Scenario - Dashlane- Major Breach

You've been hired to come in as a Security Analyst working for Dashlane. Dashlane, a password management service, recently discovered a hole in the system which has resulted in 5.4 million user's information being stolen and sold online. Dashlane is interested in trying some different forms of protection on their system to ensure users' data stays protected. Your CTO is concerned that this stems from a strange email someone received earlier that month. You will be working closely with Jeffery Mariner to complete this project.

Incident Response Report:

For a Phishing Email Incident at Dashlane

Date

08 March 2024

Author

Saima Ahmed

TLP of document

TLP:RED

Not for disclosure, restricted to incident responders only.

A breach which has occurred at Dashlane when a newly hired intern received an email from an individual posing as an employee of the

company. The intern inadvertently opened the email and clicked on a link, resulting in abnormal behavior on his computer. Recognizing the issue, the intern promptly shut down his computer and reported the incident. The incident is currently being analyzed by a senior security personnel and their team, and the report is provided below

Background : What is phishing ?

During a phishing attack, scammers and hackers pretend to be someone representing an organization or company that you trust. The hacker then sends out emails, and within them are links to fake sites or attachments with **malware**. The objective of the attack is to fool the recipient into providing **personal information** that will allow them to take control of the device.

The goal of a phishing attack is to steal personal or financial information. To understand which data[1] in your organization is at risk, it is important to comprehend why hackers want it. Attackers attempt to obtain information that will somehow earn them a profit.

Recipients should take extra time for responding to emails, specifically to allow time for a thoughtful phishing analysis process. By carefully implementing this step, a person or organization can mitigate phishing attacks.

[1] Data and information at a high risk of being stolen through a phishing attack include credit card information, social security numbers, login information, information that can be used to answer two-factor authentication (2FA) questions (e.g., codes sent to a mobile device), full names, birth dates, addresses, company financial information, company secrets, future plans of a business, proprietary data and information (e.g., schematics, designs, and content), phone numbers and email addresses, passwords and numeric codes for a company's physical and digital resources, and health records.

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

Figure: Image of an email received by Intern at Dashlane

Email Analysis

From an incident response perspective, several indicators of compromise (IOCs) suggest that this email may be part of a phishing attempt or other malicious activity.

Indicators of Compromise

Phishing email analysis steps include the following three steps:

1. Checking the content of the email for anything that is uncharacteristic of the supposed sender. The following observations are noted:

- The content of the email has a malicious intent as it shows excessive use of capitalized words, to request urgent action repeatedly.

- A sense of urgency is created in the email so the receiver can take urgent action.

- A malicious link with obvious fishy word “clickme” http://dashlanedataanalytics.com/clickme

- When hover over the link it leads to a suspicious website i.e., https://fakeupdate.net/sarcastic/
    - Virus total website (https://www.virustotal.com/gui/home/url) flagged this link as suspicious.

- The email appears to be unsolicited, as it does not mention any previous correspondence or relationship between the sender and recipient. Phishing emails often target individuals who may not be expecting such requests.

- The email uses generic language and does not provide specific details about the recipient's expertise or how they were chosen for assistance, which is common in phishing emails sent to a wide audience.

2. Conducting email header analysis for phishing, such as checking for headers that are formatted differently than typical company emails.

    - The email subject is not a common subject heading i.e., Urgent Request from Data Team.

- The email address is not from dashlane.com, instead dashlanedata.com is used which is not the domain name of dashlane.

- When the email id is checked on (https://clean.email/verifier/how-to-check-if-an-email-is-valid) , email id status shows invalid.

- The name of the person *Joyace S* does not seem to be the correct full name.

