VIGILANCE

Managed Security Services

# Security Incident Summary

This report demonstrates how Vigilance MXDR services effectively responds to threats and breaches with gold standard detection and response. Providing incident source, affected resources, and recommendations.

SUMMIT7

# Introduction

## Security Incident Summary

Cybersecurity incidents can have a devastating impact on a company's operations and reputation. Summit 7's Vigilance (MSSP) is dedicated to providing the tools and expertise needed to safeguard critical data and assets.

**This report from a real-life scenario will provide valuable insights into the mechanisms Vigilance has in place to protect against emerging threats.**

The goal of this summary is not only to highlight the effectiveness of Vigilance, but also to provide tangible proof that our client's investment in cybersecurity is justified. By examining real-life examples of Summit 7 threat detection capabilities, we can demonstrate how our clients can stay ahead of cybercriminals and minimize the potential damage of a breach.

# The Challenge

**In today's world where threats are constantly evolving and growing more sophisticated, it is essential to leverage threat intelligence in order to effectively detect, contain, investigate any breach in an environment**

# Key Highlights:

## 1. Detect

Vigilance detects a Sharepoint upload from a foreign IP promting initial triage.

## 2. Contain

Vigilance begins investigation analysis of potential affected resources.

## 3. Investigate

Vigilance submits a full analysis and offers recommendations to the client's security posture.

# [The Incident]

## Incident Date:

3/15/2023

## Client:

[redacted]

## Summary:

On 3/15/2023 S7-Vigilance discovered a SharePoint upload from a foreign IP and began triage. Interview with customer revealed additional security risks related to this incident. Based on interview with developer management **high risk behaviors were revealed** and reported as common practice by [redacted] development team. [Key Risk #3 and #4]

Upon further investigation and interview with suspected user. The team determined the alert was triggered by BYOD device using VPN services while traveling. [Key Risk #5]

## Affected Resources:

“[redacted] EnterpriseDevelopSolutions” SharePoint site

## Participants:

**Vigilance (Summit 7)**
- SOC Manager
- SOC analyst
- Jr. SOC analyst
- SOC analyst
- Jr. SOC analyst
- Customer Engineer
- vCIO

**Client participants**
- [redacted]

# Incident Timeline

3/15/23:

9:18 AM

SOC relayed to the IT POC on Email redirects pertaining to the employee [redacted] to his Gmail account.

The Team notified the SOC the account needed to have the personal email removed and verbal communication had been relayed to the end user on behavior.

Ticket opened internally within Summit 7(S7) to have the account removed

11:07AM

The SOC received an alert pertaining to the end user on OfficeActivity in relation to the "[redacted] EnterpriseDevelopSolutions" SharePoint site. Files were accessed/uploaded from an international IP from the end users account.

11:55 AM

Event triaged by (SOC Tier 1) and investigation begins

12:00 PM

Enlisted the help of (SOC Tier 2) for further investigation

12:10 PM

SOC Analyst begin gathering preliminary evidence

12:23 PM

SOC Analyst begins drafting email to [redacted]

12:38 PM

Finalized initial email sent to [redacted].

12:39 PM

SOC Tier 2 brought in on call

12:53 PM

[redacted]'s sessions were revoked by (SOC Tier 2)

12:58 PM

SOC Manager brought into call

1:00 PM

Called [redacted – IT POC], left voicemail

1:04 PM

The team begins further investigation of [redacted] actions in M365D

1:06 PM

[redacted]called back

[redacted] is [redacted] manager

1:09 PM

SOC disables [redacted] account in AAD

Informed [redacted] that the user's sessions are revoked and the account is locked.

1:10 PM

Advised [redacted IT POC] to initiate incident response.

BEGIN INCIDENT RESPONSE PROCEDURE

1:12 PM

Informed [redacted IT POC] that we will be sending the data that we have in order for them to make a judgement call.

