Invictus Incident Response

Invictus IR Dataset - CloudTrail Analysis Report (CORRECTED)

Phase 1: Foundation & Setup - Complete Analysis

Executive Summary

Dataset: Invictus Incident Response AWS CloudTrail Logs

Source: GitHub - invictus-ir/aws_dataset

Total Events: 1,237

Incident Date: July 10, 2023

Incident Duration: 55 minutes (11:42 AM - 12:37 PM EDT)

Primary Region: us-east-1

Attack Type: Red Team Simulation (Stratus Red Team Framework)

1. Basic Data Statistics

Metric	Value
Total Events	1,237
Earliest Event	2023-07-10 11:42:18 EDT
Latest Event	2023-07-10 12:37:50 EDT
Incident Duration	55 minutes (single-day attack)
Success Rate	88.52% (1,095 events)
Failure Rate	11.48% (142 events)

✅ **Corrected Analysis:** This is a **concentrated, single-day red team exercise** lasting less than 1 hour, not a multi-year campaign.

2. Event Distribution Timeline

Daily Activity Pattern

Date	Events	Percentage
2023-07-10	1,220	98.6%
Other dates	17	1.4% (residual/cleanup)

Hourly Breakdown - Attack Progression

Time Window	Events	Event Rate	Attack Phase
11:00 - 11:59 AM	405	6.75 events/min	Initial access & reconnaissance
12:00 - 12:37 PM	815	21.7 events/min	**Major attack escalation**

Key Observation: Attack intensity **more than tripled** in the second hour (6.75 → 21.7 events/min), indicating automated tooling and rapid exploitation.

---

3. Top 20 API Calls (Attack Indicators)

Rank	Event Name	Count	Attack Phase
1	Decrypt	73	Secrets access
2	DescribeRouteTables	68	Network reconnaissance
3	DescribeParameters	46	SSM enumeration
4	GetUser	42	IAM reconnaissance
5	DeleteParameter	41	Evidence destruction
6	GetBucketAcl	40	S3 reconnaissance
7	GetParameter	29	Secrets exfiltration
8	ListTagsForResource	29	Resource enumeration
9	DescribeEventAggregates	28	Health monitoring
10	PutParameter	28	Persistence mechanism
11	Encrypt	21	KMS operations
12	DescribeInstanceAttribute	20	EC2 reconnaissance
13	GetBucketPolicyStatus	20	S3 security assessment
14	GetBucketPublicAccessBlock	19	S3 exposure check
15	DescribeNatGateways	18	Network mapping
16	DescribeVpcs	18	VPC enumeration
17	**AssumeRole**	17	**Lateral movement**
18	DescribeAccountAttributes	17	Account reconnaissance
19	DescribeOrderableDBInstanceOptions	17	RDS enumeration
20	DescribeDBInstances	15	Database discovery

---

4. Threat Actor Profiling

Primary Actors

🔴 bert-jan (Primary Attacker)

- **Total Events:** 1,037 (83.8% of all activity)
- **Unique Actions:** 187 different API calls
- **Source IPs:** 6 distinct IPs
  - `192.168.10.20` (751 events) - Primary attack source
  - `10.8.8.10` (170 events) - Reconnaissance source
  - `10.107.159.90`, `AWS Internal`, `health.amazonaws.com`, `secretsmanager.amazonaws.com`
- **Attack Capabilities:**
  - Infrastructure creation/destruction
  - IAM manipulation

- Secrets management
- Database operations
- CloudTrail tampering
- Lambda function manipulation

🟡 benjamin (Secondary Actor/Reconnaissance)

- **Total Events:** 124 (10% of activity)
- **Unique Actions:** 20 API calls
- **Source IPs:** 4 distinct IPs
  - `10.248.16.43` (111 events) - Primary source
  - `10.107.112.14`, `AWS Internal`, `health.amazonaws.com`
- **Focus Areas:**
  - IAM enumeration (`GetAccountAuthorizationDetails`)
  - S3 security assessment
  - Account-level reconnaissance
  - Route53 enumeration

🤖 Stratus Red Team Roles (Automated Attack Framework)

