How to run a real-world attack on cloud and protect from it

@Rootcon 2024

by Niko Akatyev

27th Sep 2024

HORANGI. A BITDEFENDER COMPANY.

Creating a safer cyberspace

Nikolay “Niko” Akatyev

As the Vice President of Security, IT, Compliance, Niko drives the internal machine that powers Horangi's efforts in contributing to a safer cyberspace. He is a regular speaker and contributor in the international cybersecurity community, from Asia to the Caribbean.

Work experience

- Horangi, a Bitdefender company (Current)
- KITRI BoB Digital Forensics Mentor (Current)
- Advisor of Cashtree, and Advisor/Investor of Teiren
- Former Senior Security Researcher at LG Vehicle Components
- Former Hallym University Researcher

11 years security experience

15 years software engineer

Pioneered Cyber Peacekeeping Academic Research

Presented @ SecuInside, VXCon, Microsoft Conf, ICDF2C, AIS3 etc.

Organizing committee of ICDF2C and GCC.

www.linkedin.com/in/kolyaak

Related talks

We ran this workshop first time in Nov 2023 in South Korea and May 2024 in Singapore.

We received the positive feedback from attendees.
So we improve on it and turn it to a talk for Rootcon 2024!

My experience with cloud security

Building in cloud (and securing it) since 2016, it looked totally different then.

Teaching cloud security at BoB for past 3 years.

Started building internal cloud security monitoring 4 years ago.

Using our own product and services.

Ran two TTX in the hybrid environment.

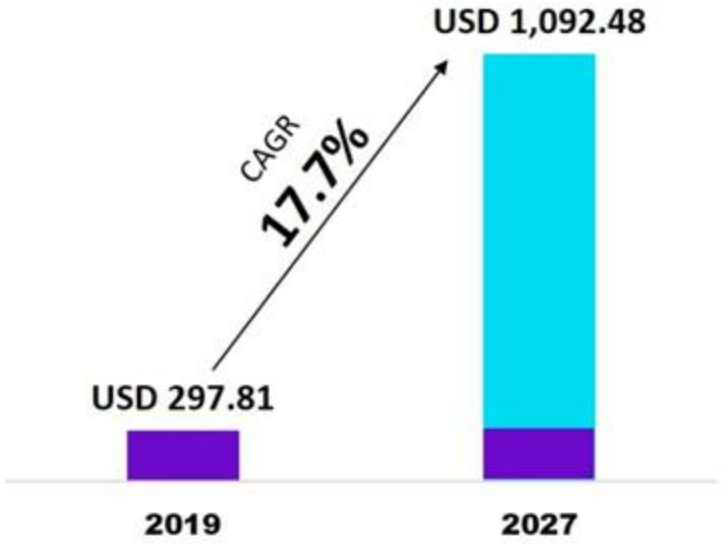
Outline of the presentation

- A quick intro to cloud and cloud security
- History of cloud breaches
- Case studies
- Threat detection in cloud
- Attack simulation

Cloud

Market

Global Cloud Computing Market Size (USD Bn) 2019-2027



- **SaaS** service segment dominated the market by nearly **55%** in 2019
- **Healthcare** segment projected to grow with the fastest CAGR of **18.6%** during 2020 to 2027
- **Asia Pacific** expected to grow with fastest CAGR of **18.5%** during the forecast period

Source: ReportCrux Market Research

Impact of cybersecurity issues

Cost of a breach

The global average cost of a data breach in 2023 was **USD 4.45 million**, a 15% increase over 3 years.
Source: IBM Cost of a Data Breach Report, 2023

Damaging

GoldenEye ransomware inflicted around $1 billion in damages to its victims.
Source: Bitdefender Business Insights

Scale of the problem

On average, 1 cloud misconfiguration is identified every 20 seconds.

Source: Horangi Threat Report, Covering H1 2023

Detect breach to survive

We live in a norm where it is not “if” but “when” data breach happens.

30,458 security incidents, of which 10,626 were confirmed data breaches in 2024 Data Breach Investigations Report (DBIR) by Verizon.

So, it's paramount to be able to detect a security event and respond to a breach timely.

Cloud Security

Quick Intro

Fundamentals of cloud

On demand resources.

API.

Management plane.

Workloads.

Cloud security

Security of the management plane.

