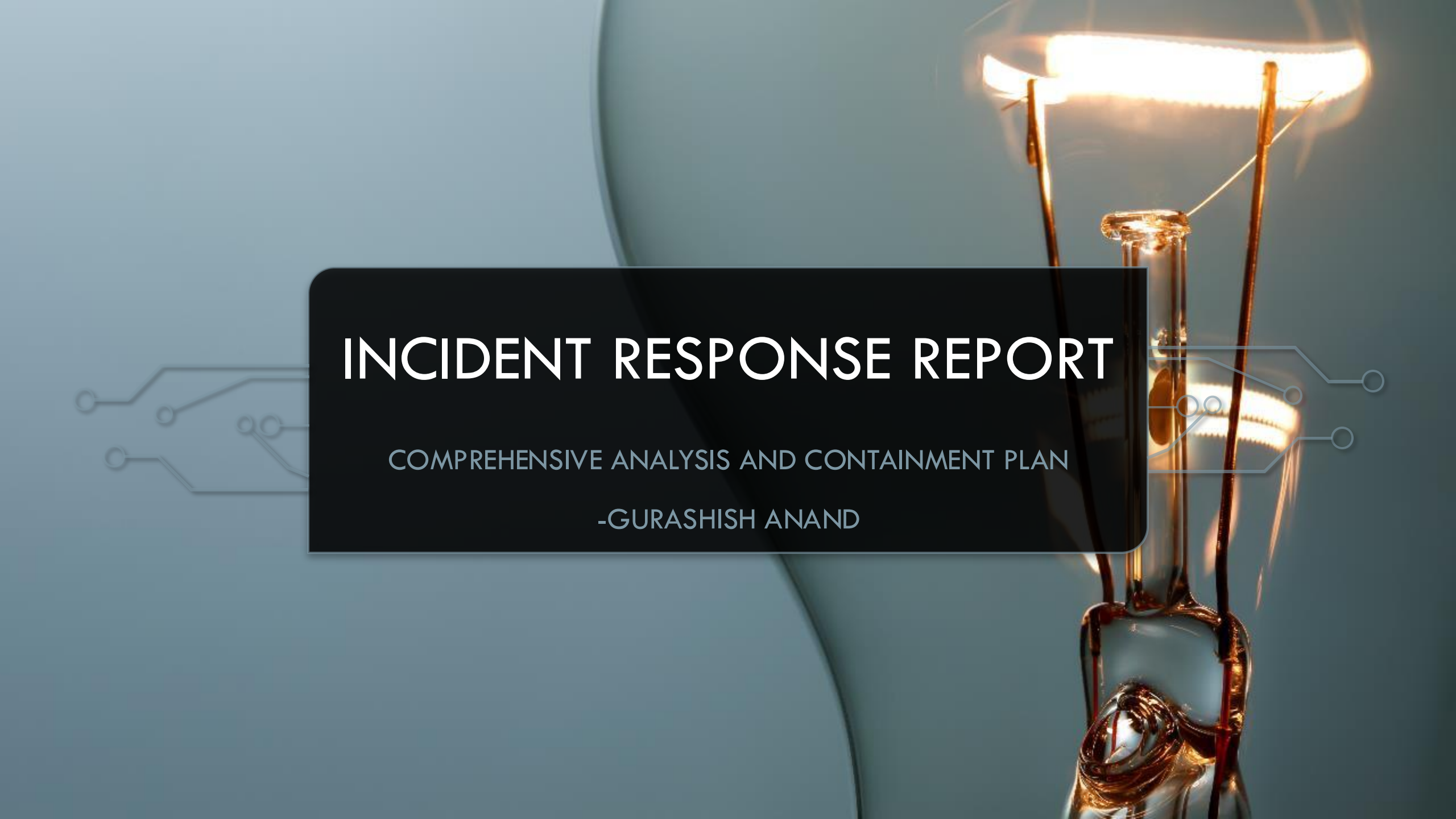


INCIDENT RESPONSE REPORT

COMPREHENSIVE ANALYSIS AND CONTAINMENT PLAN

-GURASHISH ANAND

AGENDA

- Introduction
- Email analysis and employee review
- File Hash analysis
- Containment Plan
- Communication Plan
- Conclusion

INTRODUCTION

This presentation provides an overview of the incident response efforts following a recent security breach, highlighting the critical aspects of email analysis, threat identification, containment strategies, and communication plans.