- `stratus-red-team-get-usr-data-role` (15 events) - EC2 user data theft
- `stratus-red-team-ec2-get-password-data-role` (5 events) - Password extraction attempts
- `stratus-red-team-ec2-steal-credentials-role` (3 events) - Credential theft
- `stratus-red-team-leave-org-role` (1 event) - Organization disruption
- `stratus-red-team-ec2-enumerate-role` (1 event) - EC2 enumeration

---

5. Source IP Analysis

Attack Infrastructure

IP Address	Events	Users	Primary Actions
192.168.10.20	772	4	Primary attack orchestration
10.8.8.10	170	1 (bert-jan)	Infrastructure reconnaissance
10.248.16.43	111	1 (benjamin)	IAM/S3 enumeration
AWS Internal	85	2	KMS operations, storage lens
secretsmanager.amazonaws.com	40	1	Secrets lifecycle management
health.amazonaws.com	18	2	Health monitoring
3.225.16.109	3	1	EC2 credential theft (external IP)
52.45.102.28	1	1	EC2 enumeration (external IP)

⚠️ **External IPs:** `3.225.16.109` and `52.45.102.28` indicate compromised EC2 instances calling back to AWS APIs.

---

6. Attack Timeline Reconstruction (55-Minute Attack)

🕐 11:00 - 11:59 AM EDT: Initial Access & Reconnaissance Phase

Duration: ~60 minutes | **Events:** 405 | **Rate:** 6.75 events/min

Minute-by-Minute Breakdown (Estimated)

11:42 AM - First Event (Attack Initiation)

- AssumeRole (lateral movement initiation)
- CreateSecret, GetSecretValue (secrets access)
- DescribeInstanceAttribute (EC2 reconnaissance)

11:45-11:50 AM - Database Targeting

- CreateDBSnapshot (data exfiltration preparation)
- DescribeDBInstances (database enumeration)
- CreateNetworkInterface (network manipulation)

11:50-11:59 AM - Systematic Reconnaissance

- DescribeRouteTables, DescribeVpcs (network mapping)
- GetUser, ListUsers (IAM enumeration)
- GetBucketAcl, GetBucketPolicyStatus (S3 assessment)
- DescribeParameters (SSM enumeration)

Actors Active: bert-jan, benjamin, stratus-red-team roles

🕐 12:00 - 12:37 PM EDT: Major Attack Escalation Phase

Duration: 37 minutes | **Events:** 815 | **Rate:** 21.7 events/min | 🚨 **CRITICAL PHASE**

Attack Intensity Spike: +221% increase in event rate

12:00-12:10 PM - Infrastructure Manipulation

- CreateVpc, CreateSubnet, CreateInternetGateway (network setup)
- CreateRole, AttachRolePolicy (privilege escalation)
- CreateLoginProfile (persistence)
- AllocateAddress, CreateNatGateway (network pivoting)

12:10-12:20 PM - Lateral Movement & Persistence

- AssumeRole (17 total, 4 failed) - role chaining
- AddRoleToInstanceProfile (privilege attachment)
- PutParameter (28 events) - SSM persistence
- CreateTrail → DeleteTrail (logging manipulation)

12:20-12:30 PM - Data Exfiltration & Evidence Destruction

- GetParameter (29 events) - secrets exfiltration
- DeleteParameter (41 events) - evidence destruction
- Decrypt (73 events) - KMS key usage for secrets

- ModifyDBSnapshotAttribute (snapshot sharing preparation)

12:30-12:37 PM - Cleanup & Final Actions

- DeleteBucket, DeleteRole, DeleteVpc (infrastructure cleanup)
- TerminateInstances (EC2 cleanup)
- StopLogging (2 events) - final logging tampering
- LeaveOrganization (1 failed attempt) - disruption attempt

12:37:50 PM - Last Event (Attack Conclusion)

Actors Active: bert-jan (primary), benjamin, multiple Stratus Red Team roles

---

7. Error Analysis - Failed Attack Attempts

Top Failed Actions (Privilege Escalation Indicators)