Security of workloads.

Cloud native.

Cloud security

Misconfigurations.

Unmanaged resources - complexity and speed of deployment.

Vulnerabilities in workloads, e.g. instances, Kubernetes, containers.

Vulnerabilities of the platform. The recent vulnerability with AWS ECR.

Threat detection.

Cloud Breaches

History that is a reality

Breaches

2023

AA: recruiting provider

ChatGPT: bug in the code

earlier

Twitter: unpatched vulnerability

Okta: compromised third party service

LastPass: compromised developer’s laptop

Cloud breaches

2023

Circle CI

2022

Uber: compromised AWS server.

Pegasus Airlines: misconfigured S3 bucket. 6.5 Terabytes.

earlier

Facebook: exposed AWS server.

Raychat: misconfigured Mongo DB.

No Security is More Expensive

Equifax
- $700 mln
- 145.5 mln consumers' data

Capital One
- $100 mln - $500 mln
- 106 mln consumers' data

Marriott
- $124 mln in Europe
- 500 mln user data

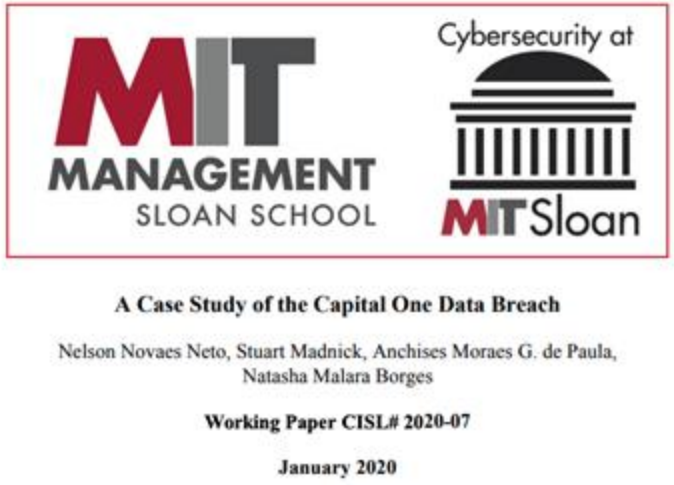
Interpark
- 4.5 bln won ($3.8 million)
- 10 mln users data

Case study

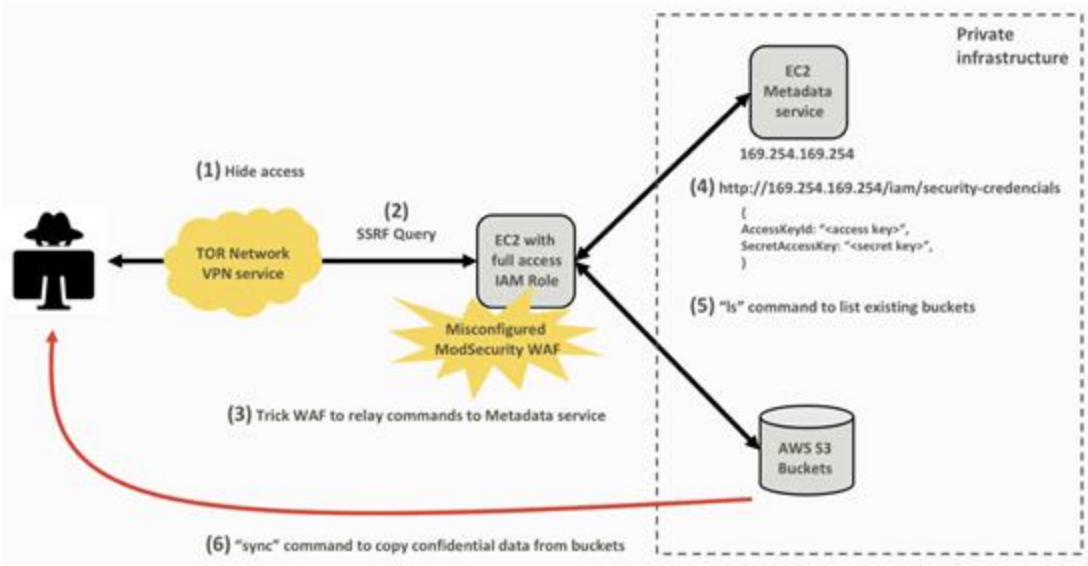
Capital One

Capital One

Using a case study of Capital One breach.
http://web.mit.edu/smadnick/www/wp/2020-07.pdf