EMAIL:-

Urgent Request from Data Team!

from:"Joyce S." joyce@dashlanedata.com

Hello,

I am writing to seek your expertise in understanding the technicalities of a document related to business analytics that I am currently reviewing for an URGENT MATTER. Given your vast experience and knowledge in this domain, I believe your insights will be valuable in helping me comprehend the complexities and of the analytics mentioned above.

To provide a bit of context, the document focuses on [customer data feedback for a new product]. While I have a foundational understanding of the topic, certain sections, specifically [audience targeting using machine learning for increased revenue], contain technical jargon and advanced methodologies that are quite challenging to decipher without an in-depth knowledge of the field.

Your guidance on the below document would be incredibly helpful:

http://dashlanedataanalytics.com/clickme

I understand that you have a busy schedule, so I am more than willing to accommodate your availability but would greatly appreciate it if you can EXPEDITE this request!!!

Thank you very much for considering this URGENT request. Your assistance in this matter is greatly appreciated, and I look forward to your guidance on making the most out of this document.

Warm regards,

Joyce Serin

Data Analytics @ Dashlane

DASHLANE

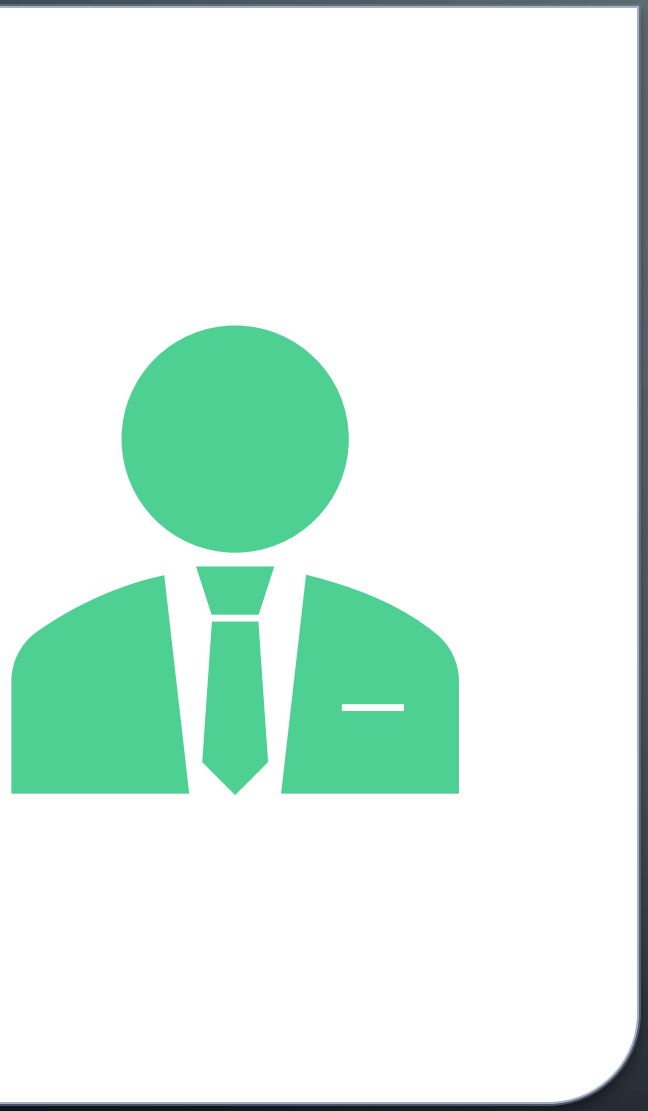
KEY FINDINGS FROM THE EMAIL ANALYSIS:-

The first and the most obvious issue with this email is the exploitation of the urgency factor of social engineering. By using the word “URGENT MATTER”, the attacker expects the end user to not think properly about this email and take immediate action.

Next issue with this email is an un-identified domain “dashlanedata.com” which is a malicious version of legit password manager website “dashlane.com”.

