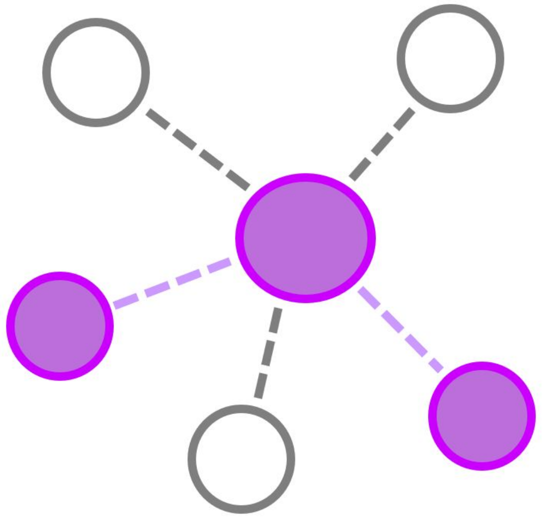
Capstone Project

Melody Neely , Rayan Hamid, Ghita Benlamin

CST 312 Network Security

- **Dataset :** AWS Cloud Bank Breach S3
- **Playbook :** Cybersecurity Incident and Vulnerability Response Playbooks
- **Tools :** Splunk



About the Dataset:

Where the Data Comes From?

- Logs from AWS EC2, showing activity on S3 buckets.
- Focuses on tracking data access and suspicious activity.

Targeted Devices/Technologies

- S3 Buckets
- AWS CLI

Three Things We Expected to Find

- Attempts to steal data from S3 buckets .
- Scans that map out storage or potential attacks points.
- Suspicious IP addresses or tools used in the attack.

About the Playbook:

Cybersecurity Incident and vulnerability response Playbooks

- Identifying
- Coordinating
- Remediating
- Recovering
- Tracking Mitigations

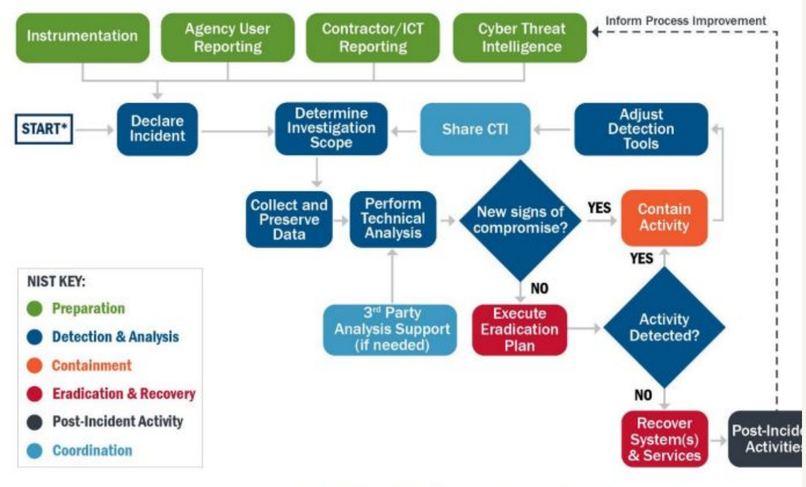


Figure 1: Incident Response Process

Impact Analysis:

Impact of the Incident:

- A sensitive file (ring.txt) was accessed and exfiltrated
- Breach exposed important data stored in the cloud.

Severity:

- High

Other Systems or Applications Affected:

- There is no direct evidence of other systems being breached,but:
    - Weak security settings could have allowed attackers to target other AWS services.

Incident Response :

Incident Response Results: Actions and Insights

Actions Taken:

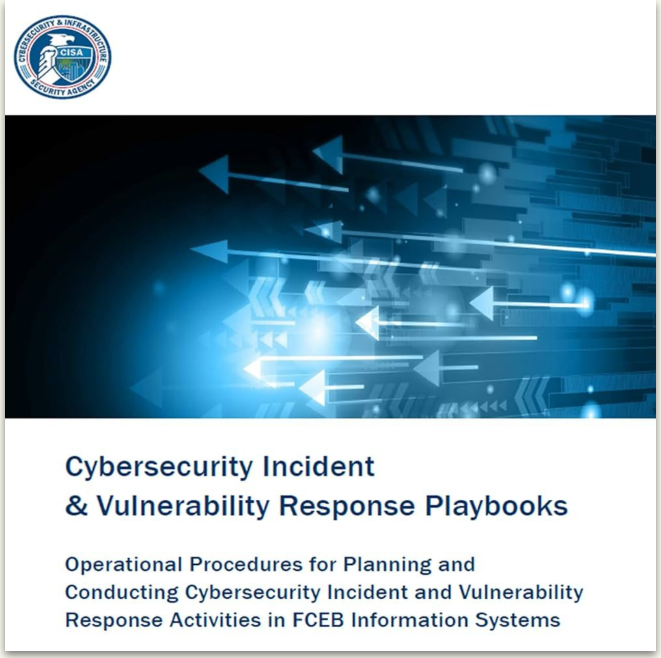
- Used Splunk to analyze AWS activity logs.
- Found suspicious IP activity and access to storage buckets.
- Linked events showing bucket exploration and data theft.

Insights Gained:

- Confirmed the process of bucket exploration and file stealing.
- Linked suspicious activities to the user agent and source IP.

Outcome:

- Clear proof of data theft.



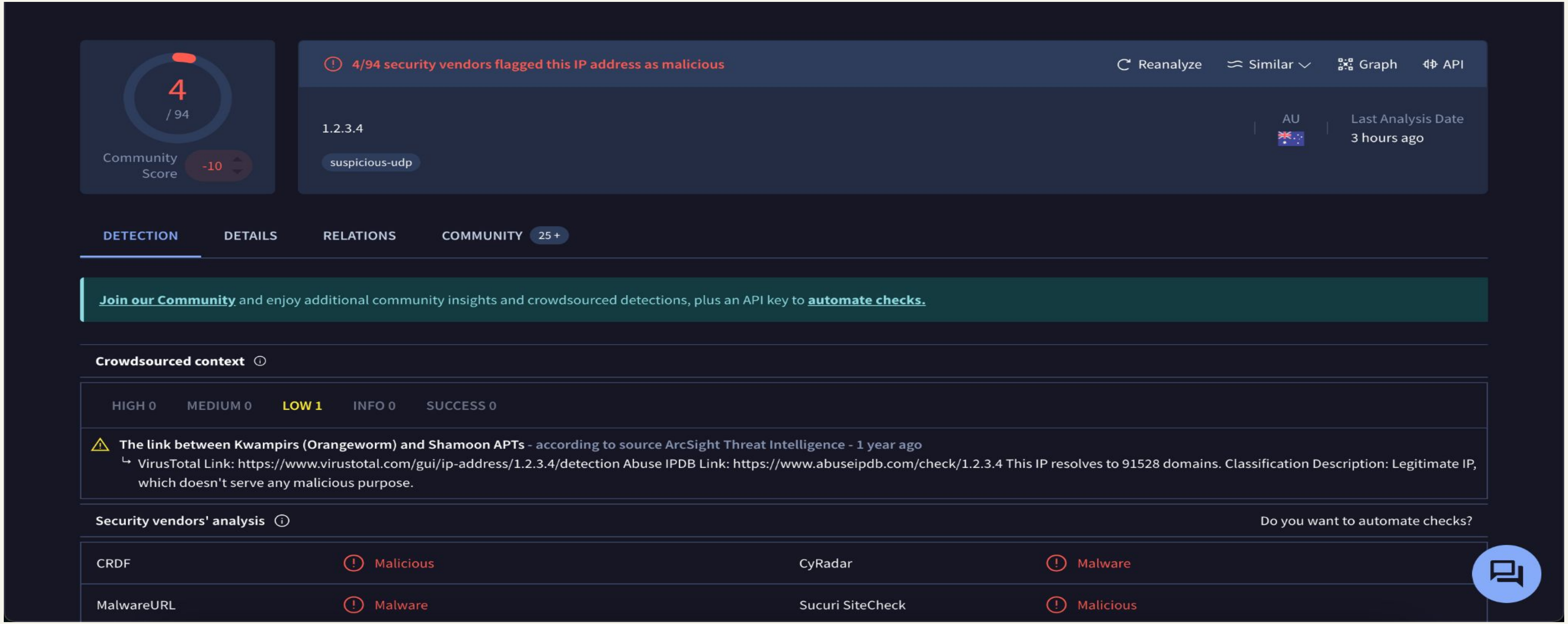
Cybersecurity Incident
& Vulnerability Response Playbooks