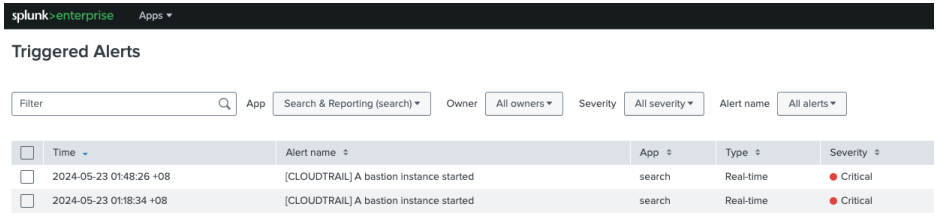
Anatomy of Capital One attack

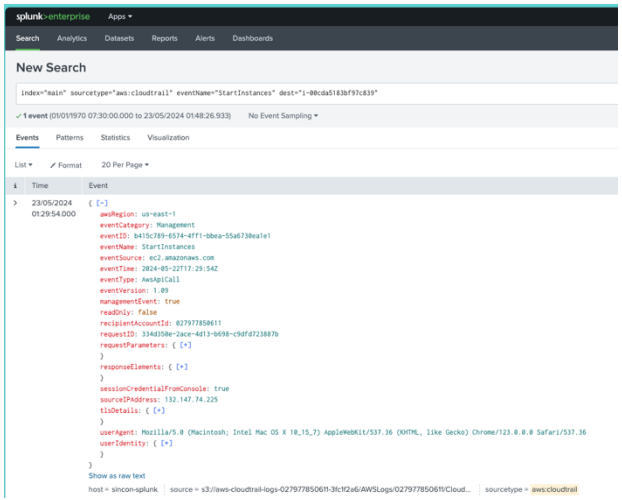


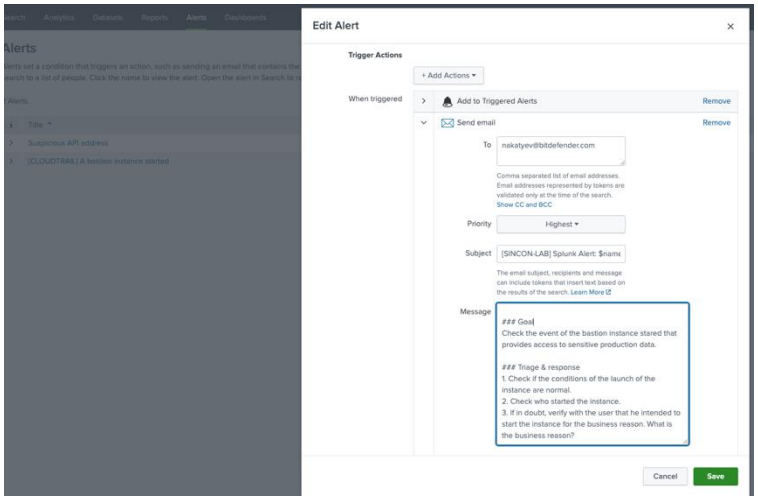
Threat Detection in Cloud

Security monitoring

Cloud security alert





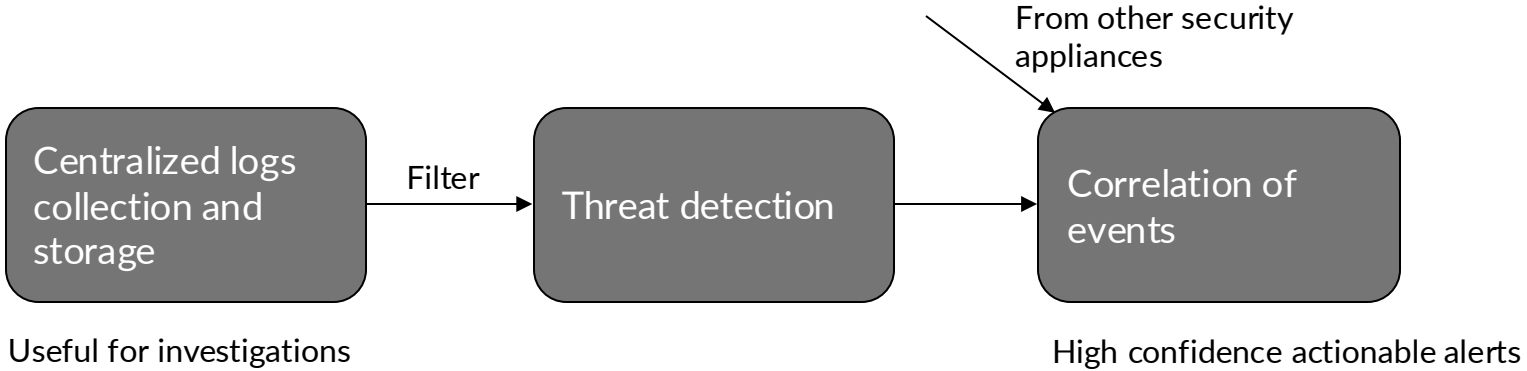


Detection based on CloudTrail

GuardDuty findings

Splunk alerts

Datadog OOTB detection rules



Quick intro to CloudTrail

```
"userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDABBBBBBBBBBBBBBBBB",
    "arn": "arn:aws:iam::111111111111:user/alice",
    "accountId": "111111111111",
    "userName": "alice"
```