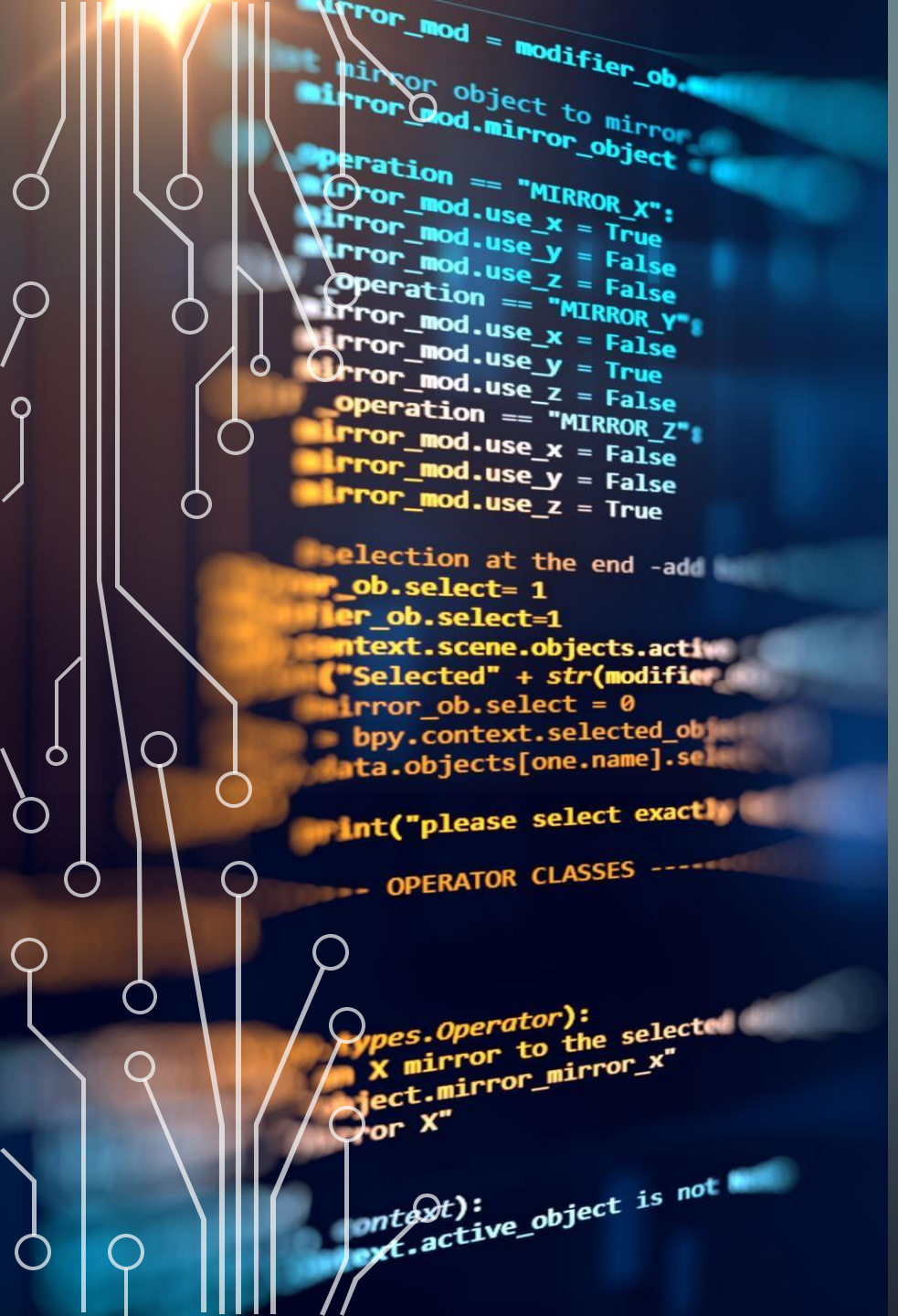
A legit employee could have just attached the document to the email (which could also be malicious), but instead, the employee includes a 'clickme’ link to the document which could be malicious too.

The formatting of this email also doesn’t look professional, like using [], instead of (), capitalizing words in the middle of sentences extra emphasis, etc.



