IMPORTANT: **For ANY question you are not able to determine the answer to, you must do the following: (1)** in your answer to that question, explicitly state that there is insufficient information available to determine the answer, & **(2)** include an appropriate RECOMMENDATION requesting access to whatever additional evidence sources would allow you to actually answer that question.

SITUATION

The SITUATION section provides a fairly brief overview of the situation or incident that triggered the investigation you are about to undertake.

SITUATION should contain NONE of your conclusions or findings determined *after* actually beginning your investigation. All investigation findings belong in the ASSESSMENT section.

S1 Write a 1-2 sentence summary of the instigating incident or "situation" that kicked off this investigation in the first place.

A suspicious email was sent to the CFO of AT-USA containing what seemed to be a harmless link which was recognized as a site that was regularly visited by AT-USA employees (www.ciso[.]guide.com). It was investigated by another analyst and was closed out, I was later asked to re-investigate the incident.

S2 If this investigation concerns a particular client, name it here. (Upon whose behalf are you conducting this investigation?)

This investigation is being conducted on behalf of Virgil and one of our client's, AT-USA.

S3 **Reiterate any relevant hypotheses or observations** included in whatever information you were provided at the onset about the instigating incident.

The current hypothesis is that the ciso.guide link that was attached in the email sent to the CFO *is* actually malicious and poses a legitimate threat.

The case was originally investigated and the email classified as benign by another analyst, Boots. Several factors noted by Boots lead to this decision: the url was found to route to a regularly visited website by AT-USA employees, no malicious binary was found on the device of P. Brand, and the email did not contain any other attachments.

S4 **Is this investigation related to any other previous OR ongoing investigations?** If so: identify and cite the previous OR ongoing investigations.

This investigation was originally conducted by another one of our analysts (Boots) in 2017, in which he concluded the incident was non-threatening.

BACKGROUND

The BACKGROUND section describes in greater detail the information you were given prior to beginning your investigation. Enrich the information about the instigating incident by determining the information can be gathered from logs or people about what might have led up to the incident.

BACKGROUND should contain NONE of your conclusions or findings determined *after* actually beginning your investigation. All investigation findings belong in the ASSESSMENT section.

B1 What is the date and time[range] of the *reported* incident? Be sure to include the timezone.

The date of the reported incident is: Friday December 29th, 2017 20:58 UTC (email first received)

B2 What exactly is the task that has been assigned to you? (What must you determine before your investigation can be considered completed?)

My task is to re-investigate the incident and determine if the email received is a legitimate threat, as well as determining if any AT-USA devices had been compromised.

B3 Who assigned the investigation of this incident to you?

Virgil has assigned this task to me.

B4 **What sources of evidence were you given access to in order to conduct your investigation?** (An older SBAR? SIEM logs? PCAP? Memory image? Forensic disk image? The ability to interview specific employees? **If you have been given access to it during your investigation, make it clear here!**)*

** If any of your provided evidence sources feature only evidence from a particular timestamp or date||time range, **this is the place to make note of it.***

For this investigation, I have been given access to SIEM logs, an older SBAR report, and the originally-received email from the first previous investigation.

ASSESSMENT

The `ASSESSMENT` section contains "answers" to all the outstanding questions your investigation was tasked with addressing.

This is usually the meatiest part of the report: you are presenting the bulk of your investigation findings in this section, providing the final analysis & implications of the information that was gathered during the course of the investigation. Remember: as an analyst, it is your job to connect all the dots based on the evidence you are able to dig up; if you describe a specific detail or event, ensure you are making it clear why you are including that information. What is its meaning||significance||implications? Your answers should clearly include this context about the information you are providing.

Details about the specific evidence you discovered that supports the findings you describe here should be included in the `TECHNICAL APPENDIX`; the answers here should **only** include findings you were able to determine from the examination of that evidence during the course of your investigation.