Operational Procedures for Planning and
Conducting Cybersecurity Incident and Vulnerability
Response Activities in FCEB Information Systems

Data :

Exfiltration Detection:

- Observed the exfiltration of the file ring.txt using AWS CLI.
- Activity sourced from IP address 1.2.3.4.
- Actions linked to suspicious GetObject events targeting a storage bucket.



4/94 security vendors flagged this IP address as malicious

1.2.3.4

suspicious-udp

AU

Last Analysis Date
3 hours ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Crowdsourced context

HIGH 0 MEDIUM 0 LOW 1 INFO 0 SUCCESS 0

The link between Kwampirs (Orangeworm) and Shamoon APTs - according to source ArcSight Threat Intelligence - 1 year ago

↳ VirusTotal Link: https://www.virustotal.com/gui/ip-address/1.2.3.4/detection Abuse IPDB Link: https://www.abuseipdb.com/check/1.2.3.4 This IP resolves to 91528 domains. Classification Description: Legitimate IP, which doesn't serve any malicious purpose.

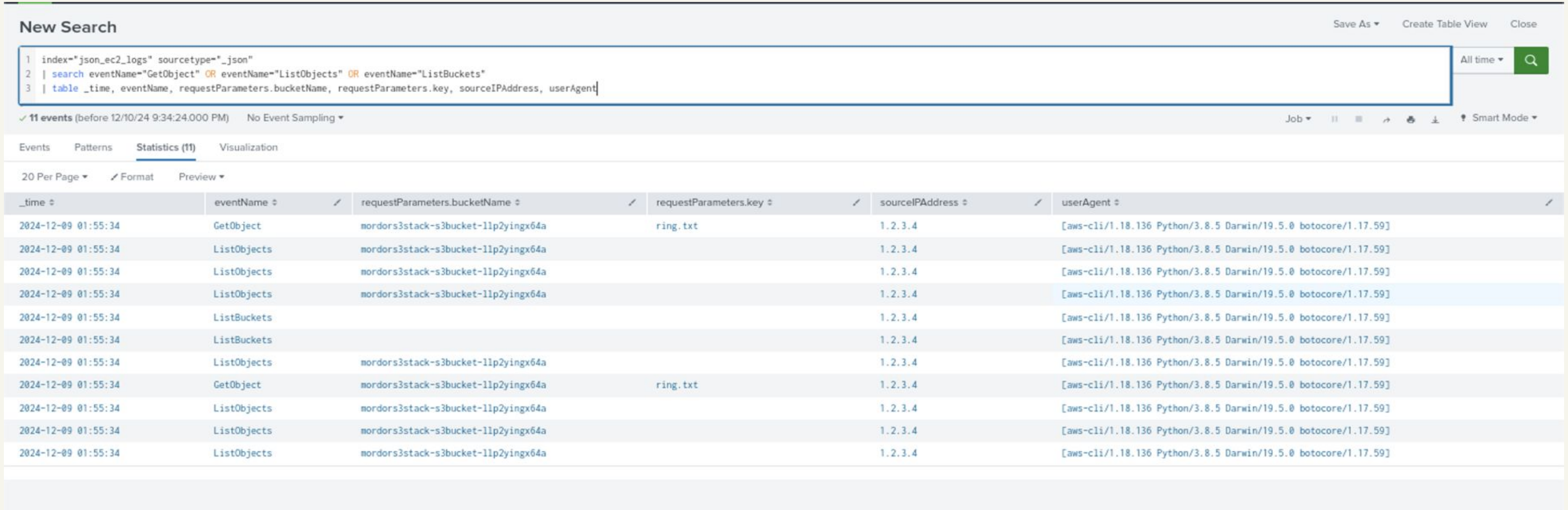
Security vendors' analysis

Do you want to automate checks?