EMPLOYEE REVIEW:-

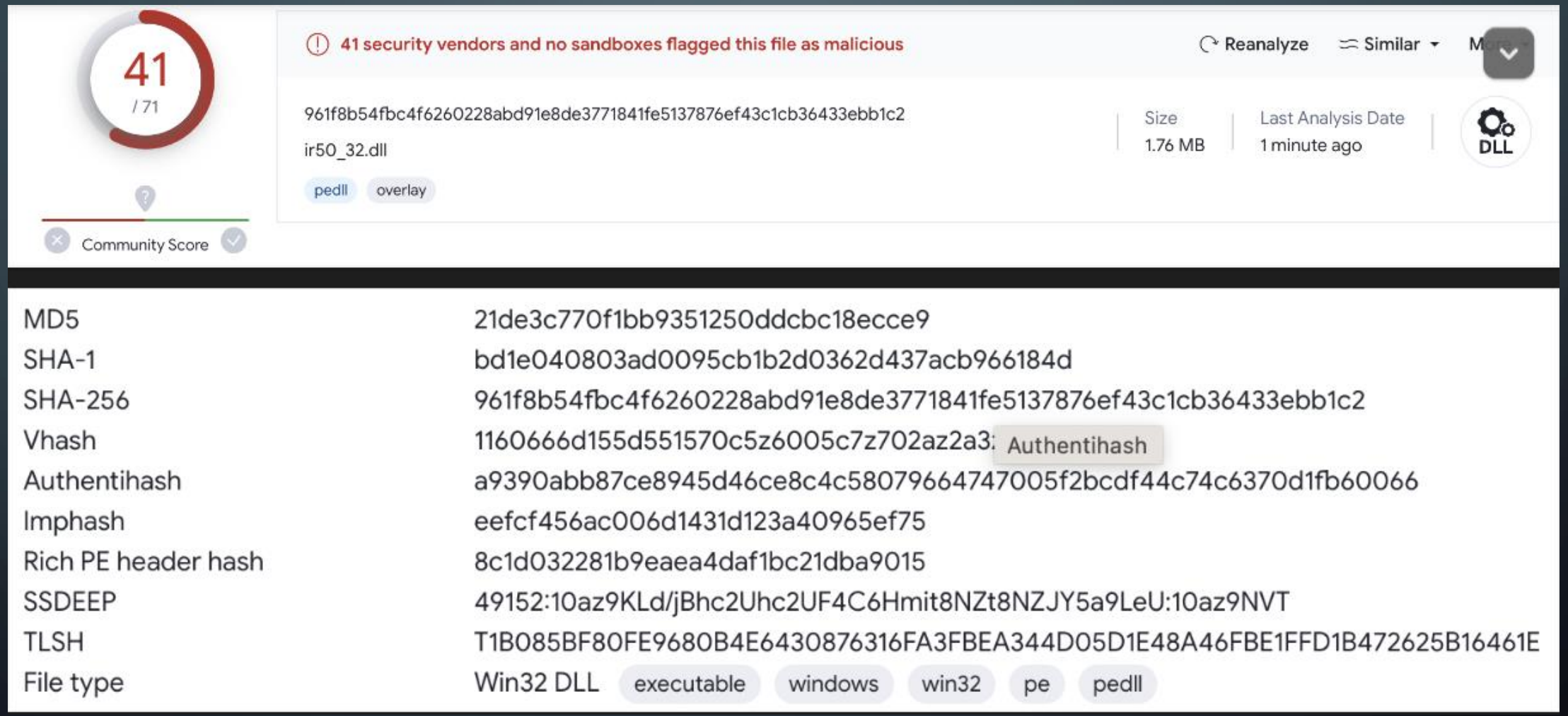
- Has the employee interacted with Joyce before? If they have, is Joyce's communication style similar?
- Did the employee exchange any credentials or any vital information with the employee following the email ?
- Did the employee find any unusual activity if they clicked the link or if they download something off the link?
- Does the employee have procedural instructions from the organization to follow in such incidents?
- Did the employee communicate this incident to the IT manager?



