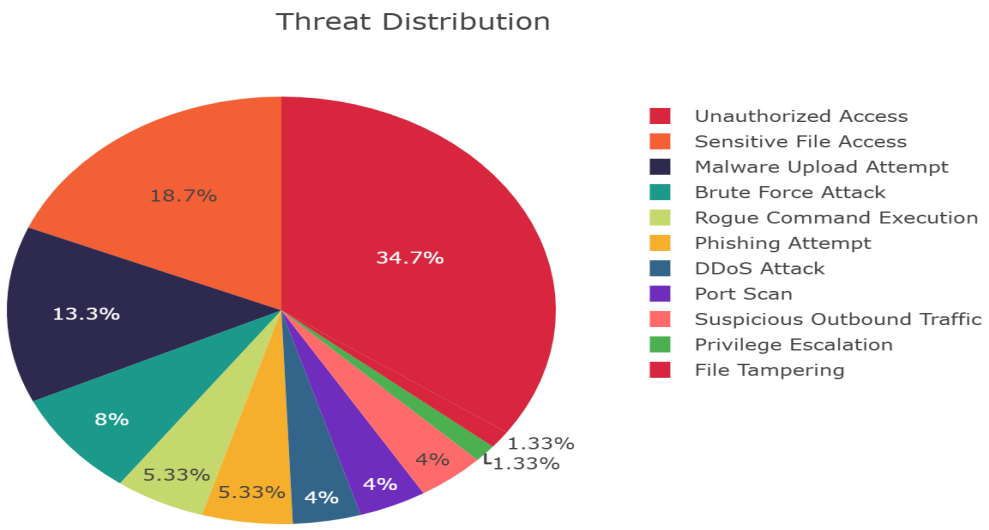
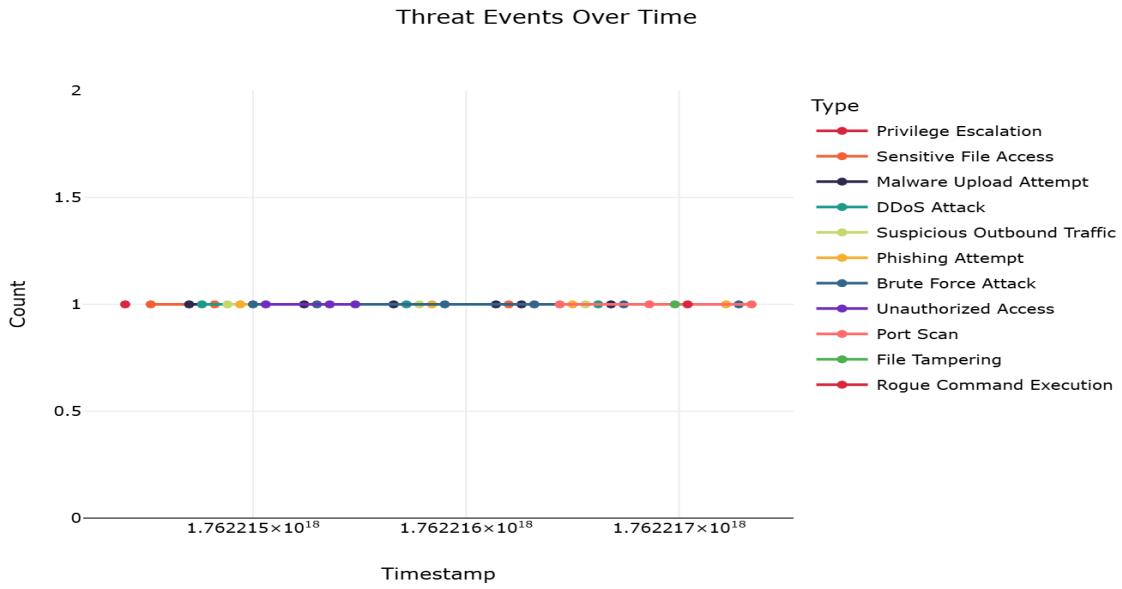
AWS Security Anomaly Report