`A1` `ANY CORRECTIONS TO MAKE TO INFO REPORTED IN S OR B?` • Did you discover that any founding hypotheses reported in the `SITUATION` or `BACKGROUND` section were incorrect? If so: you should state explicitly what you determined to be incorrect, along with the relevant corrected information.

~~Corrections that I would make would be that this threat appears to be much larger than anticipated, as it seems an exploit kit is involved and a device has been compromised and infected.~~

Boots believed that the only threat vector was the spear phishing email itself and had surmised that the email posed no threat and that P. Brand's device was the only workstation needing to be examined - overlooking another AT-USA device that had actually been compromised and infected. It appears that the threat is much larger than originally anticipated, with an

exploit kit utilized to carry out a drive-by compromise/watering hole attack via (ciso[.]guide.com).

A2a WHAT HAPPENED • **How did this take place?** (What tool(s) or technique(s) caused the incident to occur?)

The incident occurred through a 'spear phishing' attack, delivering a Rig Exploit kit which is responsible for delivering malware to vulnerable devices as a part of a watering hole attack. It should be noted that having interacted with the email was not a prerequisite for a device to be susceptible to attack as it was found a device was compromised without having received the suspicious email.

A2b WHAT HAPPENED • **What is the full date||time range of the entire incident? Are there distinct timeranges that define specific "clusters" of activity? At what particular timestamps did important events occur at?**

~~[2017-12-29 15:58 EST] Spear phishing attack (begins): A suspicious email was sent to p.brand@at-usa.co (10.5.10.116) as well as d.walker@at-usa.co (10.5.10.127), s.adams@at-usa.co (10.5.10.129), and m.land@at-usa.co (10.5.10.128); email sent from daniel@mail.at-usa.co (10.5.10.130/125).~~

~~[2017-12-29 21:25:22.617 UTC] Host\user LAB-Win7-01\s.adams has obfuscated javascript code run (siem_event_id: sysmon:0:5350081)~~

~~[2017-12-29 21:26:28.856 UTC] Host\user LAB-Win7-01\s.adams file 'bilo439.exe' is created (siem_event_id: sysmon:0:5345629)~~

~~[2017-12-29 21:36:30.534 UTC] Host\user LAB-Win7-01\s.adams file 'bilo494.exe' is created (siem_event_id: sysmon:0:5336417)~~

~~[2017-12-29 21:46:21.166 UTC] Host\user LAB-Win7-01\s.adams file 'bilo161.exe' is created (siem_event_id: sysmon:0:5326341)~~

~~[2017-12-29 21:47:16.149 UTC] Host\user LAB-Win7-01\s.adams file 'bilo467.exe' is created (siem_event_id: sysmon:0:5324093)~~

~~[2017-12-29 23:15:03.161 UTC] Host Daniel PC has file 'obommhdf.exe' created from process 'bilo400.exe' (siem_event_id: sysmon:0:4184879)~~

~~[2017-12-29 23:16:01.940 UTC] Host Daniel PC has file 'xwgrttjl.exe' created from process 'obommhdf.exe' (siem_event_id: sysmon:0:4172006)~~

~~[2017-12-29 23:16:04.787 UTC] Host Daniel PC has file 'fgkhroxg.exe' created from process 'obommhdf.exe' (siem_event_id: sysmon:0:4171533)~~

~~[2017-12-29 23:21:49.898 UTC] Host Daniel PC has file 'inwqbuvx.exe' created from process 'svchost.exe' (siem_event_id: sysmon:0:4025152)~~

Initial event: [2017-12-29 20:58:29 UTC] Spear phishing (S.P.) emails are sent
Final event: [2018-01-08 16:40:49.938 UTC] Last attempted C2 communication (unsuccessful)

[2017-12-29 20:58:29 UTC] Spear phish attack (begins): S.P. email sent to p.brand@at-usa.co. *AT-USA employees' personal emails are vulnerable to internal risk.* [daniel@mail.at-usa.co, LAB-Win10-04]