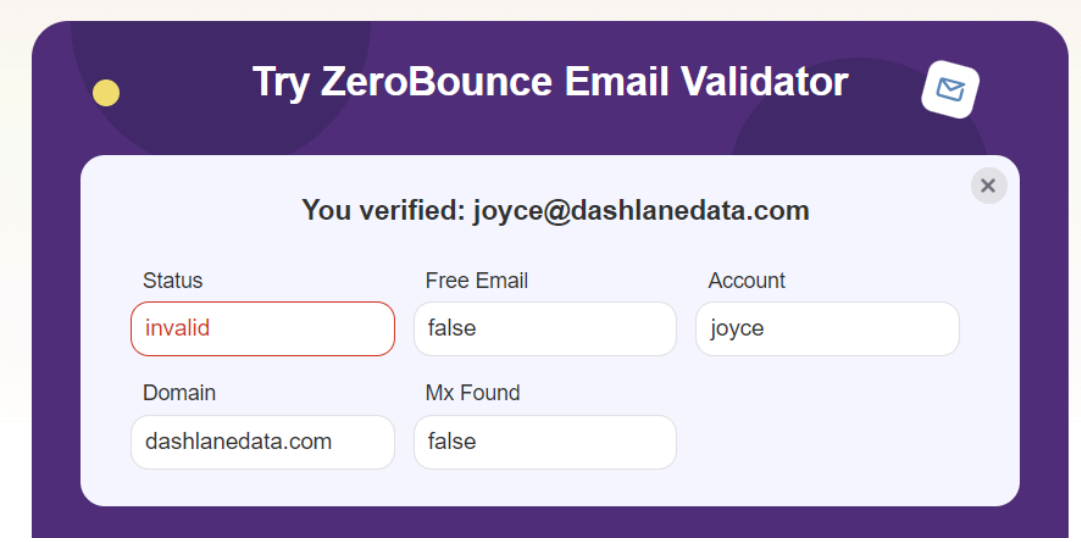

Figure: The email validator.

3. The recipient can verify the authenticity of the link from these websites mentioned below.

    1. VirusTotal "https://www.virustotal.com/gui/home/url"
    2. https://securitytrails.com/
    3. https://urlscan.io/
    4. https://dnschecker.org/
    5. host.io