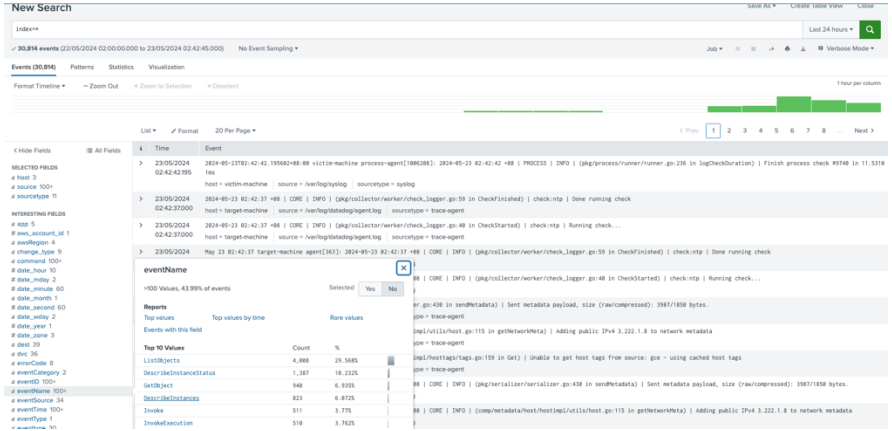
```
"eventTime": "2020-09-23T09:09:56Z",
"eventSource": "signin.amazonaws.com",
"eventName": "ConsoleLogin",
"awsRegion": "us-east-1",
"sourceIPAddress": "1.2.3.4",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like G
```

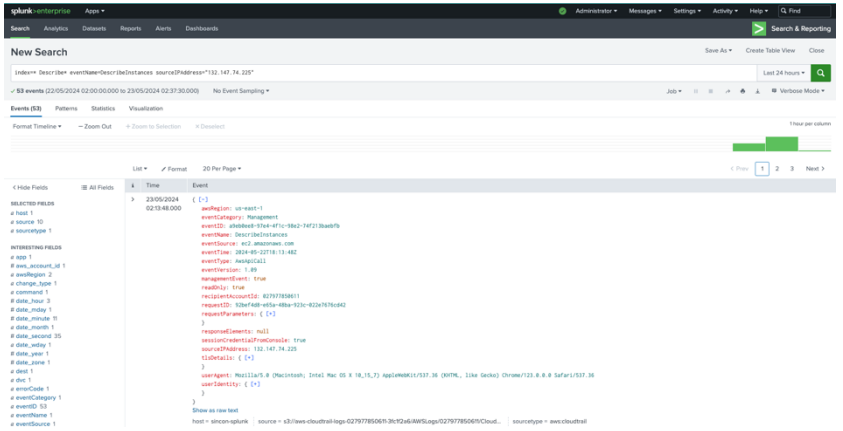
https://www.datadoghq.com/blog/monitoring-cloudtrail-logs/

Triage

- First quickly confirm whether the security event indicates an incident.
- Confirm severity.
- If it's critical, urgently continue the detailed analysis.
- If it indicates an incident, start the incident response process.