Overview Charts





Threat Details & Logs

1. Brute Force Attack | Severity: Medium | Count: 6

- 2025-11-04T00:10:11Z Warning: Possible brute-force attempt detected from 203.0.113.11 attempts=12
- 2025-11-04T00:15:16Z Warning: Brute-force login suspected from 203.0.113.16 attempts=16
- 2025-11-04T00:25:26Z Brute force attempt 203.0.113.26 attempts=8
- 2025-11-04T00:32:33Z Brute force attempt 203.0.113.33 attempts=14
- 2025-11-04T00:39:40Z Brute force attempt 203.0.113.40
- 2025-11-04T00:48:49Z Brute force 203.0.113.49

2. DDoS Attack | Severity: Critical | Count: 3

- 2025-11-04T00:06:07Z Critical: DDoS attack detected from 203.0.113.7 pps=186133
- 2025-11-04T00:22:23Z Critical: DDoS detected 203.0.113.23 pps=157571
- 2025-11-04T00:37:38Z DDoS detected 203.0.113.38

3. File Tampering | Severity: Medium | Count: 1

- 2025-11-04T00:43:44Z Suspicious file overwrite /boot/grub.cfg 203.0.113.44

4. Malware Upload Attempt | Severity: High | Count: 10

- 2025-11-04T00:05:06Z Alert: Malware upload attempt: /uploads/invoice.exe from 203.0.113.6
- 2025-11-04T00:14:15Z Alert: Malware upload attempt: /var/www/index.php from 203.0.113.15
- 2025-11-04T00:21:22Z Alert: Malware upload: /uploads/configure.scr.exe from 203.0.113.22
- 2025-11-04T00:29:30Z Malware upload /boot/grub.cfg from 203.0.113.30
- 2025-11-04T00:31:32Z Unauthorized wget http://malware.xyz from 203.0.113.32
- 2025-11-04T00:38:39Z Malware upload suspicious 203.0.113.39
- '203.0.113.5 - admin [04/Nov/2025:00:00:15 +0000] "POST /upload HTTP/1.1" 401 - "curl/7.79.1"',■
- '192.168.3.33 - unknown [04/Nov/2025:00:10:59 +0000] "POST /upload HTTP/1.1" 415 0 "curl/7.58.0"',■
- '198.51.100.33 - service [04/Nov/2025:00:15:05 +0000] "POST /api/v1/upload HTTP/1.1" 500 12 "curl/7.64.1"',■
- '198.51.100.240 - - [04/Nov/2025:00:34:05 +0000] "POST /upload HTTP/1.1" 401 0 "curl/7.65.0"',■

5. Phishing Attempt | Severity: Medium | Count: 4

- 2025-11-04T00:09:10Z Alert: Phishing link distributed: http://fake-login.com from 203.0.113.10
- 2025-11-04T00:24:25Z Phishing link: http://secure-banking-login.com from 203.0.113.25
- 2025-11-04T00:35:36Z Phishing link http://secure-reset-password.com 203.0.113.36
- 2025-11-04T00:47:48Z Phishing link 203.0.113.48

6. Port Scan | Severity: Low | Count: 3

- 2025-11-04T00:34:35Z Port scan 203.0.113.35
- 2025-11-04T00:41:42Z Port scan 203.0.113.42
- 2025-11-04T00:49:50Z Port scan 203.0.113.50

7. Privilege Escalation | Severity: Critical | Count: 1

- 2025-11-04T00:00:01Z Alert: Privilege escalation attempt via sudo su root from 203.0.113.1

