

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.



Speaker Intro.

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.

HORANGI. A BITDEFENDER COMPANY.



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.

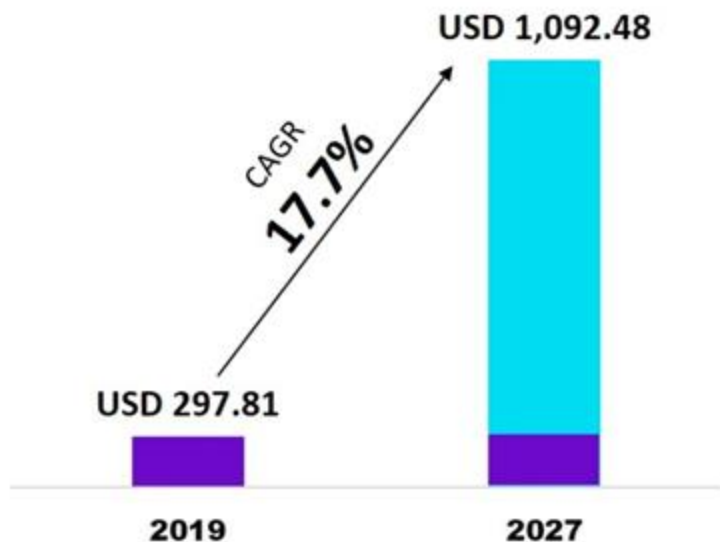
Outline of the presentation

- 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>



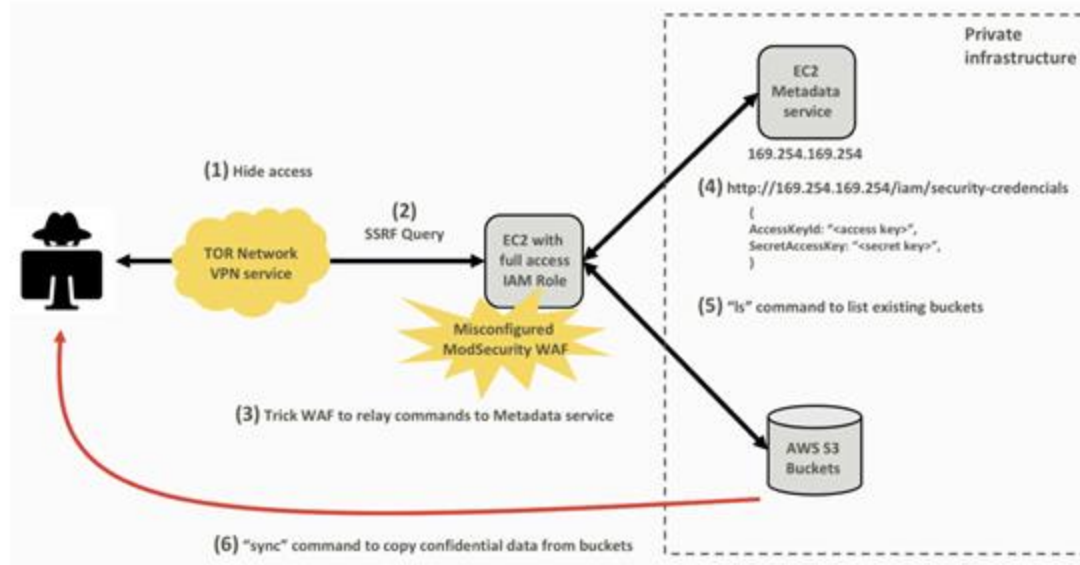
A Case Study of the Capital One Data Breach

Nelson Novaes Neto, Stuart Madnick, Anchises Moraes G. de Paula,
Natasha Malara Borges

Working Paper CISL# 2020-07

January 2020

Anatomy of Capital One attack



Threat Detection in Cloud

Security monitoring

Cloud security alert

splunk>enterprise Apps ▾

Triggered Alerts

Filter App Search & Reporting (search) ▾ Owner All owners ▾ Severity All severity ▾ Alert name All alerts ▾