Splunk search

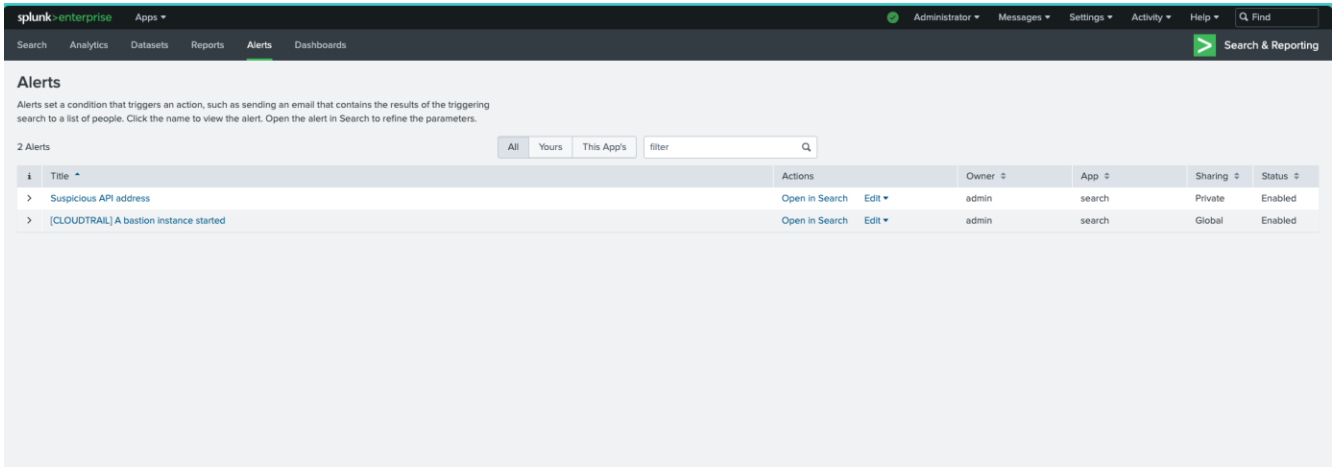




Splunk query

- Start with "index=*", set specific date/time range.
- Select and add fields into the query.
- By default, parts of the query joint with AND
- Use AND NOT to filter out noise
- `index=* AND NOT userAgent="Datadog" AND NOT userAgent="rds.amazonaws.com"`