8. Rogue Command Execution | Severity: High | Count: 4

- 2025-11-04T00:44:45Z Critical: rm -rf logs executed by 203.0.113.45
- '198.51.100.78 - root [04/Nov/2025:00:06:14 +0000] "GET /admin HTTP/1.1" 200 3042 "curl/7.68.0"',■
- '198.51.100.155 - svc [04/Nov/2025:00:21:52 +0000] "POST /api/exec HTTP/1.1" 500 8 "curl/7.69.1"',■
- '198.51.100.210 - admin [04/Nov/2025:00:26:45 +0000] "GET /admin/credentials HTTP/1.1" 200 780 "curl/7.80.0"',■

9. Sensitive File Access | Severity: High | Count: 14

- 2025-11-04T00:02:03Z Alert: Restricted area access attempt: /root/keys from 203.0.113.3

- 2025-11-04T00:07:08Z Notice: Suspicious file modification /etc/passwd host=203.0.113.8
- 2025-11-04T00:30:31Z Suspicious modification /etc/passwd host=203.0.113.31
- '198.51.100.12 - root [04/Nov/2025:00:00:42 +0000] "GET /admin-panel HTTP/1.1" 200 1245 "Mozilla/5.0 (Windows NT 10.0; W
- '192.168.1.10 - hacker [04/Nov/2025:00:02:21 +0000] "GET /secret.env HTTP/1.1" 404 0 "python-requests/2.31.0"',■
- '203.0.113.70 - scanner [04/Nov/2025:00:12:08 +0000] "GET /admin-panel HTTP/1.1" 200 3010 "nmap"',■
- '192.168.4.41 - attacker [04/Nov/2025:00:15:41 +0000] "GET /.ssh/authorized_keys HTTP/1.1" 404 0 "python-requests/2.28.1
- '198.51.100.120 - root [04/Nov/2025:00:17:34 +0000] "GET /admin-panel/config HTTP/1.1" 200 204 "Mozilla/5.0"',■
- '192.168.6.77 - intruder [04/Nov/2025:00:22:30 +0000] "GET /secret.env HTTP/1.1" 404 0 "python-requests/2.27.1"',■
- '203.0.113.130 - - [04/Nov/2025:00:23:41 +0000] "GET /admin-panel HTTP/1.1" 200 3010 "Mozilla/5.0"',■
- '198.51.100.220 - root [04/Nov/2025:00:29:12 +0000] "GET /admin-panel HTTP/1.1" 200 3050 "Mozilla/5.0"',■
- '192.168.3.34 - - [04/Nov/2025:00:32:15 +0000] "GET /secret-keys.pem HTTP/1.1" 404 0 "curl/7.61.0"',■
- '10.0.4.4 - admin [04/Nov/2025:00:32:52 +0000] "GET /admin-panel HTTP/1.1" 200 2900 "Mozilla/5.0"',■
- '203.0.113.170 - hacker [04/Nov/2025:00:33:29 +0000] "GET /secret.env HTTP/1.1" 404 0 "python-requests/2.26.0"',■

10. Suspicious Outbound Traffic | Severity: Low | Count: 3

- 2025-11-04T00:08:09Z Warning: Suspicious outbound traffic from 203.0.113.9 bytes_sent=17339513
- 2025-11-04T00:23:24Z Suspicious outbound traffic 203.0.113.24 bytes_sent=10027735
- 2025-11-04T00:36:37Z Outbound exfiltration suspected 203.0.113.37

