| **Ticket ID** | **Alert Message** | **Severity** | **Details** | **Ticket status** |
| --- | --- | --- | --- | --- |
| A-2703 | Phishing attempt - possible download of malware | Medium | The user may have opened a malicious email and opened attachments or clicked links. | **Escalated** |

| **Ticket comments** |
| --- |
| * This phishing attempt involved an email with an attached file (filename="bfsvc.exe") claiming to be a resume and cover letter. The attachment hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) was confirmed to be malicious through a threat intelligence tool. * Due to the presence of a confirmed malicious attachment, this phishing attempt is a medium severity incident and requires escalation to a level-two SOC analyst for further investigation and potential user containment actions. |

### **Additional Notes:**

### The specific details of the email content (sender, message body) are not necessary to determine escalation in this instance due to the confirmed malicious attachment. However, these details can be investigated by the level-two SOC analyst for additional context.

### 

### **Additional information**

**Known malicious file hash**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

**Email**:  
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>

Sent: Wednesday, July 20, 2022 09:30:14 AM

To: <hr@inergy.com> <176.157.125.93>  
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,  
  
I am writing for to express my interest in the engineer role posted from the website.  
  
There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.   
  
Thank you,  
  
Clyde West

Attachment: filename="bfsvc.exe"