<input type="checkbox"/>	Time ▾	Alert name ▾	App ▾	Type ▾	Severity ▾
<input type="checkbox"/>	2024-05-23 01:48:26 +08	[CLOUDTRAIL] A bastion instance started	search	Real-time	● Critical
<input type="checkbox"/>	2024-05-23 01:18:34 +08	[CLOUDTRAIL] A bastion instance started	search	Real-time	● Critical

splunk>enterpriseApps ▾

SearchAnalyticsDatastoreportsAlertsDashboards

New Search

index="main" sourcetype="aws-cloudtrail" eventName="StarInstances" dest="1-8bda6183bf73c39"

✓ 1 event (01/01/1970 07:30:00.000 to 23/05/2024 01:48:26.933) No Event Sampling ▾

EventsPatternsStatisticsVisualization

List ▾Format20 Per Page ▾

Time	Event
23/05/2024 01:29:54.000	<pre>{ "region": "us-east-1", "eventCategory": "Management", "eventID": "b415c789-6534-4f71-bbea-55a673bea1e1", "eventName": "StarInstances", "eventSource": "ec2.amazonaws.com", "eventTime": "2024-05-22T17:29:54Z", "eventType": "AwsApiCall", "eventVersion": 1.89, "managementEvent": true, "readOnly": false, "recipientAccountID": "827977850611", "requestID": "334d558e-2ace-4d11-b698-c9df6723887b", "requestParameters": { "": {} }, "responseElements": { "": {} }, "sessionCredentialFromConsole": true, "sourceIPAddress": "132.147.74.225", "details": { "": {} }, "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 18_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.8.8.8 Safari/537.36", "userIdentity": { "": {} } }</pre>

Show as raw text

host = sincon-splunk | source = s3://aws-cloudtrail-logs-02797785061-31c12d6/AWSLogs/02797785061/Cloud... | sourcetype = awscloudtrail

SearchAnalyticsDatastoreportsAlertsDashboards

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the search to a list of people. Click the name to view the alert. Open the alert in Search to...

Alerts

- Title *
- Suspicious API address
- [CLOUDTRAIL] A bastion instance started

Edit Alert

Trigger Actions

+ Add Actions ▾

When triggered

Add to Triggered AlertsRemove

Send emailRemove

To

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search. Show CC and BCC.

PriorityHighest ▾

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 ID

Message

Goal
Check the event of the bastion instance started 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?

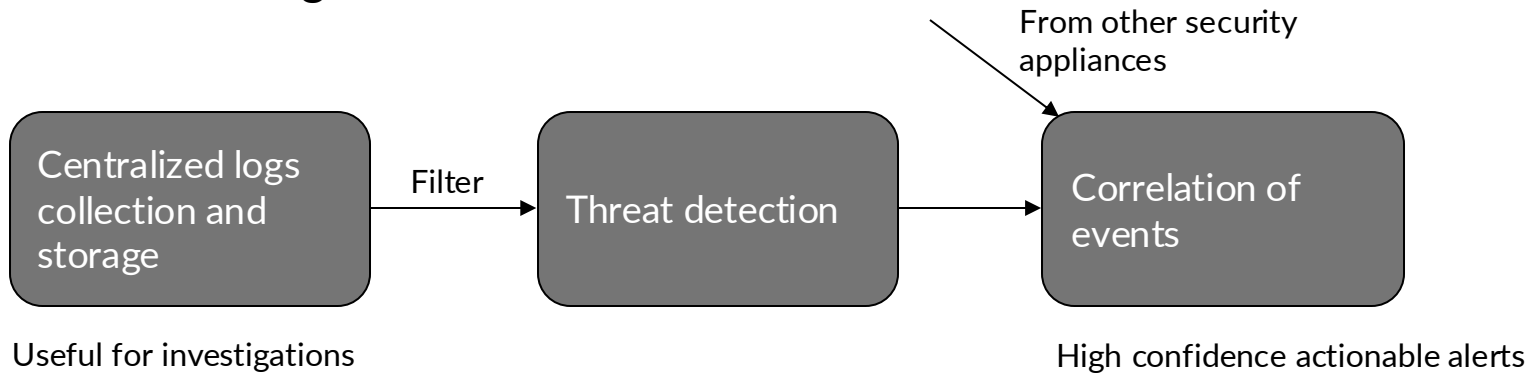
CancelSave

Detection based on CloudTrail

GuardDuty findings

Splunk alerts

Datadog OOTB detection rules



Quick intro to CloudTrail

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAB8888888888888888",
    "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 Gecko) Chrome/86.0.4267.160 Safari/537.36",
  "requestParameters": null,
  "responseElements": {
    "ConsoleLogin": "Success"
  },
  "additionalEventData": {
    "LoginTo": "https://console.aws.amazon.com/console/home",
    "MobileVersion": "No",
    "MFALUsed": "No"
  },
  "eventID": "a994a371-9f3a-47bd-b75c-5f6ca347281a",
  "eventType": "AwsConsoleSignIn",
  "recipientAccountId": "111111111111"
}
```

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAB8888888888888888",
  "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 Gecko) Chrome/86.0.4267.160 Safari/537.36"
```