Error Code	Event Name	User	Count	Significance
ThrottlingException	DeleteParameter	bert-jan	16	Rapid evidence destruction attempt
Client.UnauthorizedOperation	DescribeInstanceAttribute	stratus-get-usr-data	15	**EC2 user data theft blocked**
ThrottlingException	DescribeParameters	bert-jan	12	SSM secrets enumeration throttled
ThrottlingException	PutParameter	bert-jan	10	Persistence mechanism blocked
NoSuchPublicAccessBlockConfiguration	GetBucketPublicAccessBlock	benjamin	8	S3 security check
Client.UnauthorizedOperation	GetPasswordData	stratus-get-password	5	**Password extraction blocked**
AccessDenied	AssumeRole	bert-jan	4	**Lateral movement blocked**
AccessDenied	LeaveOrganization	stratus-leave-org	1	**Organization disruption blocked**
AccessDenied	GetCostAndUsage	bert-jan	1	Cost visibility blocked

Key Findings:

- **15 unauthorized EC2 user data access attempts** - Clear credential theft pattern
- **5 password extraction failures** - Automated password harvesting blocked
- **4 AssumeRole failures** - Lateral movement attempts denied
- **1 LeaveOrganization failure** - Critical organization disruption prevented
- **38 ThrottlingExceptions** - Automated tooling hitting API rate limits

8. AWS Services Targeted

Rank	Service	Events	Attack Focus
1	**EC2**	341	Infrastructure reconnaissance & manipulation
2	**S3**	201	Data access & security assessment
3	**SSM**	191	Parameter store enumeration & secrets
4	**IAM**	133	Identity & permission reconnaissance
5	**KMS**	102	Encryption key operations
6	**Secrets Manager**	71	Secrets lifecycle manipulation
7	**RDS**	63	Database discovery & snapshot creation
8	**Health**	28	Service health monitoring
9	**STS**	22	Temporary credential generation
10	**CloudTrail**	20	Logging manipulation
11	**Lambda**	10	Serverless function enumeration
12	**Organizations**	4	Account structure reconnaissance
13	**GuardDuty**	3	Security service assessment
14	**Route53**	3	DNS enumeration

9. MITRE ATT&CK Mapping

Reconnaissance (TA0043)

- **T1580** - Cloud Infrastructure Discovery
  - DescribeVpcs, DescribeSubnets, DescribeRouteTables (104 events)
- **T1526** - Cloud Service Discovery
  - DescribeDBInstances, DescribeParameters, ListBuckets (90+ events)
- **T1087.004** - Account Discovery: Cloud Account
  - GetUser, ListUsers, GetAccountAuthorizationDetails (42+ events)

Initial Access (TA0001)

- **T1078.004** - Valid Accounts: Cloud Accounts
  - bert-jan and benjamin user accounts compromised

Credential Access (TA0006)

- **T1552.005** - Unsecured Credentials: Cloud Instance Metadata API
  - DescribeInstanceAttribute (20 events, 15 failed)
  - GetPasswordData (5 failed attempts)
- **T1555.006** - Credentials from Password Stores: Cloud Secrets Management Stores
  - GetParameter, GetSecretValue (58 events)

Lateral Movement (TA0008)

- **T1550.001** - Use Alternate Authentication Material: Application Access Token
  - AssumeRole (17 events, 4 failed)

Persistence (TA0003)

- **T1098** - Account Manipulation
  - CreateLoginProfile, CreateAccessKey, AttachRolePolicy
- **T1136.003** - Create Account: Cloud Account
  - CreateRole, CreateUser
- **T1098.001** - Account Manipulation: Additional Cloud Credentials
  - PutParameter (28 events) - SSM-based persistence

Defense Evasion (TA0005)

- **T1562.008** - Impair Defenses: Disable Cloud Logs
  - StopLogging, DeleteTrail (4 events)
- **T1070.004** - Indicator Removal on Host: File Deletion
  - DeleteParameter, DeleteSecret (82 events)

Collection (TA0009)

- **T1530** - Data from Cloud Storage Object
  - GetBucketAcl, GetParameter (69 events)
- **T1005** - Data from Local System
  - CreateDBSnapshot (database exfiltration preparation)

Impact (TA0040)

