The SOC Analyst Method Template

Reason

This alarm fired because <specific user/device/IoC> was observed <what they did> and <why it looked malicious>.

Supporting Evidence

Event start time:
Event end time:
Timezone:

Source Identity:
<name of employee involved>
<title>
<username>
<email>
<manager>
<last login>
<location>
<standard/privileged/vip>

Destination Identity:
<name of employee involved>
<title>
<username>
<email>
<manager>
<last login>
<location>
<standard/privileged/vip>

Source Device: <source fully qualified domain name/hostname from alert>
Source IP Address: <source IP address from alert>
Source Device Type: <endpoint/server/dev/prod/web server/domain controller..etc>
Source Email Address: <email address of the source if in the alert>

Destination Device: <destination fully qualified domain name/hostname from alert>
Destination IP address: <destination IP address from alert>
Destination Device Type: <endpoint/server/dev/prod/web server/domain controller..etc>
Destination Email Address: <email address of the destination if in the alert>

File name: <filename of the file associated with the alert>

File MD5: <MD5 hash of the file associated with the alert>
File SHA1: <SHA1 hash of the file associated with the alert>
File Size: <File size of the file associated with the alert
Signed By: <file signature, N/A if no signer>

Original URL:

Raw Logs:
<paste relevant logs>

Account Actions:
<paste any relevant actions the account has taken>

Analysis

Whois:
<paste whois information for the IoC>

Landing URL: <wheregoes landing url>
Domain age: <age of domain>
Reverse IP: <paste how many websites are hosted at this IP>

VT: <virustotal results “3/63 as malicious”>
IPVoid: <ipvoid results>
URLVoid: <URLVoid results>

URLScan.io Verdict: <malicious/clean>
Joe Sandbox Verdict: <malicious/clean>

TOR Exit Node: “Y/N”

Historical Alerts:
<paste any relevant ticket numbers for user/device/threat actor>

Google Results:
<paste any blogs or other websites that describe the reputation/nature of the IoC>

Actions:
<write immediate actions that you took such as disabling an account, resetting password, deleting emails..etc>

Conclusion

<reason for the alarm><supporting evidence that was analyzed and its resulting verdict><action that you took and how you closed the ticket>

Next Steps

<any outstanding or recommended items that need to be addressed>