<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.
-

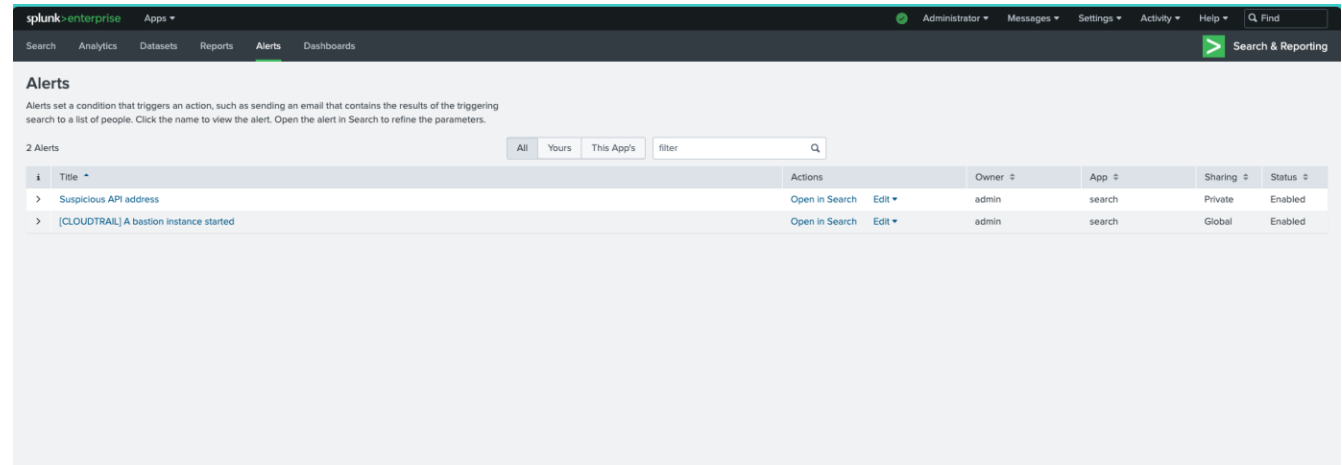
Splunk search

[illegible][illegible]

