FLAWS.CLOUD DATASET - VISUAL GRAPHS & CHARTS

📊 GRAPH 1: EVENT DISTRIBUTION BY USER

```
TOTAL EVENTS: 1,939,207 (Feb 2017 - Oct 2020)

backup   ████████████████████████████████████████████████ 915,834 (47.2%)
Level6   ███████████████████████████████████████████████  905,082 (46.7%)
Unknown  ███                                               57,617 ( 3.0%)
flaws    ▌                                                 3,372 ( 0.2%)
piper    ▌                                                 147 ( 0.0%)
Level5   ▌                                                 39 ( 0.0%)
Others   ▌                                                 56,116 ( 2.9%)

Legend: Each ▌ = 20,000 events
```

KEY INSIGHT: backup and Level6 DOMINATE (93.9% of all events!)

📅 GRAPH 2: CHRONOLOGICAL TIMELINE

```
WHEN EACH USER FIRST APPEARED:

Feb 12, 2017      Feb 19-23       Feb 26          Sept 18
    |                 |              |               |
    ▼                 ▼              ▼               ▼
┌─────────┐      ┌─────────┐    ┌─────────┐     ┌─────────┐
│ backup  │      │ Level5  │    │ Level6  │     │  flaws  │
│ starts  │      │  (39)   │    │ starts  │     │ (root)  │
└─────────┘      └─────────┘    └─────────┘     └─────────┘
    │                 │              │               │
    │<── 7 days ──>   │  <── 6 days ──>  <── 218 days ──>
    │                 │              │               │
915,834           39 events      905,082         3,372
events            (4 days)       events          events
```

TIME GAPS:

```
├─ backup → Level5: 7 days
├─ Level5 → Level6: 6 days
├─ Level6 → flaws:  218 days (7 months!)
└─ All run for: 1,333 days (3.6 years)
```

📈 GRAPH 3: MONTHLY ACTIVITY OVER TIME

```
MONTHLY EVENT DISTRIBUTION (Feb 2017 - Oct 2020)

Events
(K)
 50 |
    |
 40 |
    |
 30 |
    |
 20 |
    |
 10 |
    |
  0 |
    2017    2018     2019     2020
    F M A M J J A S O N D J F M A M J J A S O N D J F M A M J J A S O
```

🔥 AUGUST 2019 🔥
1,347,680 events!
(OFF SCALE)

If we include August 2019, the graph would look like:

```
1347 |
     |
     |
     |
 100 |
     |
  50 |
```


```

---

## 🔥 GRAPH 4: AUGUST 2019 DAILY BREAKDOWN

```
THE EXPLOSION - AUGUST 2019 DAILY EVENTS

Events
(K)
600 |
    |
500 |
    |
400 |
    |
300 |
    |
200 |
    |
100 |
    |
  0 |
    1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
                                                    ▲ ▲ ▲
                                                   21 22 23
                                                   THE 3-DAY
                                                   APOCALYPSE

Daily Breakdown:
Aug 1-20:   Average ~1,000 events/day (normal)
Aug 21:   421,560 events 🔥
Aug 22:   591,688 events 🔥 PEAK!
Aug 23:   301,547 events 🔥
Aug 24-31: Average ~1,000 events/day (back to normal)