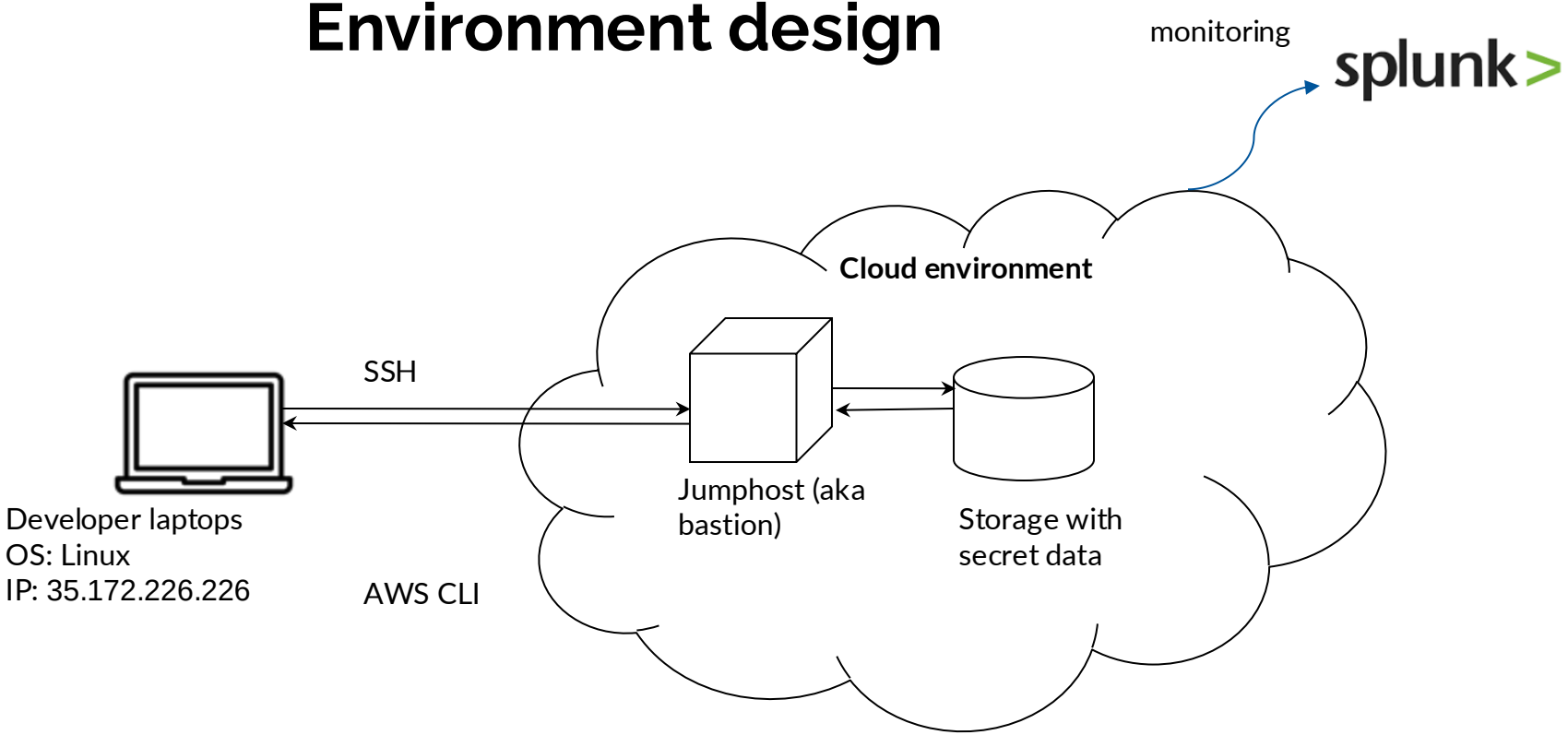
Splunk alerts



Run cloud attack

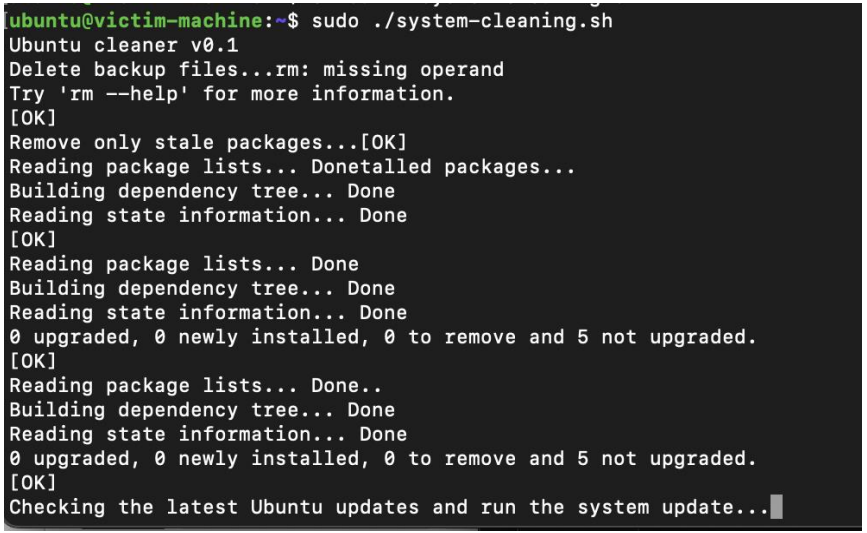
Real-world simulation

Environment design



Initial attack vector