CRDF	Malicious	CyRadar	Malware
MalwareURL	Malware	Sucuri SiteCheck	Malicious

Connecting Events to Data Theft:

- Found multiple ListObjects and GetObject events.
- These events suggest file scanning and possible data theft.
- Indicates a clear link between suspicious activity and the targeted bucket.



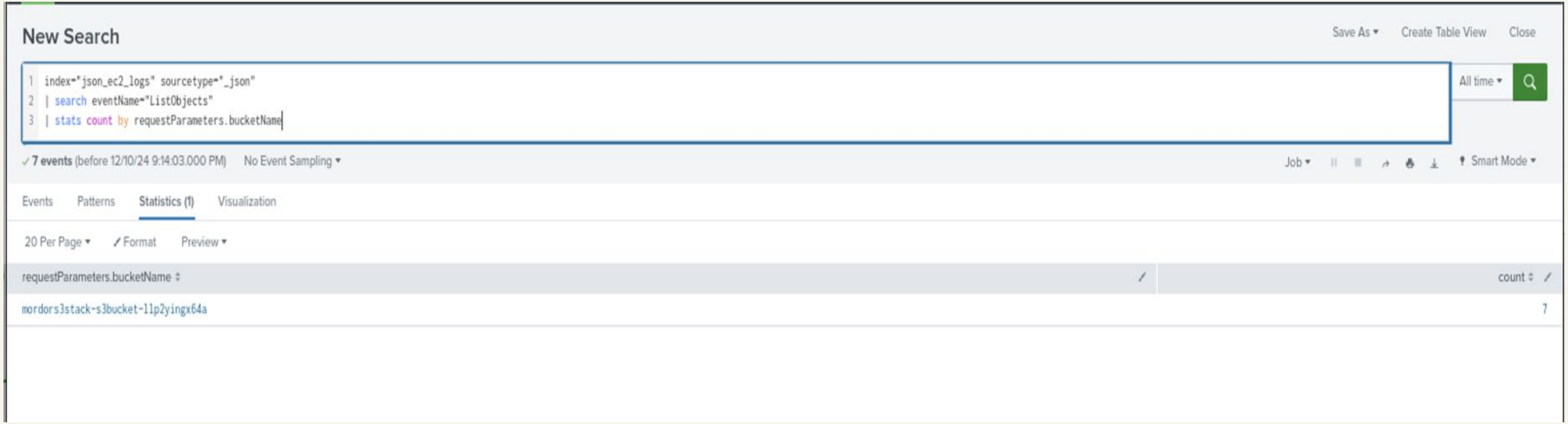
```
index="json_ec2_logs" sourcetype="_json"
| search eventName="GetObject" OR eventName="ListObjects" OR eventName="ListBuckets"
| table _time, eventName, requestParameters.bucketName, requestParameters.key, sourceIPAddress, userAgent
```

✓ 11 events (before 12/10/24 9:34:24.000 PM) No Event Sampling ▾

_time	eventName	requestParameters.bucketName	requestParameters.key	sourceIPAddress	userAgent
2024-12-09 01:55:34	GetObject	mordors3stack-s3bucket-1lp2yingx64a	ring.txt	1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	ListObjects	mordors3stack-s3bucket-1lp2yingx64a		1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	ListObjects	mordors3stack-s3bucket-1lp2yingx64a		1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	ListObjects	mordors3stack-s3bucket-1lp2yingx64a		1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	ListBuckets			1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	ListBuckets			1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	ListObjects	mordors3stack-s3bucket-1lp2yingx64a		1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	GetObject	mordors3stack-s3bucket-1lp2yingx64a	ring.txt	1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	ListObjects	mordors3stack-s3bucket-1lp2yingx64a		1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	ListObjects	mordors3stack-s3bucket-1lp2yingx64a		1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]
2024-12-09 01:55:34	ListObjects	mordors3stack-s3bucket-1lp2yingx64a		1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]

Bucket Scanning Analysis:

- **Bucket Identified:** The S3 bucket mordors3stack was accessed multiple times.
- **Repeated Actions:** Several ListObjects events suggest scanning for files.
- **Key Insight:** Indicates preparation for potential data theft.