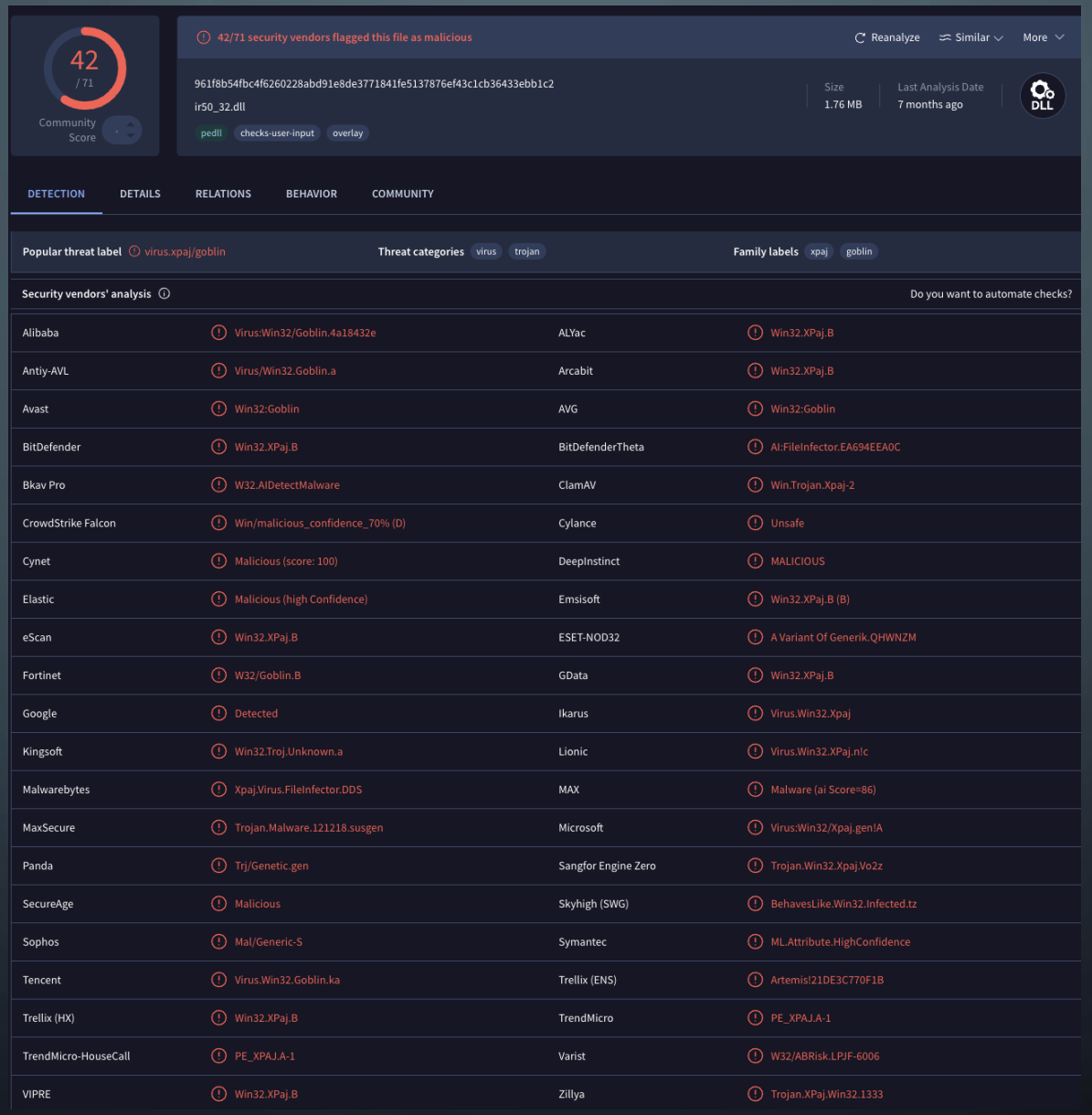
FILE HASH ANALYSIS:-

- As we just have the hash and executable text, and not the actual file to be scanned, it's best to use the hash on "virustotal" to scan for potential threats.
- Hash value:- "961f8b54fbc4f6260228abd91e8de3771841fe5137876ef43c1cb36433ebb1c2".
- Upon analyzing the hash on virus-total, the hash seems to be of a windows trojan file called "virus.xpaj/goblin". This analysis can be trusted as it is detected by 42 security vendors.
- Virus total also gives us more details about the hash, like other hash conversions, file type, Mitre signatures, IDS criticality, etc.