[2017-12-29 20:58:29 UTC] Spear phish attack (begins): S.P. email sent to m.land@at-usa.co. *AT-USA employees' personal emails are vulnerable to internal risk.* [daniel@mail.at-usa.co, LAB-Win10-03]

[2017-12-29 20:58:30 UTC] Spear phish attack (begins): S.P. email sent to d.walker@at-usa.co. *AT-USA employees' personal emails are vulnerable to internal risk.* [daniel@mail.at-usa.co, LAB-Win10-02]

[2017-12-29 20:58:31 UTC] Spear phish attack (begins): S.P. email sent to s.adams@at-usa.co. *AT-USA employees' personal emails are vulnerable to internal risk.* [daniel@mail.at-usa.co, LAB-Win7-01]

[2017-12-29 21:24:12 UTC] Exposed: LAB-Win7-01\s.adams is exposed to the threat associated with ciso[.]guide. *Host is vulnerable to a drive-by-compromise/other malicious redirects.* [Ciso[.]guide, LAB-Win7-01]

[2017-12-29 21:26:28.856 UTC] Payload dropped: LAB-Win7-01\s.adams file 'bilo439.exe' is created. *Malicious malware payload is dropped onto the device.* [vds.cs59923.timeweb.ru, LAB-Win7-01]

[2017-12-29 21:36:30.534 UTC] Payload dropped: LAB-Win7-01\s.adams file 'bilo494.exe' is created. *Malicious malware payload is dropped onto the device.* [vds.cs59923.timeweb.ru, LAB-Win7-01]

[2017-12-29 21:46:21.166 UTC] Payload dropped: LAB-Win7-01\s.adams file 'bilo161.exe' is created. *Malicious malware payload is dropped onto the device.* [vds.cs59923.timeweb.ru, LAB-Win7-01]

[2017-12-29 21:47:16.149 UTC] Payload dropped: LAB-Win7-01\s.adams file 'bilo467.exe' is created. *Malicious malware payload is dropped onto the device.* [vds.cs59923.timeweb.ru, LAB-Win7-01]

[2017-12-29 21:40:33.974 - 21:55:53.103 UTC] Exposed: LAB-Win10-03 is exposed to the threat associated with ciso[.]guide. *Host is vulnerable to a drive-by-compromise/other malicious redirects.* [Ciso[.]guide, LAB-Win7-01]

[2017-12-29 22:50:07.951 - 23:10:11.405 UTC] Exposed: Daniel-PC is exposed to the threat associated with ciso[.]guide. *Host is vulnerable to a drive-by-compromise/other malicious redirects.* [Ciso[.]guide, LAB-Win7-01]

[2017-12-29 23:14:33.073 UTC] Infection occurs: First payload 'bilo400.exe' is dropped on host Daniel-PC. *Malicious Ramnit malware payload is dropped onto the device.* [vds.cs59923.timeweb.ru, Daniel-PC]

[2017-12-29 23:15:03.161 UTC] Continued infection: Daniel-PC has file ‘obommhdf.exe’ created from process ‘bilo400.exe’. *File is created from initial malware, spreading infection.* [vds.cs59923.timeweb.ru, Daniel-PC]

[2017-12-29 23:16:04.787 UTC] Continued infection: Daniel-PC has file ‘fgkhroxg.exe’ created from process ‘obommhdf.exe’. *File is created from initial malware, spreading infection.* [vds.cs59923.timeweb.ru, Daniel-PC]

[2017-12-29 23:15:03.190 UTC] Malware binary stops: Last execution of malware binary occurs. *Malware process execution has been successfully completed.* [vds.cs59923.timeweb.ru, Daniel-PC]

[2017-12-29 23:16:34 UTC] C2 Connection: Initial connection with C2 server. *C2 server plays a central role in coordinating and executing malicious activities on the compromised devices, this is its initial connection.* [ckkxyupextanlvcrdig[.]com, Daniel-PC]