- Compromise of the developer laptop



Misconfigurations

- Cloud misconfigurations to exploit

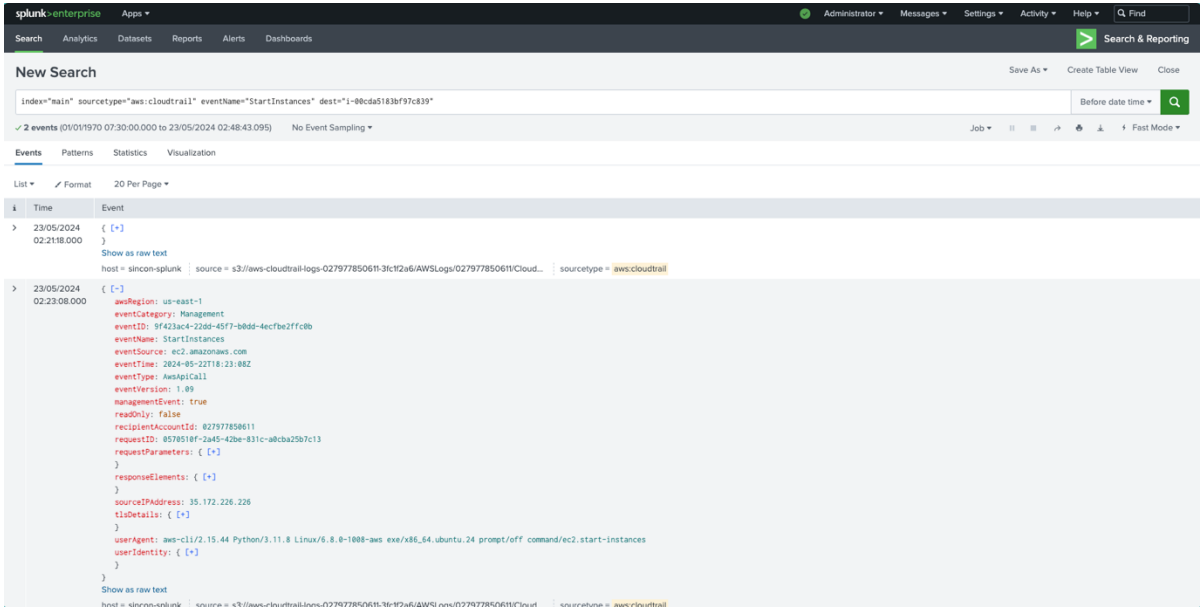
Notification and analysis of cloud security alert