BRIEF FINDINGS(1):-



BRIEF FINDINGS(2):-



42 / 71
Community Score

42/71 security vendors flagged this file as malicious

Reanalyze | Similar | More

961f8b54fbc4f6260228abd91e8de3771841fe5137876ef43c1cb36433ebb1c2
ir50_32.dll
pedll | checks-user-input | overlay

Size 1.76 MB | Last Analysis Date 7 months ago | DLL

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Popular threat label virus.xpaj/goblin | **Threat categories** virus | trojan | **Family labels** xpaj | goblin

Security vendors' analysis | Do you want to automate checks?

Alibaba	Virus:Win32/Goblin.4a18432e	ALYac	Win32.XPaj.B
Antiy-AVL	Virus/Win32.Goblin.a	Arcabit	Win32.XPaj.B
Avast	Win32:Goblin	AVG	Win32:Goblin
BitDefender	Win32.XPaj.B	BitDefenderTheta	AI:FileInfector.EA694EEA0C
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Xpaj-2
CrowdStrike Falcon	Win/malicious_confidence_70% (D)	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
Elastic	Malicious (high Confidence)	Emsisoft	Win32.XPaj.B (B)
eScan	Win32.XPaj.B	ESET-NOD32	A Variant Of Generik.QHWNZM
Fortinet	W32/Goblin.B	GData	Win32.XPaj.B
Google	Detected	Ikarus	Virus.Win32.Xpaj
Kingsoft	Win32.Troj.Unknown.a	Lionic	Virus.Win32.XPaj.n!c
Malwarebytes	Xpaj.Virus.FileInfector.DDS	MAX	Malware (ai Score=86)
MaxSecure	Trojan.Malware.121218.susgen	Microsoft	Virus:Win32/Xpaj.gen!A
Panda	Trj/Genetic.gen	Sangfor Engine Zero	Trojan.Win32.Xpaj.Vo2z
SecureAge	Malicious	Skyhigh (SWG)	BehavesLike.Win32.Infected.tz
Sophos	Mal/Generic-S	Symantec	ML.Attribute.HighConfidence
Tencent	Virus.Win32.Goblin.ka	Trellix (ENS)	Artemis!21DE3C770F1B
Trellix (HX)	Win32.XPaj.B	TrendMicro	PE_XPAJ.A-1
TrendMicro-HouseCall	PE_XPAJ.A-1	Varist	W32/ABRisk.LPJF-6006
VIPRE	Win32.XPaj.B	Zillya	Trojan.XPaj.Win32.1333

IMPLICATIONS OF THE IDENTIFIED TROJAN AND ITS CHARACTERISTICS:-

- As this trojan mainly exploits windows systems, it would be a good idea to look it up on Microsoft database to know more about it.
- As we do that, we come to know that this trojan can get into your system through various ways, some of them are:-
- 1. Spam emails.
- 2. Malicious office macros.
- 3. Infected removable devices.
- 4. Bundled with other software.
- 5. Hacked or compromised webpages:-

Note:- Fortunately, Windows defender and Microsoft security essentials can be used to detect and removed this trojan if a device is infected with it. Microsoft also advices to often run full system scans to detect and remove such trojans.