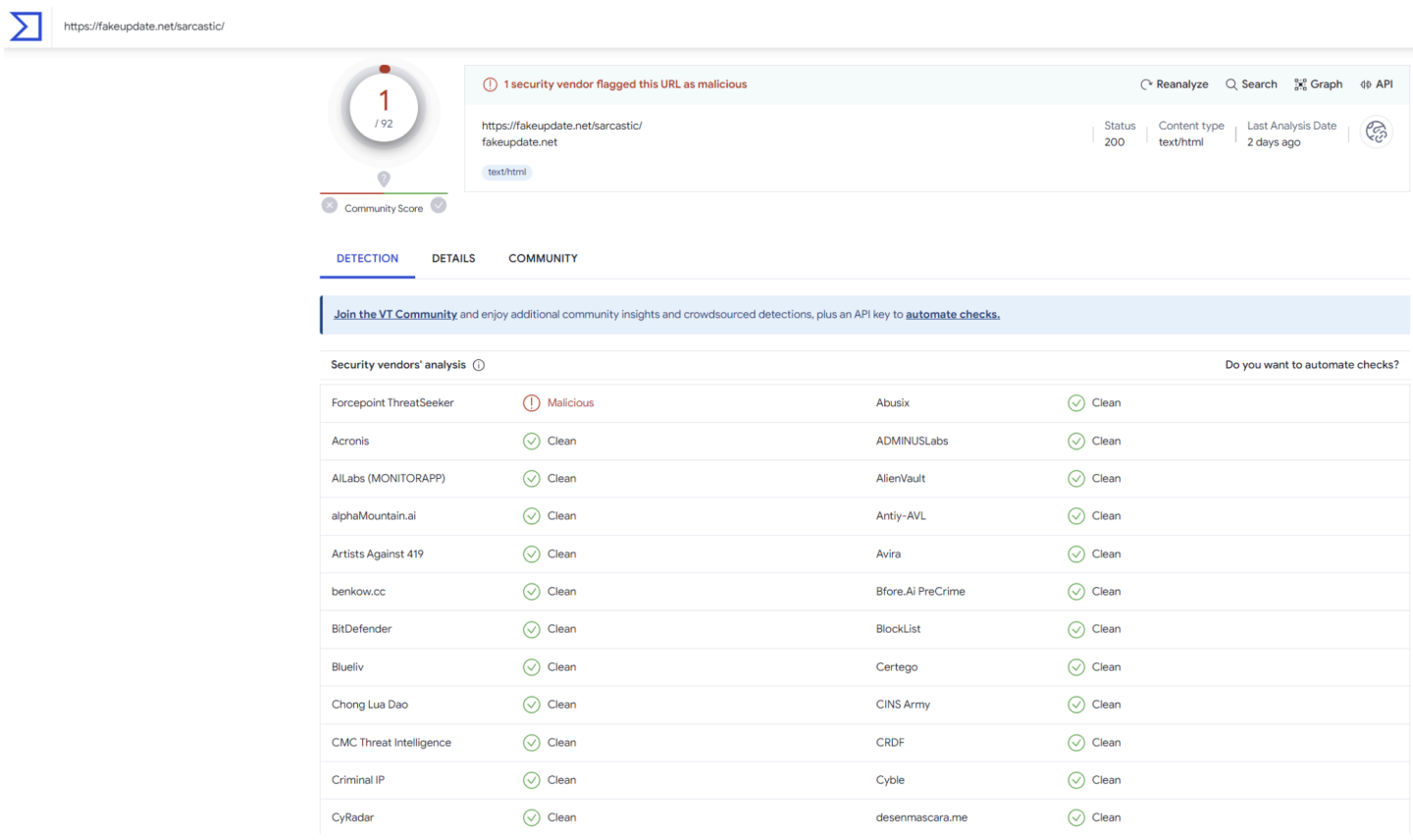

Figure: VirusTotal for https://fakeupdate.net/sarcastic/ screenshot.

Questions For The Employee:

1. **Action you took when you found that email:**

    a. Did you take your time to think about taking the right action ?
    b. Did you click on any links or download any attachments from the email?

2. **Reporting/Delete it for protecting your laptop**

    a. Did you report the email?
    b. Did you report the email to the IT or security team before or after opening it?
    c. Did you delete the email from your inbox and trash folder ?

3. **Forwarding or Sharing:**

    a. Have you forwarded or shared the email with anyone else?
    b. Do you have any information that someone in your department also received the same email?

4. **System Impact:**

    a. Have you noticed any unusual activity or changes on your system or network after receiving the email?
    b. How did you discover that there was an issue?
    c. What if any abnormal behaviors did you observe?
    d. When did it begin?
    e. Were there any other incidents related to this e.g. phone calls, remote sessions, follow-up emails?

5. **Other Observations:**

    a. Is there any additional information or observations you can provide about the email or related incidents?

6. **Awareness Training:**

    a. Have you received cybersecurity awareness training on identifying and handling suspicious emails?

7. **System setup**:

    a. Can you provide some details about your current work setup, such as whether you're working remotely through a VPN or in person at the office?

These questions can assist the security analyst in gathering information to evaluate the potential threat posed by the email and implementing suitable measures to mitigate any risks.

According to the employee's account, he was physically present at work when he received the email. Upon opening the email and clicking the link, his system displayed unusual behavior.

File Hash Analysis:

Figure: File hash community score on VirusTotal.

1. The VirusTotal analysis reveals that the file lacks a digital signature from a verified source, which raises concerns about its trustworthiness and potential security risks. Organizations should exercise caution when dealing with unsigned files and consider additional analysis and response measures to mitigate potential threats.