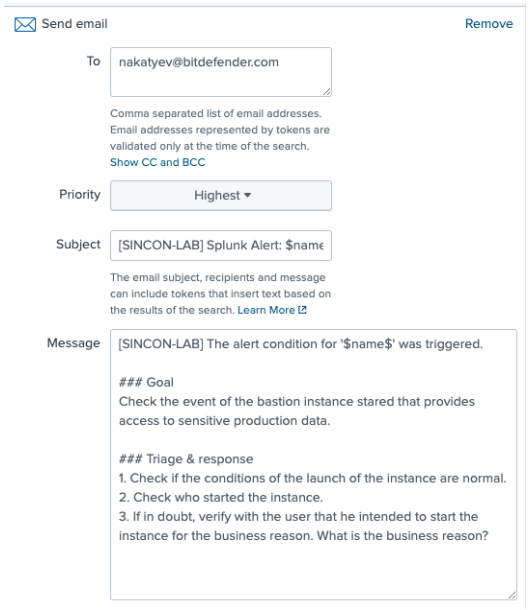
Triage

Collection of additional data

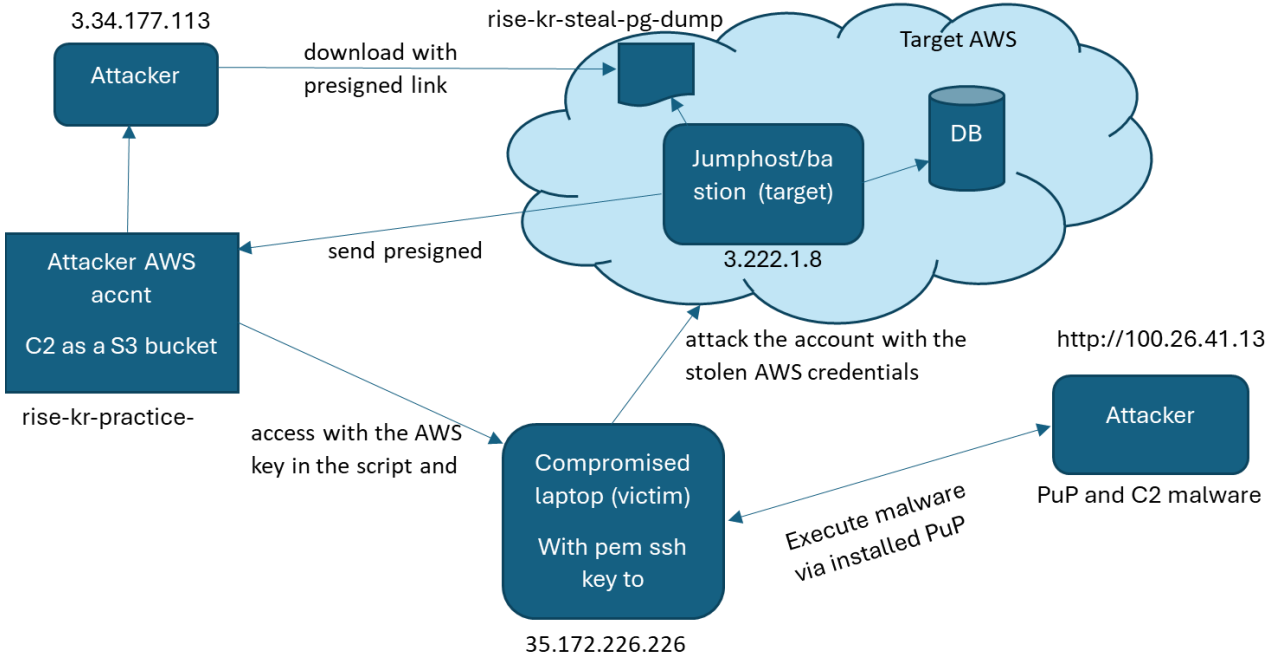
Confirmation of the incident

Alert


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="main" sourcetype="aws:cloudtrail" eventName="StartInstances" dest="i-00cda5183bf97c839"
Before date time
2 events (01/01/1970 07:30:00.000 to 23/05/2024 02:48:43.095)
No Event Sampling
Job
Fast Mode
Events
Patterns
Statistics
Visualization
List
Format
20 Per Page
Time
Event
23/05/2024 02:21:18.000
{ [+] }
Show as raw text
host = sincon-splunk
source = s3://aws-cloudtrail-logs-027977850611-3fc1f2a6/AWSLogs/027977850611/Cloud...
sourcetype = aws:cloudtrail
23/05/2024 02:23:08.000
{ [-]
awsRegion: us-east-1
eventCategory: Management
eventID: 9f423ac4-22dd-45f7-b0dd-4ecfbe2ffc0b
eventName: StartInstances
eventSource: ec2.amazonaws.com
eventTime: 2024-05-22T18:23:08Z
eventType: AwsApiCall
eventVersion: 1.09
managementEvent: true
readOnly: false
recipientAccountId: 027977850611
requestID: 0570510f-2a45-42be-831c-a0cba25b7c13
requestParameters: { [+] }
responseElements: { [+] }
sourceIPAddress: 35.172.226.226
tlsDetails: { [+] }
userAgent: aws-cli/2.15.44 Python/3.11.8 Linux/6.8.0-1008-aws exe/x86_64.ubuntu.24 prompt/off command/ec2.start-instances
userIdentity: { [+] }
}
Show as raw text


Send email
Remove
To
nakatyev@bitdefender.com
Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.
Show CC and BCC
Priority
Highest
Subject
[SINCON-LAB] Splunk Alert: $name
The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More
Message
[SINCON-LAB] The alert condition for '$name$' was triggered.
Goal
Check the event of the bastion instance stared that provides access to sensitive production data.
Triage & response
1. Check if the conditions of the launch of the instance are normal.
2. Check who started the instance.
3. If in doubt, verify with the user that he intended to start the instance for the business reason. What is the business reason?

Attack flow


3.34.177.113
Attacker
download with
presigned link
rise-kr-steal-pg-dump
Target AWS
DB
Jumphost/ba
stion (target)
3.222.1.8
send presigned
Attacker AWS
accnt
C2 as a S3 bucket
rise-kr-practice-
attack the account with the
stolen AWS credentials
http://100.26.41.13
Attacker
PuP and C2 malware
access with the AWS
key in the script and
Compromised
laptop (victim)
With pem ssh
key to
35.172.226.226
Execute malware
via installed PuP

Q&A

https://www.linkedin.com/in/kolyaak/
nakatyev@bitdefender.com