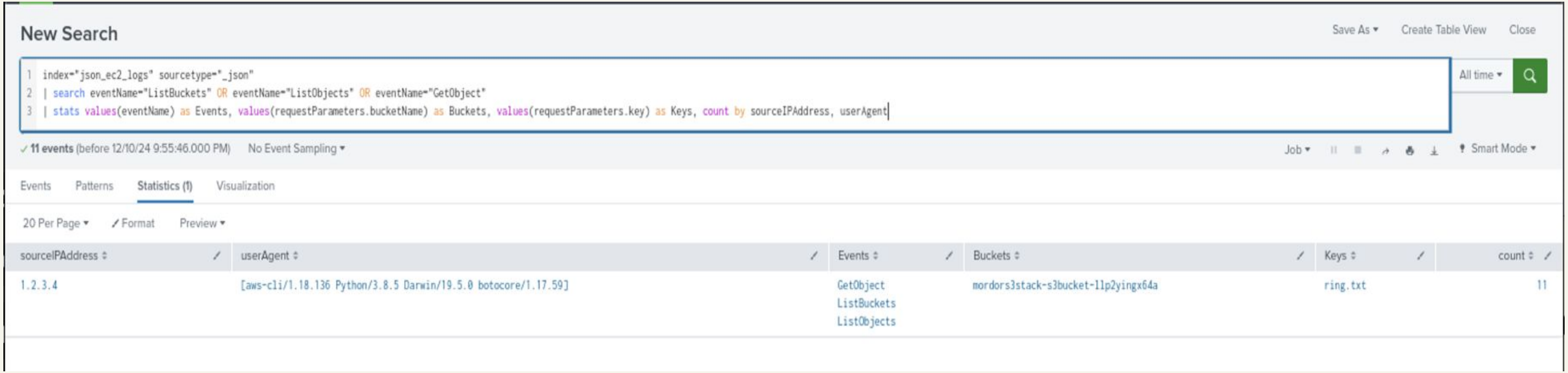
```
index="json_ec2_logs" sourcetype="_json"
| search eventName="ListObjects"
| stats count by requestParameters.bucketName
```

✓ 7 events (before 12/10/24 9:14:03.000 PM) No Event Sampling ▾

requestParameters.bucketName	count
mordors3stack-s3bucket-1lp2yingx64a	7

Data Scanning and Exfiltration Connection:

- **What Happened:** IP address 1.2.3.4 accessed and scanned bucket contents.
- **File Targeted:** The file ring.txt was accessed using AWS CLI commands.
  - The tool aws-cli/1.18.136 was used repeatedly.
- ❖ **Key Insight:** Clear evidence links bucket scanning activity to the theft of sensitive data.



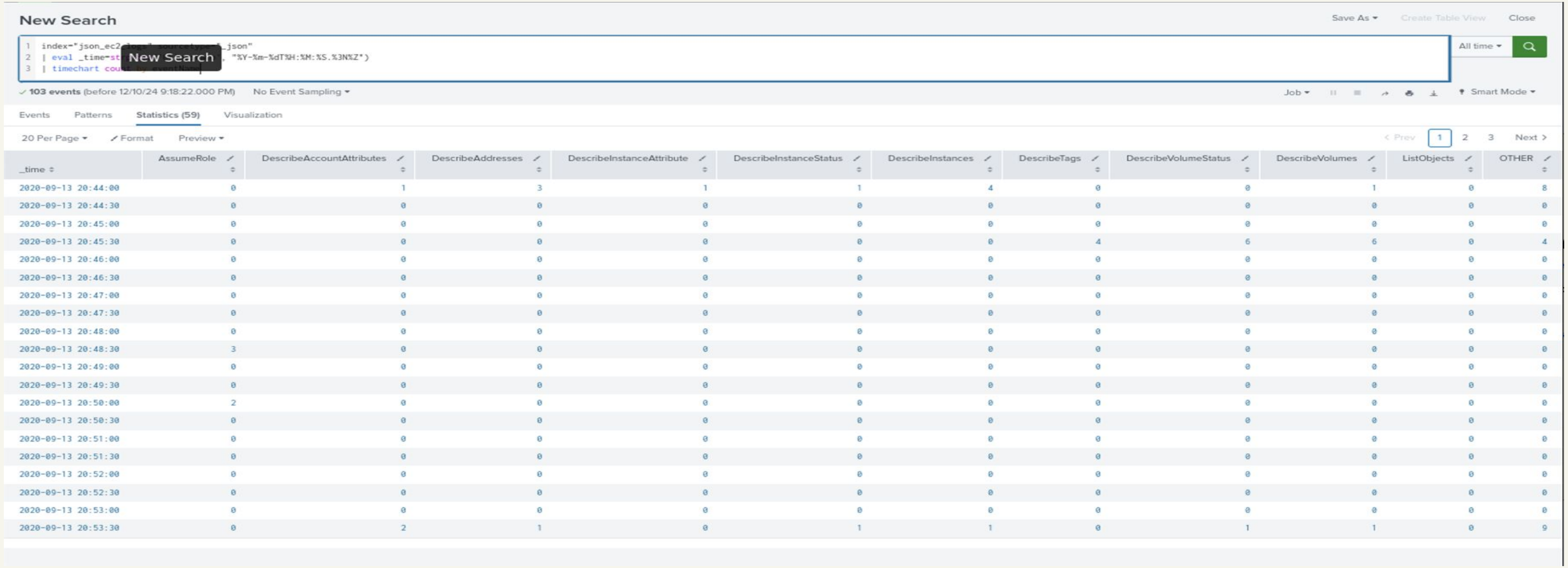
```
index="json_ec2_logs" sourcetype="_json"
| search eventName="ListBuckets" OR eventName="ListObjects" OR eventName="GetObject"
| stats values(eventName) as Events, values(requestParameters.bucketName) as Buckets, values(requestParameters.key) as Keys, count by sourceIPAddress, userAgent
```