Total Aug 21-23: 1,314,795 events (97.6% of August!)
```
```

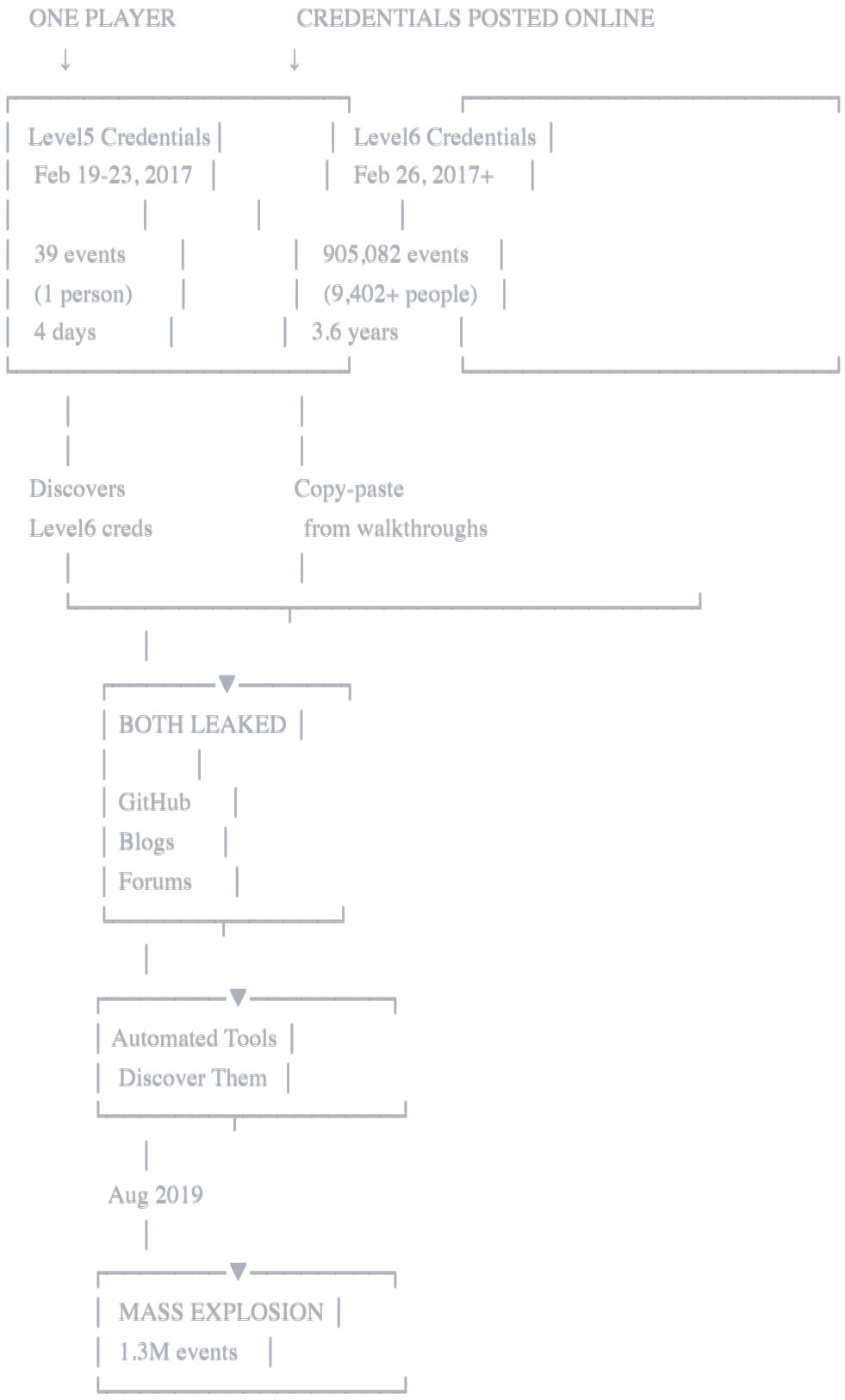
👥 GRAPH 5: WHO DID WHAT IN AUGUST 2019?

```
AUGUST 2019 ACTIVITY BREAKDOWN

By User:
Level6   ████████████████████████████████████████ 700,148 (52%)
backup   ████████████████████████████████████     644,676 (48%)
Unknown  ▌                                        1,966 ( 0%)
Others   ▌                                        890 ( 0%)

By Action:
RunInstances      ████████████████████████████████████ 1,299,186 (96.4%)
DescribeSnapshots ▌                                    5,596 ( 0.4%)
GetCallerIdentity ▌                                    5,508 ( 0.4%)
DescribeInstances ▌                                    5,043 ( 0.4%)
CreateDefaultVpc  ▌                                    4,565 ( 0.3%)
Others            ▌                                    27,782 ( 2.1%)

Success vs Failure:
SUCCESS  ▌                                             34,212 ( 2.5%)
FAILURE  ████████████████████████████████████         1,313,468 (97.5%)

Legend: Each ▌ = 25,000 events
```