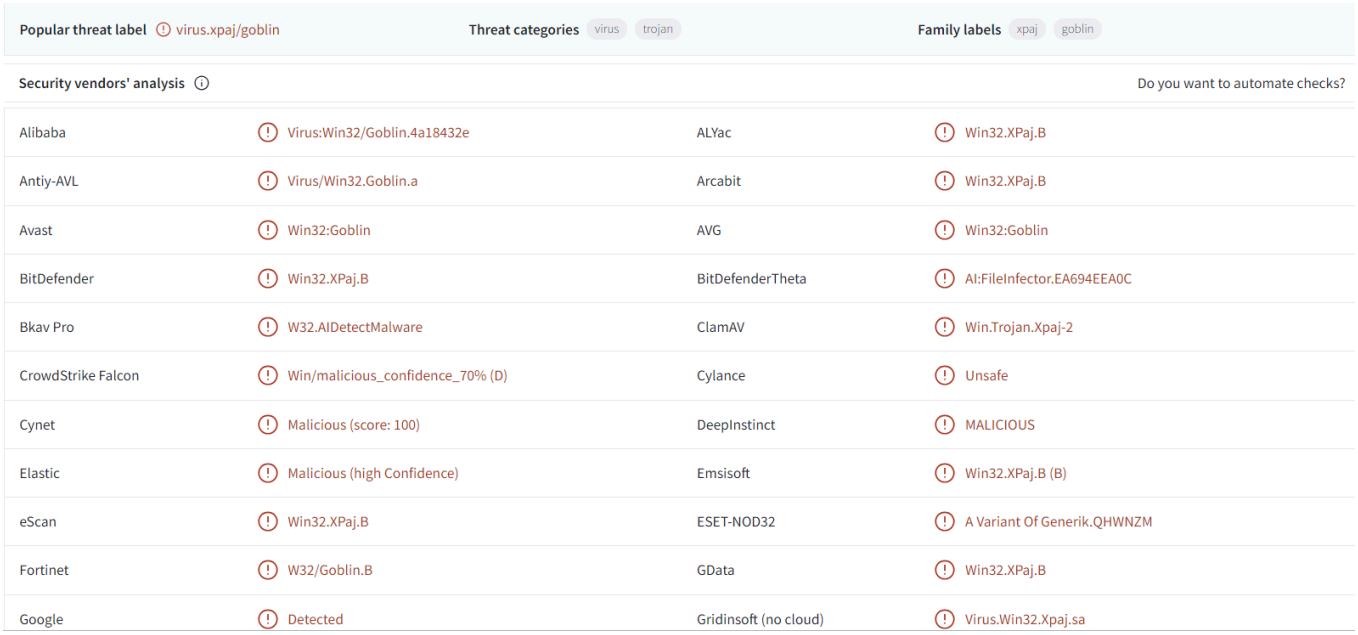

Figure: File hash screenshot on VirusTotal.

2. Out of 70 security engines on VirusTotal, 42 flag this file hash as malicious. It appears that it has infected an employee's computer with malware, such as a trojan. **(virus.xpaj/goblin)**

a. Trojans or viruses often disguise themselves as legitimate files to evade detection and deceive users into executing them. They employ various techniques to appear legitimate, including hiding malicious code within otherwise genuine files, such as documents, executables, or multimedia files. This enables them to circumvent security controls reliant on file signatures or reputation-based detection.

3. Furthermore, the file hash analysis from VirusTotal indicates that the file type is a **win32 DLL (ir50_32.dll)**. An adversary could disguise a malicious payload within a DLL file, which could then be executed on a victim's system. This DLL may contain malicious code or routines designed to perform harmful actions, such as downloading additional malware, stealing data, or providing remote access to the attacker.

Basic properties

MD5	21de3c770f1bb9351250ddcbc18ecce9
SHA-1	bd1e040803ad0095cb1b2d0362d437acb966184d
SHA-256	961f8b54fbc4f6260228abd91e8de3771841fe5137876ef43c1cb36433ebb1c2
Vhash	1160666d155d551570c5z6005c7z702az2a3z28z8
Authentihash	a9390abb87ce8945d46ce8c4c58079664747005f2bcdf44c74c6370d1fb60066
Imphash	eefcf456ac006d1431d123a40965ef75
Rich PE header hash	8c1d032281b9eaea4daf1bc21dba9015
SSDEEP	49152:10az9KLd/jBhc2Uhc2UF4C6Hmit8NZt8NZJY5a9LeU:10az9NVT
TLSH	T1B085BF80FE9680B4E6430876316FA3FBEA344D05D1E48A46FBE1FFD1B472625B16461E
File type	Win32 DLL executable windows win32 pe pedll
Magic	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
TrID	DirectShow filter (53.9%) | Windows ActiveX control (31.1%) | Win32 Executable MS Visual C++ (generic) (8.3%) | Win32 Dynamic Link Library (generic) (1.7%
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (5.0) [DLL32] | Compiler: Microsoft Visual C/C++ | Linker: Microsoft Linker (5.10.7303) | Tool: Visual Studio
File size	1.76 MB (1841810 bytes)
PEiD packer	Microsoft Visual C++ DLL

Figure: Basic file properties.

