Report back to Virgil on what you have discovered in the SIEM based on the information you were given in the email.

- Cite **specific pivots for anything you discover that stands out as unusual** to you.
- Do you feel that this is indeed something that needs to be investigated?
- Be sure to include your initial impressions on:
    - **what might be taking place**;
    - whether a **particular threat** appears to be involved;
    - the **potential scope** (which device(s) were exposed to a particular threat?) of the incident.

PLEASE NOTE: this first submission should NOT be in the form of an SBAR report. Think of this as just a quick email back to your supervisor letting them know, in broad strokes, what you think might have happened during this incident. You do NOT have to determine if any workstations have been compromised at this point in the investigation.

(First submission)
~~The following details are based on the information given to me in the email, along with information analyzed in the SIEM:~~

~~I would recommend looking into this issue further. Despite the link being classified as non-malicious, email logs showing back and forth traffic with several addresses containing '@at-usa.co' (which I'm assuming are other executives such as P. Brand) around the same time as the reported incident by Brand alludes to suspicious activity. Emails were sent to (3) other addresses (S. Adams, D. Walker, M. Land) within 0.08 seconds of the email to P. Brand was sent.~~

~~I suspect someone *could* be spear phishing in an attempt to gather high-ranking employee credentials - though, I do not believe there is sufficient evidence at this time in order to back this claim.~~

~~Host LAB-WIN10-04 (connected to P. Brand) is the only device I believe should be further inspected mainly for precautionary measures.~~

~~Pivots related to the queries with 'daniel@mail.at-usa.co' and 'that_one_guy24@yahoo.com' seem suspicious. If these addresses can both be traced to legitimate users that would alleviate suspicions.~~

—---

(2nd submission)

The following details are based on the information given to me in the email, along with information analyzed in the SIEM:

Despite the URL in the body of the email being classified as non-malicious, there is evidence of suspicious activity and potential device compromise within the SIEM logs.

After the email was sent, it unfortunately seems that (4) different internal devices accessed ‘https;//ciso.guide/’.

A strange looking, obfuscated URI was also located in a log that appears to be redirecting from ‘http;//ciso.guide/’ - which the same previous (4) internal devices also accessed. This along with an unusual URI IP address, leads me to potentially believe that ‘http;//ciso.guide/’ may be compromised, and could potentially be being used as a landing site for a drive-by compromise exploit.

It is my recommendation to further investigate this incident.

- IP that did not resolve and uri that followed: 176.57.214.103 /?MjY4NzM0&zFgggRTovMMcmVwb3J0ZnpMc2dOYnJUTnZRY2FwaXRhbA==&CfrFHAL=bG9jYXRlZA==&ESyyTsE=ZGVub21pbmF0aW9ucw==&UQlqALxy=Y2FwaXRhbA==&cXJAzhGr=dW5rbm93bg==&gRGwPutcuh=cmVwb3J0&gh23mXN32dfg3=CwjBeJKgBjlYIZUV0U9qD_iUDUnEedg8KK_kSMYA4W_sOXErEz2In2nbQkeMMixB6E6lETi-IL&cTRfaa=Y2FwaXRhbA==&YcbDwOaLaVB=YXR0YWNrcw==&TaTfmVdWv=Y2FwaXRhbA==&WnZNVgRfBEtMx=c3Rvcm1lZA==&giwjCD=YXR0YWNrcw==&JzhYRaHphq=cmVwb3J0&CjffGT=ZGVub21pbmF0aW9ucw==&L5sdmX1Zfhds=xX_QMvWfbRXQDp3EKvncT6NHMVHRGECL2YqdmrHSefjaelWkzrfFTF_3ozKATgSG6_dtdfJSDQ&NYPnxuuEBlxdW5rbm93bg==

-Strange http_referrer: http://seclists.org/bugtraq/2005/Oct/118