[2017-12-29 23:16:10.787] Exposed: LAB-Win10-02 is exposed to the threat associated with ciso[.]guide. *Host is vulnerable to a drive-by-compromise/other malicious redirects.* [Ciso[.]guide, LAB-Win10-02]

[2018-01-02 05:39:55 UTC] Most recent successful connection with C2 server. *C2 communication most likely denotes instructions for malicious activity.* [ckkxyupextanlvcrdig[.]com, Daniel-PC]

[2018-01-08 16:40:49.938 UTC] Last attempted (but unsuccessful) connection with C2 server. *Contact with the C2 server is halted, did they get what they were looking for?* [ckkxyupextanlvcrdig[.]com, Daniel-PC]

[2017-12-29 20:58:29-20:58:31 UTC] Spear phish attack (begins): S.P. email sent to p.brand@at-usa.co, m.land@at-usa.co, d.walker@at-usa.co, and s.adams@at-usa.co . *AT-USA employees' personal emails are vulnerable to internal risk.* [daniel@mail.at-usa.co, LAB-Win10-04/10-03/10-02 & LAB-Win7-01]

A2c WHAT HAPPENED • **What actually happened during this incident?** This should be a description of the sequence of events that occurred during this incident, listed in chronological order. This should be one of the lengthier answers in your SBAR

A suspicious email was sent to several AT-USA employees: S. Adams, P. Brand, D. Walker, and M. Land. This message contained a link to a well-known, regularly visited site by company employees (ciso[.]guide.com). The link and email were found to be a part of a spear phish, leading to a watering hole which redirected traffic to a Rig EK landing page. Of the original recipients, P. Brand did not visit ciso[.]guide while it was compromised. Devices LAB-Win10-03 and LAB-Win10-02 were both exposed but were not compromised. The device 'Daniel-PC' should be considered compromised and infected. This device was compromised by the EK and the malware the EK distributed. LAB-Win7-01 should be considered compromised by the EK, but not infected. Device LAB-Win10-04 was not exposed to the threat.

Through this, a Rig exploit kit was used and successfully compromised and delivered Ramnit malware to one device (Daniel-PC). It seems the vulnerabilities exploited were related to Microsoft Internet Explorer, Microsoft Office, and Adobe Flash (could potentially include Microsoft Silverlight as well)

A3 ROOT CAUSE ANALYSIS • **What vulnerable services or threat vectors were taken advantage of during this incident?** Note version number whenever possible.

~~The "human" element was taken advantage of in this incident. The spear phishing attack (and phishing attacks in general) ultimately depend on the person being targeted to click on the link themselves, opening the door for~~

~~risk.~~

The threat utilized in this attack was a Rig EK, delivered by a drive-by-compromise, as part of a watering hole attack. Threat vectors that allowed for this attack include common targeted vulnerabilities such as Microsoft Internet Explorer and Adobe Flash, with focus on Internet Explorer in particular.

A4a SCOPE • **How large is the scope of the incident?** *How* many devices were affected in *what* way?

(4) internal host devices associated with AT-USA seem to have been affected, ranging from only exposed to the threat (3 of the 5 devices), to fully compromised and infected (1 of the 5 devices).

LAB-Win7-01: exposed and compromised, but not infected

Daniel-PC: compromised and infected with Ramnit malware

LAB-Win10-03: exposed to EK landing page, not compromised

LAB-Win10-04: this device was not exposed to the threat

LAB-Win10-02: exposed to EK landing page, not compromised

A4b SCOPE • **Which internal hosts were involved?** Be sure to list the role that each internal device played in this incident. *Include both hostname and IP address whenever possible.*

Daniel-PC (10.5.10.130, 10.5.10.125); \daniel (daniel@mail.at-usa.co) - this device was exposed, compromised, and infected by the malware delivered by the Rig EK; AND also has a different email header than the other AT-USA employees.