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



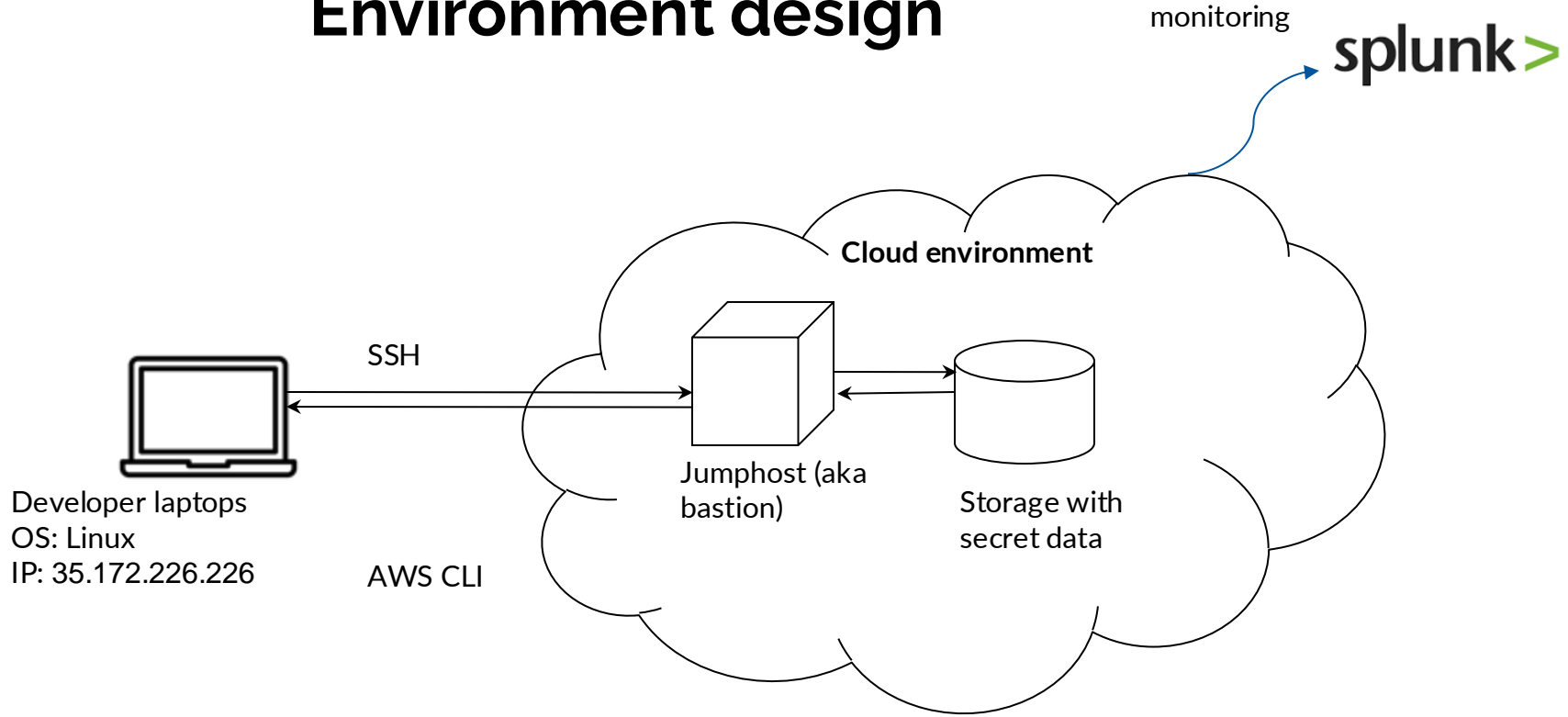
The screenshot displays the Splunk Alerts management page. At the top, the navigation bar includes 'splunk > enterprise', 'Apps', and user settings like 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this, a secondary navigation bar lists 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts' (which is highlighted), and 'Dashboards'. On the right of this bar is a 'Search & Reporting' button. The main content area is titled 'Alerts' and contains a brief explanation: 'Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.' Below the text, it shows '2 Alerts' and a filter bar with tabs for 'All', 'Yours', and 'This App's', followed by a search input field. A table lists the alerts with columns for 'i', 'Title', 'Actions', 'Owner', 'App', 'Sharing', and 'Status'. Two alerts are listed: 'Suspicious API address' and '[CLOUDTRAIL] A bastion instance started', both owned by 'admin' and associated with the 'search' app.

i	Title	Actions	Owner	App	Sharing	Status
>	Suspicious API address	Open in Search Edit	admin	search	Private	Enabled
>	[CLOUDTRAIL] A bastion instance started	Open in Search Edit	admin	search	Global	Enabled

Run cloud attack

Real-world simulation

Environment design



Initial attack vector

- Compromise of the developer laptop

```
ubuntu@victim-machine:~$ sudo ./system-cleaning.sh
Ubuntu cleaner v0.1
Delete backup files...rm: missing operand
Try 'rm --help' for more information.
[OK]
Remove only stale packages...[OK]
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
[OK]
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
[OK]
Reading package lists... Done..
Building dependency tree... Done
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.
[OK]
Checking the latest Ubuntu updates and run the system update...
```

Misconfigurations

- Cloud misconfigurations to exploit

Notification and analysis of cloud security alert

Triage

Collection of additional data

Confirmation of the incident

Alert

splunkenterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Index="main" sourcetype="aws:cloudtrail" eventName="StartInstances" dest="1-8cda5183f97c839"

