_ip	10.0.2.10
Entity: method	GET
Entity: uri	/api/execute

Entity: status_code	403
MITRE Techniques	T1190 (0.80), T1059.001 (0.56)

Finding 49: f-20260111-66106af2

Field	Value
Finding ID	f-20260111-66106af2
Timestamp	2026-01-11T17:22:34.465432Z
Severity	medium
Data Source	waf
Anomaly Score	0.917
Cluster ID	
Entity: src_ip	198.51.100.10
Entity: dst_ip	10.0.2.10
Entity: method	POST
Entity: uri	/data/export
Entity: status_code	500
MITRE Techniques	T1190 (0.94), T1059.001 (0.52)

Finding 50: f-20260111-0b21d416

Field	Value
Finding ID	f-20260111-0b21d416
Timestamp	2026-01-11T17:36:34.465432Z
Severity	high
Data Source	waf
Anomaly Score	0.844
Cluster ID	
Entity: src_ip	198.51.100.10
Entity: dst_ip	10.0.2.10
Entity: method	GET
Entity: uri	/api/upload
Entity: status_code	403
MITRE Techniques	T1190 (0.82), T1059.001 (0.48)