LAB-Win7-01 (10.5.10.129); \s.adams (s.adams@at-usa.co) - this device was exposed and compromised by the EK, but not infected.

LAB-Win10-03 (10.5.10.128); \m.land (m.land@at-usa.co) - this device was exposed to the threat.

LAB-Win10-04 (10.5.10.116); \p.brand (p.brand@at-usa.co) - this device was not exposed to the threat, but did receive an email.

LAB-Win10-02 (10.5.10.127); \d.walker (d.walker@at-usa.co) - this device was exposed to the threat.

A4c SCOPE • **Were any users OR services OR devices compromised?** If so: describe what, exactly, was compromised...& what caused the compromise?

~~It does look like host\user LAB-Win7-01\s.adams has been compromised and infected; heavily obfuscated javascript code (that appears to be malicious) was found in sysmon logs on this host which originated from executable files named 'cmd.exe' and 'wscript.exe'. These two processes were found to have created additional files on this device.~~

The device 'Daniel-PC' should be considered compromised and infected. This device was compromised by the EK and the malware the EK distributed. LAB-Win7-01 should be considered compromised by the EK, but not infected. User '\Daniel' from Daniel-PC\Daniel should be included and considered compromised.

A4d SCOPE • **Which external hosts were involved?** Be sure to list the role that each external host played in this incident. *Include both resolved domain name and IP address whenever possible.*

Ciso[.]guide.com (IP: 35[.]196[.]138[.]220) - this is the watering hole that redirected traffic to the Rig EK landing page

Vds[.]cs59923[.]timeweb[.]ru (IP: 176[.]57[.]214[.]103) - this is the EK landing page for the Rig EK

Ckkxyupextanlvcrdig[.]com (194[.]87[.]109[.]183) - this is the malware's C2 server used for communication

A5a `SEVERITY` • **How serious is this incident?** Assess the severity of the incident by taking into consideration factors like whether anything of potential value was compromised, and how much this incident disrupted normal business functioning.

~~This incident is pretty serious, depending on what information is on the compromised host. Could affect the entire business and related constituents.~~

There is currently insufficient information for a definitive assessment of severity. Although Daniel-PC did get infected, the situation could have been much worse had other workstations been infected as well. Further questioning and investigation is needed to determine whether Daniel-PC has access to sensitive business-related information which could result in business function disruption.

A5b `SEVERITY` • **Of the compromised users OR services OR devices, were any of particular value to an attacker?** This answer should address whatever you described in the answer to `Were any users OR services OR devices compromised?`.

There is insufficient evidence to determine whether any of the users/devices compromised contained/have access to data or sensitive information that is of value.

A5c SEVERITY • **Did `$whatever_was_compromised` have access to `$anything_of_value`?**

There is insufficient evidence to determine whether any of the users/devices compromised contained/have access to data or sensitive information that is of value.

A5d SEVERITY • **Was `$anything_of_value` stolen||exfiltrated during this incident?**

At this time it is unknown whether anything of value was exfiltrated, but there is evidence of successful pipe connections being created from one of the compromised devices (Daniel-PC - EventCode=18) - indicating connection between client and server. [170 cases between 22:18:37.239 - 23:59:34.539 UTC 2017-12-29]

A6a INCIDENT RESPONSE (SO FAR) • **Has the threat been contained?**

To my knowledge the threat has not been contained.

A6b INCIDENT RESPONSE (SO FAR) • **To your knowledge, were any immediate mitigations put into place?**

I do not believe any mitigations have been put into place.

RECOMMENDATION

The `RECOMMENDATION` section is where you reflect on how the organization might prevent incidents like this from happening in the future—be proactive! Be forward-thinking!

Always explicitly state your reasoning for making a particular recommendation.