2 events (01/01/1970 07:30:00.000 to 23/05/2024 02:48:43.095) No Event Sampling

EventsPatternsStatisticsVisualization

ListFormat20 Per Page

i	Time	Event
>	23/05/2024 02:21:18.000	<div>{ }</div> <div>Show as raw text</div> <div>host = sincon-splunk source = s3://aws-cloudtrail-logs-027977850611-3fc92a6/AWSLogs/027977850611/Cloud... sourcetype = aws:cloudtrail</div>
>	23/05/2024 02:23:08.000	<div>{ }</div> <div>Show as raw text</div> <div>awsRegion: us-east-1 eventCategory: Management eventID: 9f423ac4-226d-45f7-b8dd-4ecfba2ffc0b eventName: StartInstances eventSource: ec2.amazonaws.com eventTime: 2024-05-22T18:23:08Z eventType: AwsApiCall eventVersion: 1.09 managementEvent: true readOnly: false recipientAccountId: 827977850611 requestID: 8578518f-2a45-42be-831c-a8c2a25b7c13 requestParameters: { } responseElements: { } sourceIPAddress: 35.172.226.226 timestamp: 1716411788000 userIdentity: { }</div> <div>Show as raw text</div> <div>host = sincon-splunk source = s3://aws-cloudtrail-logs-027977850611-3fc92a6/AWSLogs/027977850611/Cloud... sourcetype = aws:cloudtrail</div>

Send emailRemove

To: nakatyeve@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

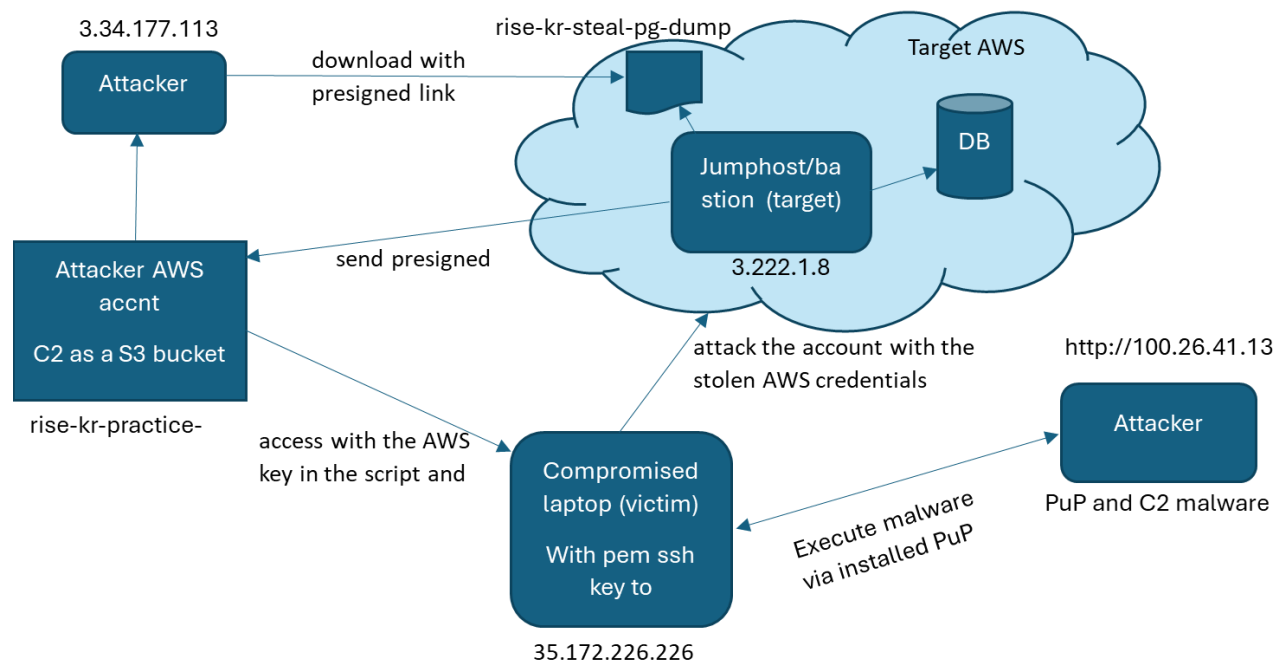
The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message: [SINCON-LAB] The alert condition for "\$name\$" was triggered.

Goal
Check the event of the bastion instance stated 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



Q&A

[https://www.linkedin.com/in/kolyaak/
nakatyevev@bitdefender.com](https://www.linkedin.com/in/kolyaak/nakatyevev@bitdefender.com)