- **T1531** - Account Access Removal
  - LeaveOrganization (1 failed attempt)
- **T1485** - Data Destruction
  - DeleteBucket, DeleteVolume, DeleteDBSnapshot

---

10. Key Attack Patterns Identified

Pattern 1: Systematic SSM Parameter Store Exploitation

- **191 SSM events** (15.4% of all activity)
- DescribeParameters (46) → GetParameter (29) → DeleteParameter (41)
- **Indicates:** Secrets enumeration → exfiltration → evidence destruction
- **Timeline:** Concentrated in 12:00-12:37 PM phase

Pattern 2: Database Snapshot Exfiltration

- CreateDBSnapshot → ModifyDBSnapshotAttribute
- **Technique:** Create snapshot, modify permissions for external access

- **MITRE:** T1530 (Data from Cloud Storage)
- **Timeline:** 11:45-11:50 AM

Pattern 3: EC2 Credential Theft via User Data

- 15 failed DescribeInstanceAttribute attempts by stratus-red-team-get-usr-data-role
- **Technique:** Extract credentials from EC2 user data
- **MITRE:** T1552.005
- **Timeline:** Throughout attack (automated)

Pattern 4: CloudTrail Tampering

- StopLogging (2 events) + DeleteTrail (1 event)
- **Technique:** Disable logging to evade detection
- **MITRE:** T1562.008
- **Timeline:** 12:30-12:37 PM (cleanup phase)

Pattern 5: Lateral Movement via AssumeRole

- 17 AssumeRole events (4 failed)
- Multiple Stratus Red Team roles assumed
- **Technique:** Role chaining for privilege escalation
- **MITRE:** T1550.001
- **Timeline:** 12:10-12:20 PM

Pattern 6: Automated Attack Acceleration

- Event rate increased from 6.75/min → 21.7/min (+221%)
- 38 ThrottlingExceptions indicate automated tooling
- **Indicates:** Scripted/automated attack framework (Stratus Red Team)

---

11. Detection Opportunities

Based on this analysis, the following detection rules would have caught this attack:

✅ Rule 1: API Reconnaissance Spike

- **Trigger:** >10 unique API calls in 10 minutes
- **Would Detect:** All attack phases (187 unique actions by bert-jan)
- **Alert Time:** 11:50 AM (within 8 minutes of attack start)

```
index=invictus (eventName=List* OR eventName=Describe* OR eventName=Get*)
|eval _time = strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| bin _time span=10m
| stats dc(eventName) as unique_api_calls,
      values(eventName) as attempted_calls,
      count as total_hits
```

```
  by _time, sourceIPAddress, userIdentity.arn
| where unique_api_calls > 10
| sort - unique_api_calls
```

✅ Rule 2: SSM Parameter Enumeration

- **Trigger:** >15 DescribeParameters/GetParameter in 10 minutes
- **Would Detect:** 75 SSM operations during 12:00-12:37 PM
- **Alert Time:** 12:10 PM

```
index = invictus eventSource="ssm.amazonaws.com"
eventName IN ("DescribeParameters", "GetParameters", "GetParameter", "GetParameterHistory")
| eval event_time = strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| bin event_time span=10m
| stats count as api_call_count
    dc(eventName) as distinct_api_calls
    dc(requestParameters.name) as unique_parameters
    count(eval(errorCode="AccessDenied")) AS access_denied_count
    values(eventName) AS api_calls
    values(errorCode) AS error_codes
    values(sourceIPAddress) AS source_ips
    values(userAgent) AS user_agents
    by userIdentity.arn, event_time
| where api_call_count > 10
| eval event_time = strftime(event_time, "%Y-%m-%dT%H:%M:%SZ")
| table event_time, userIdentity.arn, source_ips, user_agents, distinct_api_calls, unique_parameters, access_de
nied_count, api_calls, error_codes
```

