# Example Incident Report: **Cloud Response for Microsoft 365**

**An incident report is a detailed account of a security breach or cyberattack.**

**BREACHES:** A specific type of security incident that involves unauthorized access or retrieval of data.

**CYBERATTACKS:** An attempt by cybercriminals to damage or destroy a computer network or system.

It typically includes information about how the incident occurred, the extent of the damage, the steps taken to resolve the issue, and recommendations for preventing future incidents. These reports are crucial for understanding the nature and impact of cyberthreats, aiding in swift response and remediation, and facilitating better cybersecurity practices to prevent similar incidents in the future.

**With incident reports, you can learn how to tell our data's story.** Harness our frontline experience to learn threat actors' behavior and showcase the value of your Blackpoint Cyber offering.

**More specifically, Blackpoint incident reports for Cloud Response include:**

- A summary
- Specific times of events
- Accounts involved
- Indicators of compromise
- Ticket information
- Post-incident actions

**In our first example incident report,** we encounter a suspicious inbox rule moving emails to a specific folder. As with all incidents, the Blackpoint team followed up with the partner via email and phone call. In this instance, a senior MDR analyst spoke to the end client to ensure they understood the incident, as well as how proceed with remediation.

**In our second example incident report,** we encounter login activity associated with a Cloud Virtual Private Server based in Saudi Arabia and associated with an Iran domain. It is worth noting that Iran is deemed one of Blackpoint's high-risk locations. Within one minute, a senior MDR analyst began investigation and disabled the account.

# 2023 – Pawn Manufacturing (CUSTOMER) – Knight & Bishop Financial (MSP) - Blackpoint Incident Report (Fake Data, Real Scenario)

## Summary

Blackpoint SOC was made aware of an unusual inbox rule titled “.” And “..” by the account shusky@ pawnmanufacturing [dot]com. The SOC, after reviewing the Cloud Response detection found that the suspicious inbox rule was moving emails to a folder titled, “RSS Subscriptions”. To prevent any potential further compromise and to halt potential unauthorized activity the user account and the inbox rule were disabled.

## 1.0 Notes

1420ET: Blackpoint SOC was alerted to the suspicious inbox rule called “**.**” and “..” by the account shusky@ pawnmanufacturing[dot]com.

1449ET: Blackpoint SOC Senior Analyst Jason B disabled the user account and the inbox rule to thwart any potentially unauthorized activity.

1450ET: Blackpoint SOC Senior Analyst Jason B called Pawn Manufacturing and spoke with Donald  W and provided details about the incident.

## 2.0 Accounts Involved

shusky@pawnmanufacturing[dot]com

## 3.0 IOC’s

**IP’s**
83[.]194[.]140[.]12 (Fort Worth, Texas, US) - Inbox Rule Creation

125[.]177[.]178[.]12 (Tacoma, Washington, US) - Express VPN Login

**Potential VPN/Proxy Used**
Express VPN

**Rule Name**
“.” And “..”

**Rule Action**
Forward emails to "RSS Subscriptions" Folder.

**Inbox Rule Details**
"Parameters":

[{"Name":"AlwaysDeleteOutlookRulesBlob","Value":"False"},
{"Name":"Force","Value":"False"},

{"Name":"MoveToFolder","Value":"RSS Subscriptions"},
{"Name":"Name","Value":"."},
{"Name":"FromAddressContainsWords","Value":"@lawfirm[dot]org;@lawfirm[dot]com"},
{"Name":"MarkAsRead","Value":"True"},
{"Name":"StopProcessingRules","Value":"True"}]

"Parameters":
[{"Name":"AlwaysDeleteOutlookRulesBlob","Value":"False"},
{"Name":"Force","Value":"False"},
{"Name":"MoveToFolder","Value":"RSS Subscriptions"},
{"Name":"Name","Value":".."},
{"Name":"SubjectOrBodyContainsWords","Value":"lawfirm[dot]org"},
{"Name":"MarkAsRead","Value":"True"},

{"Name":"StopProcessingRules","Value":"True"}]

## 4.0 Alerts / Tickets

SNAP Alert

TICKET#457621

## 5.0 Post Incident Actions

Reset the user's credentials.

Validate they are not using the same or similar password for other accounts.

Enable Multi-Factor-Authentication on the account if not currently implemented.

Enable Conditional Access if not already implemented.

# 2023 – Fjord Roadways (CUSTOMER) – Shovel International (MSP) - Blackpoint Incident Report (Fake Data, Real Scenario)

## Summary

Blackpoint SOC was made aware of a log in from a potential proxy IP address by the account gretriever@ fjordroadways [dot]com. The SOC, after reviewing the Cloud Response detection found that this activity was associated with a Cloud Virtual Private Server based in Saudi Arabia and associated with an Iran domain. To prevent any unauthorized activity the user account was disabled.

## 1.0 Notes

14:42 Est. Blackpoint SOC Senior MDR Analyst Joseph C. begins to investigate.

14:42 Est. Blackpoint SOC Senior MDR Analyst disables the account after discovering this is a Cloud Virtual Private Server based in Saudi Arabia and associated with an Iran Domain.

14:47 Est. Blackpoint SOC calls the customer and informs them of the incident.

## 2.0 Accounts Involved

gretriever@fjordroadways [dot]com

## 3.0 IOC's

**IP's**
95[.]177[.]110[.]22  (Tabuk, Saudi Arabia, SA)

**Potential VPN/Proxy Used**
ProxyLine

**User Agent/Browser**
Browser: Chrome
User Agent: Windows 7

## 4.0 Alerts / Tickets

SNAP Alert

Ticket #5069831

## 5.0 Post Incident Actions

Reset the user’s credentials.

Validate they are not using the same or similar password for other accounts.

Enable Multi-Factor-Authentication on the account if not currently implemented.

Enable Conditional Access if not already implemented.

Block the IOC IP Address in the connection filter.

Perform an audit of account activity while compromised.