✓ 11 events (before 12/10/24 9:55:46.000 PM) No Event Sampling ▾

sourceIPAddress	userAgent	Events	Buckets	Keys	count
1.2.3.4	[aws-cli/1.18.136 Python/3.8.5 Darwin/19.5.0 botocore/1.17.59]	GetObject ListBuckets ListObjects	mordors3stack-s3bucket-1lp2yingx64a	ring.txt	11

Attack Timeline:

- Showed the sequence of suspicious events.
- Revealed patterns of scanning and data theft.
- Highlighted key moments in the attack's progression.



```
index="json_ec2_logs" sourcetype="_json"
| eval _time=st New Search , "%Y-%m-%dT%H:%M:%S.%3N%Z")
| timechart count by eventName
```

✓ 103 events (before 12/10/24 9:18:22.000 PM) No Event Sampling

_time	AssumeRole	DescribeAccountAttributes	DescribeAddresses	DescribeInstanceAttribute	DescribeInstanceStatus	DescribeInstances	DescribeTags	DescribeVolumeStatus	DescribeVolumes	ListObjects	OTHER
2020-09-13 20:44:00	0	1	3	1	1	4	0	0	1	0	8
2020-09-13 20:44:30	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:45:00	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:45:30	0	0	0	0	0	0	4	6	6	0	4
2020-09-13 20:46:00	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:46:30	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:47:00	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:47:30	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:48:00	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:48:30	3	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:49:00	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:49:30	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:50:00	2	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:50:30	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:51:00	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:51:30	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:52:00	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:52:30	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:53:00	0	0	0	0	0	0	0	0	0	0	0
2020-09-13 20:53:30	0	2	1	0	1	1	0	1	1	0	9

Remediation:

Areas of Weakness:

- Publicly accessible S3 bucket.
- No IP restrictions in place.
- Limited monitoring for suspicious activities.
- Potential misuse of AWS credentials.

Recommended Remediation:

- Restrict S3 bucket access to authorized users.
- Allow specific trusted IP addresses to access AWS resources,
- Set up logging and alerts for unusual activity.
- Rotate and secure AWS credentials.

What we Learned:

- **Was our hypothesis correct?:**
  - Yes, the analysis confirmed unauthorized access and data theft from an S3 bucket.
- **New Findings:**
  - User agents and IPs exposed threat behavior.
  - Events from the data set showed attackers searching for files.
- **Insights Gained:**
  - **Playbooks:** Gave clear steps for handling the incident.
  - **Threat analysis:** Helped us identify suspicious events.
  - **Documentation:** Made findings easier to share and improved processes.

Thank You!