🎯 GRAPH 6: THE CREDENTIAL PROGRESSION

```
THE INTENDED CTF PATH vs ACTUAL USAGE

INTENDED:

┌──────────┐    ┌──────────┐    ┌──────────┐    ┌──────────┐    ┌──────────┐    ┌──────────┐
│ Level 1  │ ─> │ Level 2  │ ─> │ Level 3  │ ─> │ Level 4  │ ─> │ Level 5  │ ─> │ Level 6  │
│ Public   │    │ External │    │ Git      │    │ Snapshot │    │ EC2 SSRF │    │ Audit    │
│ S3       │    │ AWS User │    │ Creds    │    │ Forensic │    │ Proxy    │    │ Policy   │
└──────────┘    └──────────┘    └──────────┘    └──────────┘    └──────────┘    └──────────┘
     0               0               0               0              39           905,082
  events          events          events          events         events         events
```

ACTUAL USAGE (Credential Leakage):




```

---

## GRAPH 7: USER ACTIVITY TIMELINE (Gantt Chart)
```

```
USER ACTIVITY PERIODS (Feb 2017 - Oct 2020)

backup
915,834
     Feb 12, 2017 ──────────────────────────────────────────> Oct 7, 2020
     (1,332 days)

Level5
     Feb 19-23, 2017
     (4 days, 39 events)

Level6
905,082
     Feb 26, 2017 ──────────────────────────────────────────> Oct 7, 2020
     (1,318 days)

piper
     May 16, 2017 ────────────────────────> Oct 3, 2018
     (505 days, 147 events)

flaws
     Sept 18, 2017 ─────────────────────────────────> Oct 7, 2020
     (1,114 days, 3,372 events - ROOT account management)

      |        |        |        |        |
    2017     2018     2019     2020     2021
    F M A M J J A S O N D J F M A M J J A S O N D J F M A M J J A S O
                             ▲
                         Aug 2019
                         EXPLOSION
```

🔄 GRAPH 8: EVENT TYPE DISTRIBUTION

```
BY IDENTITY TYPE:

IAMUser          1,825,650 (94.14%)
AWSService       57,616 ( 2.97%)
AssumedRole      42,315 ( 2.18%)
```

Root 10,997 (0.57%)
AWSAccount 2,628 (0.14%)
Unknown 1 (0.00%)

KEY USERS (IAMUser type only):