✅ Rule 3: Failed Privilege Escalation

- **Trigger:** >3 AccessDenied/UnauthorizedOperation in 5 minutes
- **Would Detect:** 15 EC2 user data theft attempts, 5 password extraction attempts
- **Alert Time:** 11:45 AM (first unauthorized attempts)

```
index=invictus errorCode="AccessDenied" OR errorCode="UnauthorizedOperation"
| eval event_time=strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| bin event_time span=5m
| stats count as failed_attempts,
dc(eventName) as unique_events,
values(eventName) as attempted_events,
values(eventMessage) as error_details
by event_time, sourceIPAddress, userIdentity.arn
| where failed_attempts > 3
| eval EventTime = strftime(event_time, "%Y-%m-%dT%H:%M:%SZ")
| eval severity=case(
    failed_attempts > 10, "CRITICAL",
    failed_attempts > 5, "HIGH",
    1=1, "MEDIUM"
```

```
 )
| table EventTime, sourceIPAddress, userIdentity.arn, failed_attempts, unique_events, attempted_events, error_details, severity
| sort - failed_attempts
```

✅ Rule 4: CloudTrail Tampering

- **Trigger:** StopLogging OR DeleteTrail events
- **Would Detect:** 3 logging manipulation attempts
- **Alert Time:** 12:30 PM (immediate)

```
index=invictus
eventName IN ("StopLogging", "DeleteTrail", "UpdateTrail", "PutEventSelectors", "DeleteDetector", "PutInsightSelectors", "CreateTrail", "ArchiveFindings")
| table eventTime, eventName, awsRegion, userIdentity.type, userIdentity.arn, userIdentity.accountId, sourceIPAddress, userAgent, requestID
```

✅ Rule 5: Lateral Movement (AssumeRole Chain)

- **Trigger:** >3 AssumeRole calls in 10 minutes
- **Would Detect:** 17 role assumption events
- **Alert Time:** 12:15 PM

```
index=invictus eventName="AssumeRole"
| eval event_time = strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| rename requestParameters.roleArn as target_role
| stats
   count as attempt_count,
   values(errorCode) as errors,
   earliest(event_time) as first_seen,
   latest(event_time) as last_seen
   by userIdentity.arn, target_role, sourceIPAddress
| eval duration = last_seen - first_seen
| sort - attempt_count
| table userIdentity.arn, target_role, sourceIPAddress, attempt_count, errors
```

```
index=invictus eventName="AssumeRole"
| eval event_time = strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| bin event_time span=10m
| stats count as total_attempts
dc(errorCode) as total_errors
values(errorCode) as errors
values(errorMessage) as error_message
by userIdentity.arn, event_time, sourceIPAddress, eventName
| where total_attempts > 3
| eval event_time = strftime(event_time, "%Y-%m-%d %H:%M:%S")
```

```
| table event_time, userIdentity.arn, sourceIPAddress, eventName, total_attempts, total_errors, errors, error_message
```

Phase 2: Detection Development

Detection Rules Summary

Rule	Detection Name	Threshold	Window	Severity	MITRE Technique
1	API Reconnaissance Spike	>10 unique calls	10 min	MEDIUM	T1595.002
2	SSM Parameter Enumeration	>10 SSM calls	10 min	HIGH	T1555.006
3	Failed Privilege Escalation	>3 AccessDenied	5 min	MED-CRIT	T1078, T1068
4	CloudTrail Tampering	Any logging event	Immediate	CRITICAL	T1562.008
5	Lateral Movement (AssumeRole)	>3 AssumeRole	10 min	HIGH	T1550.001
6	Mass Deletion/Destruction	>20 deletes / Critical	5 min	MED-CRIT	T1485, T1490

Rule 1: API Reconnaissance Spike

Detection Logic Identifies automated discovery patterns where a single identity performs a high volume of unique `List`, `Describe`, or `Get` API calls to map out account resources.

Splunk Query

```
index=your_index (eventName=List* OR eventName=Describe* OR eventName=Get*)
| eval _time = strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| bin _time span=10m
| stats dc(eventName) as unique_api_calls,
      values(eventName) as attempted_calls,
      count as total_hits
  by _time, sourceIPAddress, userIdentity.arn
| where unique_api_calls > 10
| sort - unique_api_calls
```

MITRE ATT&CK: T1595.002 (Active Scanning: Vulnerability Scanning)

Rule 2: SSM Parameter Enumeration

Detection Logic Detects excessive access attempts to AWS Systems Manager (SSM) Parameter Store, which often contains sensitive environment variables, API keys, and database credentials.