11. Unauthorized Access | Severity: Medium | Count: 26

- 2025-11-04T00:11:12Z Alert: Unauthorized shell command: chmod 777 /etc from 203.0.113.12
- 2025-11-04T00:16:17Z Alert: Forbidden API access /internal-api from 203.0.113.17
- 2025-11-04T00:18:19Z Critical: Unauthorized command: cat /etc/shadow from 203.0.113.19
- '192.168.1.10 - - [04/Nov/2025:00:00:01 +0000] "GET /sensitive-data.txt HTTP/1.1" 403 - "Mozilla/5.0"',■
- '10.0.0.1 - system [04/Nov/2025:00:01:33 +0000] "DELETE /prod-db-backup.sql HTTP/1.1" 403 42 "curl/7.29.0"',■
- '198.51.100.45 - service [04/Nov/2025:00:03:55 +0000] "GET /.env HTTP/1.1" 403 12 "Mozilla/5.0"',■
- '172.16.0.3 - auditor [04/Nov/2025:00:05:00 +0000] "GET /admin/settings HTTP/1.1" 401 98 "Mozilla/5.0"',■
- '192.0.2.88 - - [04/Nov/2025:00:08:39 +0000] "GET /backup.tar.gz HTTP/1.1" 403 0 "Wget/1.20.3"',■
- '10.0.0.5 - system [04/Nov/2025:00:09:11 +0000] "DELETE /backups/weekly.tar.gz HTTP/1.1" 403 22 "curl/7.50.0"',■
- '203.0.113.60 - - [04/Nov/2025:00:09:49 +0000] "GET /api/keys HTTP/1.1" 401 0 "python-requests/2.25.1"',■
- '10.8.0.21 - - [04/Nov/2025:00:11:33 +0000] "GET /config.yaml HTTP/1.1" 403 0 "Go-http-client/1.1"',■
- '198.51.100.2 - root [04/Nov/2025:00:12:45 +0000] "GET /secure/data.csv HTTP/1.1" 403 0 "Mozilla/5.0"',■
- '203.0.113.85 - - [04/Nov/2025:00:14:30 +0000] "GET /admin/.git HTTP/1.1" 403 0 "Mozilla/5.0"',■
- '203.0.113.95 - admin [04/Nov/2025:00:16:59 +0000] "DELETE /users/1001 HTTP/1.1" 403 16 "curl/7.76.1"',■
- '192.168.5.55 - - [04/Nov/2025:00:18:10 +0000] "GET /api/v1/secret HTTP/1.1" 401 0 "Java/11.0.11"',■
- '10.8.0.24 - sys [04/Nov/2025:00:19:25 +0000] "PATCH /etc/hosts HTTP/1.1" 403 0 "curl/7.72.0"',■
- '192.0.2.111 - user4 [04/Nov/2025:00:20:40 +0000] "POST /login HTTP/1.1" 401 32 "Mozilla/5.0"',■
- '203.0.113.120 - - [04/Nov/2025:00:21:15 +0000] "GET /downloads/keys.zip HTTP/1.1" 403 0 "Wget/1.21.1"',■
- '10.0.2.2 - system [04/Nov/2025:00:23:06 +0000] "DELETE /prod-db-backup.sql HTTP/1.1" 403 22 "curl/7.58.0"',■
- '198.51.100.200 - root [04/Nov/2025:00:24:18 +0000] "GET /hidden/.env HTTP/1.1" 403 0 "Mozilla/5.0"',■
- '10.1.1.1 - system [04/Nov/2025:00:27:58 +0000] "DELETE /secrets/old.key HTTP/1.1" 403 18 "curl/7.77.0"',■
- '203.0.113.150 - - [04/Nov/2025:00:28:36 +0000] "GET /api/admin HTTP/1.1" 401 0 "python-requests/2.30.0"',■
- '10.0.3.3 - - [04/Nov/2025:00:30:25 +0000] "GET /backup/secret.tar.gz HTTP/1.1" 403 0 "Wget/1.20.1"',■
- '203.0.113.160 - attacker [04/Nov/2025:00:31:02 +0000] "GET /.git/config HTTP/1.1" 403 0 "python-requests/2.28.0"',■
- '10.0.5.5 - sys [04/Nov/2025:00:35:19 +0000] "PATCH /etc/passwd HTTP/1.1" 403 0 "curl/7.79.0"',■
- '192.168.4.55 - intruder [04/Nov/2025:00:37:09 +0000] "GET /.env HTTP/1.1" 403 0 "python-requests/2.25.0"',