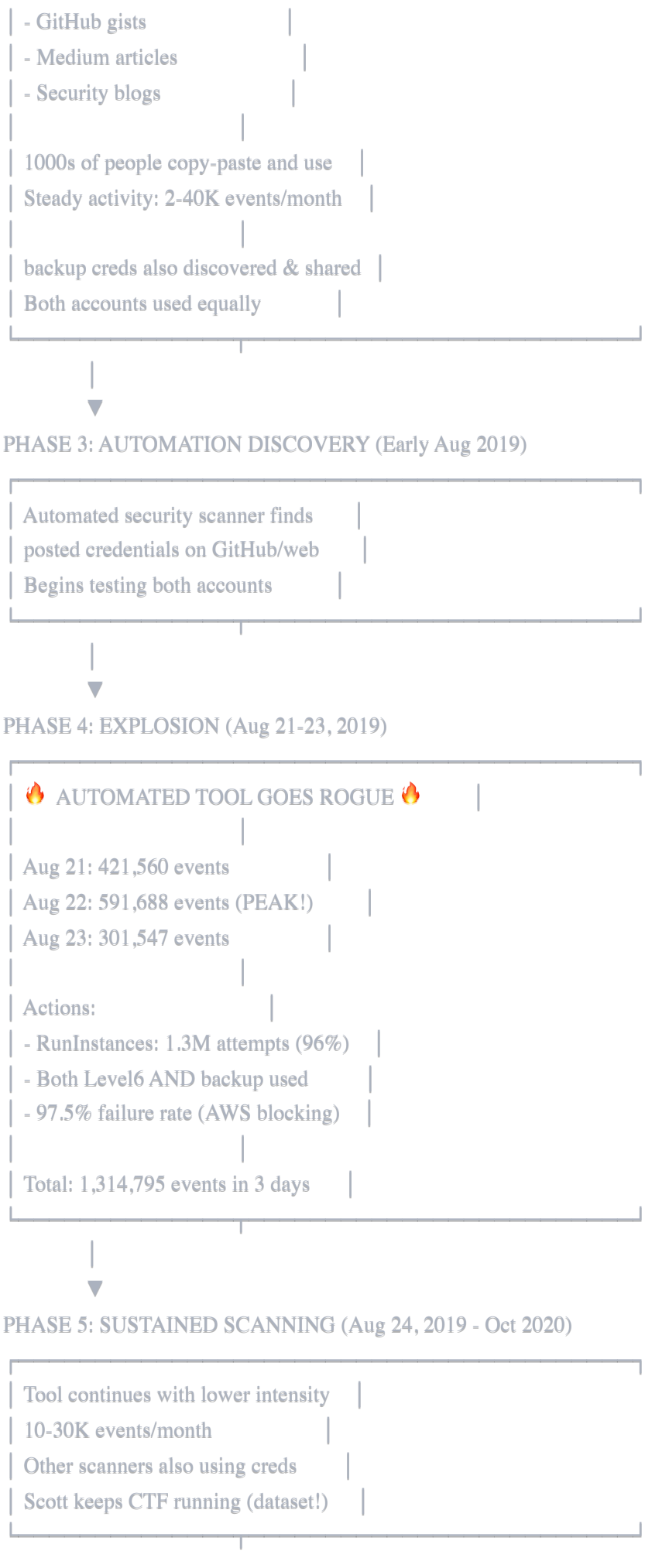
backup 915,834 (50.2%)
Level6 905,082 (49.6%)
piper 147 (0.0%)
Level5 39 (0.0%)
Others 4,548 (0.2%)

Legend: Each = 50,000 events
```

---

## 🎬 GRAPH 9: THE COMPLETE STORY (Flow Diagram)

```
PHASE 0: SETUP (Feb 12, 2017)

┌──────────────────────────────────────┐
│ Scott Piper creates flaws.cloud   │
│ - Creates backup IAMUser   │
│ - Creates Level5 IAMUser   │
│ - Creates Level6 IAMUser   │
│ - Enables CloudTrail   │
└──────────────────┬───────────────────┘
                   │
                   ▼
PHASE 1: FIRST PLAYER (Feb 19-23, 2017)

┌──────────────────────────────────────┐
│ ONE person solves Level 4   │
│ Gets Level5 credentials   │
│ Does reconnaissance: 39 events   │
│ Discovers Level6 credentials   │
│ Posts walkthrough online   │
└──────────────────┬───────────────────┘
                   │
                   ▼
PHASE 2: CREDENTIAL SHARING (Feb 26 - Jul 2019)