Splunk Query

```
index=your_index eventSource="ssm.amazonaws.com"
eventName IN ("DescribeParameters", "GetParameters", "GetParameter", "GetParameterHistory")
| eval event_time = strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| bin event_time span=10m
| stats count as api_call_count,
```

```
    dc(requestParameters.name) as unique_parameters,
    count(eval(errorCode="AccessDenied")) AS access_denied_count,
    values(eventName) AS api_calls
    by userIdentity.arn, event_time
| where api_call_count > 10
```

MITRE ATT&CK: T1555.006 (Credentials from Password Stores)

Rule 3: Failed Privilege Escalation

Detection Logic Monitoring for multiple `AccessDenied` or `UnauthorizedOperation` errors. High frequency suggests an attacker is testing permissions or attempting to brute-force privilege escalation.

Splunk Query

```
index=your_index errorCode IN ("AccessDenied", "UnauthorizedOperation")
| eval event_time=strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| bin event_time span=5m
| stats count as failed_attempts,
    values(eventName) as attempted_events,
    values(eventMessage) as error_details
  by event_time, sourceIPAddress, userIdentity.arn
| where failed_attempts > 3
```

MITRE ATT&CK: T1078 (Valid Accounts), T1068 (Exploitation for Privilege Escalation)

Rule 4: CloudTrail Tampering

Detection Logic Detects administrative actions aimed at disabling security auditing. This is a high-fidelity indicator of defense evasion.

Splunk Query

```
index=your_index
eventName IN ("StopLogging", "DeleteTrail", "UpdateTrail", "PutEventSelectors", "DeleteDetector", "PutInsight
Selectors")
| table eventTime, eventName, awsRegion, userIdentity.arn, sourceIPAddress, userAgent
```

MITRE ATT&CK: T1562.008 (Impair Defenses: Disable Cloud Logs)

Rule 5: Lateral Movement (AssumeRole Chain)

Detection Logic Detects rapid or excessive `AssumeRole` operations, which may indicate an attacker moving between accounts or roles to escalate permissions or hide their origin.

Splunk Query (Version 1 - Role Tracking)

```
index=your_index eventName="AssumeRole"
| eval event_time = strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| rename requestParameters.roleArn as target_role
| stats
    count as attempt_count,
```

```
    values(errorCode) as errors
    by userIdentity.arn, target_role, sourceIPAddress, event_time
| where attempt_count > 3
```

Splunk Query (Version 2 - Time-Based Detection)

```
index=invictus eventName="AssumeRole"
| eval event_time = strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| bin event_time span=10m
| stats count as total_attempts
    dc(errorCode) as total_errors
    values(errorCode) as errors
    values(errorMessage) as error_message
  by userIdentity.arn, event_time, sourceIPAddress, eventName
| where total_attempts > 3
| eval event_time = strftime(event_time, "%Y-%m-%d %H:%M:%S")
| table event_time, userIdentity.arn, sourceIPAddress, eventName, total_attempts, total_errors, errors, error_m
essage
```

MITRE ATT&CK: T1550.001 (Use Alternate Authentication Material)

Rule 6: Mass Deletion/Destruction

Detection Logic Alerts on bulk deletion of resources (S3, EC2, RDS) or the deletion of critical security infrastructure like KMS keys and CloudTrail logs.

Splunk Query

Code snippet

```
index=your_index (eventName="Delete*" OR eventName="Terminate*" OR eventName="Drop*")
| eval event_time = strptime(eventTime, "%Y-%m-%dT%H:%M:%SZ")
| bin event_time span=5m
| stats
    count as deletion_count,
    values(eventName) as actions_taken
    by userIdentity.arn, sourceIPAddress, event_time
| where deletion_count > 20 OR (deletion_count > 0 AND (actions_taken="DeleteTrail" OR actions_taken="Del
eteKMSKey"))
```

MITRE ATT&CK: T1485 (Data Destruction), T1490 (Inhibit System Recovery)