REMEMBER:
• **You must always make a cost||benefit analysis when considering recommendations—prioritize solutions that offer the *greatest coverage* for the *least amount of effort*.** The amount of effort required by the organization to implement a suggestion should absolutely be justified by the degree of protection undertaking such an implementation would afford. Your recommendations are only as valuable as they are realistic to actually implement.
• **Be sure to include sufficient information about each recommendation** so that if another employee were tasked with implementing your recommendations, they will not need to do any additional research in order to implement your suggestion. If you're recommending that additional research into determining a viable specific solution be made, that should be stated explicitly.
• **Do not make *generic* security recommendations that are NOT related to what occurred during this incident;** each recommendation you make should be obviously related to something that is involved in the incident you are writing this SBAR about.

INCIDENT RESPONSE||TRIAGE

Try to include some immediate incident response triage recommendations. What immediate recommendations would you make to help contain the incident and prevent it from potentially escalating in `SEVERITY` &&|| `SCOPE`?

R1a `INCIDENT RESPONSE||TRIAGE` • **Should any devices be considered compromised and quarantined and/or reimaged?** If so: list each, describing what exactly should be done.

The device 'Daniel-PC' should be considered compromised and infected. This device was compromised by the EK and the malware the EK distributed - given this information, it is my recommendation that this device be promptly quarantined, forensically imaged for additional evidence, and then reimaged.

LAB-Win7-01 should be considered compromised by the EK, but not infected - recommendation would be to quarantine this device and remove undetonated payloads, reimaging not required. File names include: bilo467.exe, bilo161.exe, bilo494.exe, bilo439.exe

Devices that were only exposed to the threat do not necessitate remediation.

R1b `INCIDENT RESPONSE||TRIAGE` • **Should any credentials be reset?** If so: belonging to which user(s) and/or services?

~~I would recommend credentials for *all* devices be reset as a precautionary measure given the circumstances - with an emphasis on Daniel-PC (a confirmed compromised and infected device), as all credentials used and inputted on this device its applications could be compromised as well.~~

Being compromised and infected, credentials on Daniel-PC should be reset as all credentials used and inputted on this device and its applications could be compromised as well.

R1c INCIDENT RESPONSE||TRIAGE • **Should any devices be singled out for additional analysis? (Should any logs be gathered from a particular device?)** If so: be sure to specify which device(s), what evidence you would want to access on each device, and what unanswered||remaining||open questions examining this additional evidence would help you resolve.

~~Daniel-PC and LAB-Win7-01 should be singled out for additional analysis. Both of these devices should have logs gathered and investigated further in order to determine whether any additional malicious activities occurred.~~

I highly recommend that Daniel-PC should be singled out for additional analysis. I recommend utilizing both disk and memory images for analysis, with an emphasis on the memory image in order to look deeper into malware and other threats/ongoing activities on this device. During this analysis, it should also be investigated whether this device contained or has access to sensitive information/data that could be of value to the attackers. An investigation into whether data was exfiltrated is also recommended to determine whether information was confirmed accessed and stolen.

R1d INCIDENT RESPONSE||TRIAGE • **Do any employees need to be questioned?** If so: whom, and regarding what? What unanswered||remaining||open questions would interviewing this employee help you resolve?

I would recommend questioning the employee (Daniel) who owns Daniel-PC. While there is no evidence that Daniel was the sender of the emails, they were sent from the address 'daniel@mail.at-usa.co'. Questioning Daniel would also shed light on whether his device contained or had access to any information that could potentially be valuable to an attacker.

R1e INCIDENT RESPONSE||TRIAGE • **Does anybody—people or companies—need to be notified about this compromise or breach?** If so: whom, and what exactly do they need to be informed about?

The client, AT-USA, should be informed as this was originally classified as non-threatening. The system administrator, and all network analysts/related employees should be informed about the situation's new findings.

R1f INCIDENT RESPONSE||TRIAGE• **Do any new investigations need to be started?** If you discovered any potentially suspicious activity that turned out to not be related to your current investigation, be sure to specify here.

I do not have any recommendations for additional investigations related to non-incident related activity at this time.