┌──────────────────────────────────────┐
│ Level6 creds posted on: │
```
```


- GitHub gists
- Medium articles
- Security blogs
1000s of people copy-paste and use
Steady activity: 2-40K events/month
backup creds also discovered & shared
Both accounts used equally
PHASE 3: AUTOMATION DISCOVERY (Early Aug 2019)
Automated security scanner finds
posted credentials on GitHub/web
Begins testing both accounts
PHASE 4: EXPLOSION (Aug 21-23, 2019)
🔥 AUTOMATED TOOL GOES ROGUE 🔥
Aug 21: 421,560 events
Aug 22: 591,688 events (PEAK!)
Aug 23: 301,547 events
Actions:
- RunInstances: 1.3M attempts (96%)
- Both Level6 AND backup used
- 97.5% failure rate (AWS blocking)
Total: 1,314,795 events in 3 days
PHASE 5: SUSTAINED SCANNING (Aug 24, 2019 - Oct 2020)
Tool continues with lower intensity
10-30K events/month
Other scanners also using creds
Scott keeps CTF running (dataset!)

```
                    |
                    ▼
PHASE 6: DATASET RELEASE (Oct 2020)
┌──────────────────────────────────────────────────┐
│ Scott releases anonymized CloudTrail             │
│ 1,939,207 events                                 │
│ 3.6 years of data                                │
│ For security research & education                │
└──────────────────────────────────────────────────┘
```

📊 GRAPH 10: ERROR RATE ANALYSIS

```
SUCCESS vs FAILURE RATES BY USER

backup:
SUCCESS ████████████████████                    173,387 (18.9%)
FAILURE ████████████████████████████████████████ 742,447 (81.1%)

Level6:
SUCCESS ████████████████████                    239,183 (26.4%)
FAILURE ████████████████████████████████        665,899 (73.6%)

Level5:
SUCCESS ████████████████████████████████████    36 (92.3%)
FAILURE ██                                      3 ( 7.7%)

flaws (Root):
SUCCESS ████████████████████████████████████    ~3,300 (~98%)
FAILURE ▓                                       ~72 ( ~2%)


KEY INSIGHT:
- Level5: Low errors (manual, careful)
- backup/Level6: High errors (automated, brute-force)
- flaws: Very low errors (legitimate management)

Legend: Each ▓ = 2%
```

🎯 GRAPH 11: THE BIG PICTURE SUMMARY

```
                    FLAWS.CLOUD DATASET SUMMARY
                    ===========================

Total Events:     1,939,207
Time Span:        1,333 days (Feb 12, 2017 - Oct 7, 2020)
Unique IPs:       9,402
Unique Agents:    8,811

┌──────────────────────────────────────────────────────────────────────────────┐
│                          EVENT DISTRIBUTION                                  │
└──────────────────────────────────────────────────────────────────────────────┘
                                    │
  The Two Giants (93.9%):           │
   ┌──────────────┐  ┌──────────────┐                    │
   │  backup      │  │  Level6      │                    │
   │  915,834     │  │  905,082     │                    │
   │  (47.2%)     │  │  (46.7%)     │                    │
   └──────┬───────┘  └──────┬───────┘                    │
          │                 │                            │
          └────────┬────────┘                            │
                   │                                     │
          Both abused                                    │
          equally by                                     │
          same tools                                     │
              │                                          │
          ┌───▼──────────┐                               │
          │  Aug 2019    │                               │
          │  EXPLOSION   │                               │
          │  1.3M events │                               │
          │  (70%)       │                               │
          └──────────────┘                               │
                                    │
  The Scout (0.002%):               │
   ┌──────────────┐                                      │
   │  Level5      │  39 events (first player)            │
   │  (39)        │  Manual reconnaissance               │
   └──────────────┘  Led to credential leakage           │
                                    │
  Infrastructure (3.2%):            │
   ┌──────────────┐  ┌──────────────┐                    │
```

RESEARCH VALUE:

✅ Only public CloudTrail attack dataset
✅ Real attacker behavior (9,402 IPs)
✅ Credential lifecycle visible
✅ Temporal evolution (manual → automated)
✅ Benchmark for cloud forensics

```

---

END OF VISUAL GRAPHS
```