1:13 PM

Further investigating the scope of data access

1:15 PM

IOC added to TI and Defender by the SOC team

1:16 PM

Client engineer brought into call



1:17 PM

Pulling Office Activity audit log for [redacted]

1:17 PM

Sentinel Logs exported and brought into investigation files

1:25 PM

SOC Discovered additional closed anomalous IP incidents in Sentinel generated around 11:00 AM CST

3/15/2023. Relationship was not confirmed

1:28 PM

(SOC Tier 2) received a call from [redacted - IT POC]

1:32 PM

Downloading user activity report

1:37 PM

Entered a Teams meeting call with [redacted- Devteam manager] and [redacted- IT POC] ; Call ended at 2:03pm

1:38 PM

All users have entered the call, beginning discussion.

1:40 PM

[redacted]- Devteam manager] explains:

[redacted] is a contractor, submits code to the dev repo

[redacted] - many software developers don't use the company email, they use slack

2:03 PM

Call with [redacted] end.

Tasks are delegated, begin official report construction.

2:14 PM

Discovered that the AD SYNC service re-enabled the user's account

2:14 PM

Logging into DC to disable and scramble the user's account

2:16 PM

User's account is now disabled and had the password scrambled on the DC.

Confirmed no access from the IP location outside of [redacted] office activity.

2:32 PM

[redacted – IT POC] sent second call invite to discuss further details and reports after they could be generated; call scheduled for 3:30pm CST.

3:12 PM

Email forwarding was confirmed cleared from user [redacted] inbox

3:31 PM

Joined call, members include [redacted- client team] , [Redacted SOC team memebers]

3:33 PM

Discussed the MFA configuration of the user

3:36 PM

Discussed potential insider risk and the need for MFA

3:37 PM

[redacted] client states that there is no CUI on the SharePoint site.

3:39 PM

Advised auditing the Duo Bypass group

3:40 PM

Discussed additional training that would be valuable for end users (CUI, Insider Risk, Data Handling)

3:51 PM

Suggested Countries CA implementation

Suggested auditing MFA configuration

Suggested implementing Intune joined devices

3:53 PM

Discussing Principle of Least Privilege for developers.

[redacted- Devteam manager] suggests that developers have a very narrow scope of access to SharePoint for developers

The base URL is: [redacted]

[redacted] says that there are others, but they are not active right now.

3:56 PM

Re-emphasized the importance of implementing a Countries CA

4:05 PM

Combine notes, awaiting user statement

4:30 PM

SOC Analyst got a Response for [redacted – IT POC] via text message where user indicated VPN usage being the root cause of the alert closing case as **“False Positive (by user report)”**

## Analysis:

3/15/23 11:07AM

The SOC received an alert pertaining to the end user on office activity in relation to [redacted] DevelopSolutions sharepoint site. Files were accessed from an international IP from the end users account.

## User Account Audit:

User account was tagged as “external” within the display name in AAD but account operates as an internal user account.

As per audit, no registered MFA logs on the user account due to the identity not tied to the group “grpcloudaccts” which triggers the conditional access policy to implement MFA for users. MFA is implemented

# Investigation Result

**False Positive (User Reported)**

## Affected CUI:

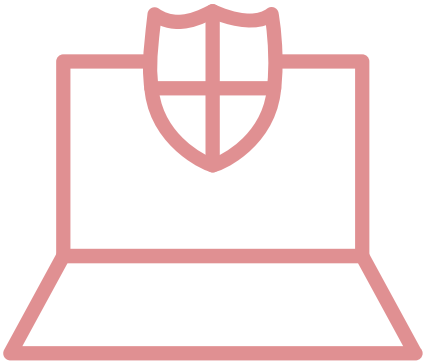
**NO**

## Key Risks:

1. Lack of MFA for Guest Users
2. Lack of user CUI Training
3. Foreign Assets accessing a CUI enclave [Rebutted]
4. Possible sharing of users credentials [Rebutted]

## Recommendations:

1. Conduct formal CUI training with users accessing the environment.
2. Audit Current MFA Policy for additional gaps
3. Notify Facility Security Officer (FSO)
4. Counsel Offending individuals (ensure VPN service is U.S. based if it must be used)



# VIGILANCE

## Managed Security Services

24/7 Threat & Intel Support

Incident Response

MXDR

Security Posture Monitoring

Microsoft Sentinel (SIEM)

**Vigilance offers gold standard MXDR services while leveraging an expert team of security professionals to provide the protection and peace of mind that organizations need to stay vigilant and focus on the core of their business.**

**Request More Information**