I would recommend looking into the email address of daniel@mail.at-usa.co as this address is responsible for delivering the original emails and seems to have a distinctly different email header than the rest of the AT-USA employees.

R1g INCIDENT RESPONSE||TRIAGE • **Should any old or ongoing investigations be amended with corrected information discovered during this investigation?** If this investigation is related to a another investigation and you were able to determine any of the other investigation's findings were incorrect, specify what needs to be amended here.

The original investigation conducted by analyst 'Boots' needs to be amended and corrected with information discovered during this investigation as the original outcome found was classified as non-threatening.

PREVENTION OF FUTURE INCIDENTS OF THIS TYPE

In your ASSESSMENT section, you should have identified in A3 (*What vulnerable services or threat vectors were taken advantage of during this incident?)*—whatever you identified in answering that question...you want to make remediation recommendations, whenever possible, on how to better protect that threat vector from being abused again in the future. What options does the client have when it comes to deciding how to prevent these in the future?

R2a PREVENTION • **Can you recommend any changes that could be implemented within the company's internal infrastructure that would actively prevent another attack like this from succeeding in the future?**

~~I would reinforce the dangers of phishing attacks with current employees. The best thing is to invest the time into educating about these attacks, and what they should do when they believe they are being targeted.~~

I would focus on implementing security measures that minimize the window for device/application vulnerabilities which includes:

- Banning Outdated or Easily-Exploitable Browser Plugins: Prohibit the use of vulnerable plugins like Flash or Silverlight. This would significantly reduce the attack surface for drive-by compromise threats.
- Implementing Built-in Exploit Protection: Utilize exploit protection strategies to intercept the exploit chain before it escapes the browser's sandbox.
- Security applications like Windows Defender Exploit Guard (WDEG) and Enhanced Mitigation Experience Toolkit (EMET) can mitigate exploitation behavior.

- Web-Based Content Filtering: Implement some form of web-based content filtering to significantly reduce the likelihood of encountering drive-by compromises within the organization's devices.
- Script blocking extensions can prevent the execution of JavaScript commonly used during the exploitation process.
- Adblockers can help prevent malicious code served through ads from executing in the first place.

R2b PREVENTION • **Can you think of any changes that could be made to the company's standard internal policies might better protect the company's infrastructure from being so vulnerable to this type of attack?**

Possibly an internal policy regarding suspicious emails that requires all employees to automatically report these, no matter how legitimate they may seem.

TECHNICAL APPENDIX

The TECHNICAL APPENDIX is where you "show your work" for the findings you have described in detail in the ASSESSMENT section.

REMEMBER:
• The potential reader of this SBAR is likely distracted and strapped for time—if they need to dig into the technical details of your analysis, they should be able to reproduce your results that led you to your conclusions using the details you include in your TECHNICAL APPENDIX. Keep the SBAR clear and concise by providing answers that are easily grasped *even if your reader is scanning your report quickly for relevant information.*
• All information required to reproduce your findings reported in the SBAR proper should be included here. If you were to need to replicate your investigation findings a year from now (after you've forgotten all the details yourself), what technical details would you want to have provided here to help save you time replicating your original findings? That's exactly what

should be included here.
• Feel free to include Splunk search result URLs for valuable search queries, but if you do: clearly describe *why* the search was valuable so that nobody has to click it, load it, and then guess how it is relevant.

[2017-12-29 20:58:29 UTC] S.P. email sent to p.brand@at-usa.co (siem_event_id: email:1:7383)

[2017-12-29 20:58:29 UTC] S.P. email sent to m.land@at-usa.co (siem_event_id: email:1:7430)

[2017-12-29 20:58:30 UTC] S.P. email sent to d.walker@at-usa.co (siem_event_id: email:1:7313)

[2017-12-29 20:58:31 UTC] S.P. email sent to s.adams@at-usa.co (siem_event_id: email:1:7255)