As previously mentioned, a recent system vulnerability was uncovered, resulting in the theft and sale of information from 5.4 million users online. The malware trojan responsible for the breach appears to operate as a data stealer, infiltrating the network and extracting user information from data servers containing usernames and passwords

Incident Management Process:

NIST and SANS Incident Response Frameworks

A data breach is an event that results in exposing confidential, sensitive, or other protected information to an unauthorized person. In our case Dashlane sensitive information is stolen and sold online. This happened because of the phishing email someone received.

If a data breach has occurred, it's necessary to respond immediately and investigate the incident as soon as possible.

Data breach/Incident response plan is a systematic way to deal with and manage the consequences of a data breach. The goal is to address the problem in a way that minimizes harm and reduces recovery time and expenses.

Two widely recognized frameworks for incident response are;

1) **NIST (National Institute of Standards and Technology)**
2) **SANS (SysAdmin, Audit, Network and Security)**

The primary difference between the two frameworks is how they organize the *actions*.

NIST takes a four-pillar approach that includes:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, & Recovery
4. Post-Incident Activity

Meanwhile, SANS consolidates the second NIST pillar while separating the third into three distinct categories:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

We can **combine the best practices of these two frameworks** to create a breach response plan according to organization structure and needs. An incident response process is a structured approach to effectively managing and mitigating security incidents typically consisting of five stages and providing a roadmap for handling incidents.

NIST Incident Response Process	SANS Incident Response Process
1. Preparation	1. Preparation
2. Detection and Analysis	2. Identification
3. Containment, Eradication, and Recovery	3. Containment
4. Post-Incident Activity	4. Recovery
	5. Recovery
	6. Lessons Learned

During the preparation phase, organizations establish incident response plans, define roles and responsibilities, and implement necessary security measures. The identification stage involves detecting and validating incidents through monitoring systems and alerts. Once an incident is confirmed, containment measures are implemented to prevent further damage. The eradication phase focuses on removing the cause of the

incident and restoring systems to a secure state. Finally, the recovery stage involves restoring normal operations, conducting post-incident analysis, and implementing improvements to prevent future incidents.

Incident response has the largest direct influence on the **overall mean time to acknowledge (MTTA) and mean time to remediate (MTTR) that measure how well security operations are able to reduce organizational risk**. Incident response teams heavily rely on good working relationships between threat hunting, intelligence, and incident management teams (if present) to actually reduce risk.

1. **Prepare for a data breach before it happens**

   Ideally organizations should be ready to handle data breach before it happens. Good preparation can significantly reduce the risk of business damage and simplify your response and recovery processes.

   1. Conduct a risk assessment.
      a. To identify existing threats and vulnerabilities.
   2. Establish/Create an incident response team.
   3. Conduct cybersecurity awareness training for employees.

2. **Identify/ Detect the data breach**

   Identifying or detecting starts by noticing abnormal activity from compromised credentials, malware, phishing, or system/network vulnerability exploitation.

   1. In our case atack vector is in the form of a phishing email:
      a. The malware is stored as an attachment.

3. **Containment**

During the containment phase, your incident response team focuses on limiting and preventing additional damage from happening. Some short term measures involve.

1. Isolate the threat.
    a. Isolating network segments containing infected workstation/s or computer/s.
2. Disconnect affected system/s from the internet.
3. Kill active processes running on the affected system.

Long-term containment focuses on getting systems to function normally and preventing the threat actor from moving laterally within the systems and networks.

4. Disable impacted email account.
5. Reset password for compromised accounts on the domain.
6. Implement MFA on all the workstations in order to avoid a repeat compromise.
7. Restoring system/s from backups.
8. Set-up a multi-factor authentication on remote access.
9. Apply all recent security patches and updates.