CONTAINMENT PLAN:-

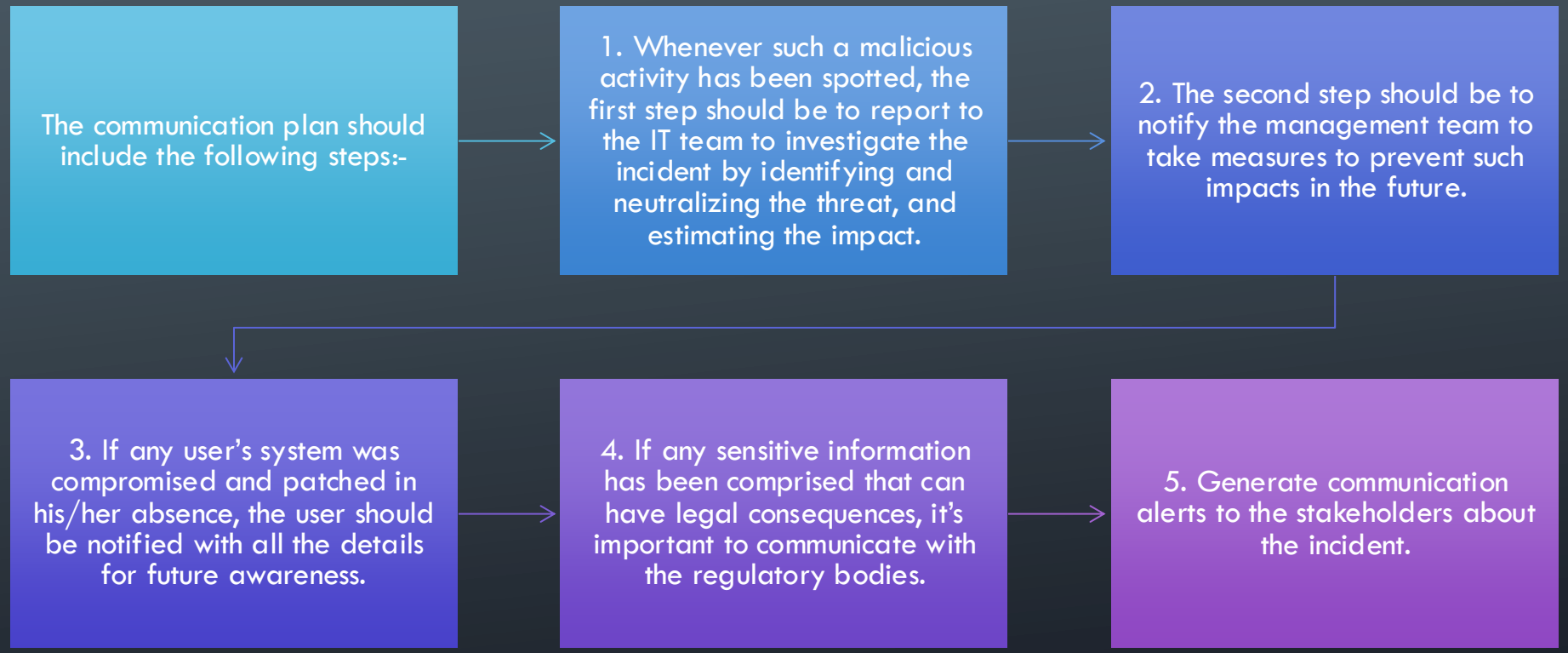
1. Identification and isolation:-

- As we know that the specific trojan can be easily detected by windows defender or any other scanning tools, its best to conduct a full system scan of all the system to identify the systems that are affected.
- Once the affected systems are identified, they can be isolated by disconnecting them from the network to prevent further spread.

2. Neutralizing the threat:-

- Make use of scanning tools like antivirus softwares to clean your system from all the junk and malicious files related to the trojan and otherwise.
- Make use of IP lookup tools to identify the IPs related to the trojan, and configure firewall tools to block those malicious IP addresses from the network.
- It's also really important to change passwords on the affected systems and implement multi-factor authentication on all systems.

COMMUNICATION PLAN:-



CONCLUSION:-

- Reflecting on the recent security incident, our team's quick and effective response played a pivotal role in managing the situation. We delved into the suspicious email and analyzed the malicious file hash, uncovering a complex trojan that posed a serious threat. Our immediate action to isolate and address the affected systems can prevent further damage and loss of sensitive information.
- This experience has highlighted the importance of staying alert and continuously updating our security measures to counter new threats. It's a reminder that in the digital age, the safety of our data requires constant vigilance and a proactive approach to security.
- Going forward, we are committed to strengthening our defenses by improving our response strategies, keeping our team informed about the latest security practices, and ensuring everyone understands their role in maintaining our cyber resilience. This incident has not only tested our readiness but also strengthened our resolve to protect our digital environment against future threats.