4. **Eradication**

During the eradication step, incident handlers remove all the attack components and work toward restoring the affected systems. As part of this process, some activities may include:

1. Deleting malware.
2. Disabling breached user account/s.

3. Identifying and mitigating vulnerabilities.
4. Identifying all affected hosts.
5. Reimaging and hardening systems with patches.
    a. Replacing affected files with clean versions.
6. Removing all artifacts left by the attacker.

5. Recovery

Finally, the recovery process brings the affected system back online after testing, monitoring, and validating that attackers will be unable to compromise it again. Recovery activities include:

1. Restoring from a clean backup.
2. Rebuilding from scratch.
3. Replacing compromised files with clean files.
4. Installing patches.
5. Changing passwords/ MFA.
6. Re-securing networks with updates to controls like new firewall rulesets or boundary router access control lists
    a. Implement EDR/anti-phishing software/Firewall throughout the organization to detect and mitigate malware.

6. Lessons Learned

After completing the recovery process, your organization needs to review its data breach response capabilities and incorporate any lessons learned. Engaging in a post-data breach incident handling analysis gives you insight into what processes worked well and what actions you can take to prevent a similar event.

Conducted as soon as possible after the incident, the lessons learned meeting should incorporate objective and subjective information that you can use to enhance processes, justify spending, and incorporate into the annual risk assessment.

A fundamental part of your data breach response plan should focus on **prevention**. Some other factors should also be considered for execution of the incident response plan.

1. **Communication**

   Notify relevant stakeholders, including IT security personnel, management, affected users, and legal or compliance teams, about the incident. Provide clear instructions on what actions to take and keep stakeholders informed throughout the incident response process.

2. **Employee Education**

   Conduct security awareness training for employees to educate them about the risks of phishing attacks, how to identify suspicious emails, and best practices for responding to potential threats.

3. **Documentation**
   Document all actions taken during the incident response process, including timelines, findings, remediation steps, and lessons learned, to facilitate post-incident analysis and improve future response efforts.

4. **Review and Follow-Up**

   Conduct a post-incident review to assess the effectiveness of the response plan, identify areas for improvement, and update policies, procedures, and training materials accordingly.

5. **Legal and Regulatory Compliance**

Ensure compliance with relevant laws, regulations, and industry standards, such as data breach notification requirements, by adhering to established incident response protocols and reporting procedures

Top Five Recommendations:

1. **Threat Mitigation**

   Continuous monitoring, prioritizing alerts, and proactively remediating potential attack vectors enable you to mitigate data breach risks. This involves frequently updating security controls, conducting security assessments and performing penetration testing to proactively identify and address security weaknesses.

2. **Automated Detection Systems**

   a. Email filtering rules can be implemented based on certain parameters.
   b. Some examples of automated phishing detection tools include:
      - Proofpoint Email Protection
      - Microsoft Defender for Office 365
      - Cisco Email Security
      - Barracuda Email Security Gateway
      - Symantec Email Security

3. **Reset Passwords**

   Promptly reset passwords to mitigate unauthorized access gained through credential guessing, phishing, or brute-force attacks. If the compromised accounts are known, prioritize their reset. However, for comprehensive data breach containment, consider forcing password

resets for all domain or authentication system accounts unless the compromise is clearly isolated.

4. **Implement MFA**

   Implementing Multi-Factor Authentication (MFA) is crucial for preventing repeat compromises. MFA combines two or more authentication types, such as something you know, something you are, or something you have, to enhance security beyond traditional username and password methods.

5. **Do not Destroy Evidence**

   During incident response, preserving evidence is essential even amidst the rush to contain the situation. Preserving data intact enables the investigation of potential data breaches, potentially avoiding the need for data breach notifications and associated costs. While immediate changes may be necessary, such as disabling compromised accounts or rules, documenting the changes with photos or screenshots ensures evidence integrity for future investigations.

References:

Systems thinking & CTI: Scenario-Based Incident Response Playbooks

5 Simple Tips for Phishing Email Analysis

4 Crucial Steps for Data Breach Containment