Logging and Monitoring Walkthrough

Wednesday, December 8, 2021

**Logging and Monitoring Agenda-**

* + What events are logged? Sign-ins? Etc. If failed attempts are repeated multiple times, are log failures recorded and identified? (From a AD perspective, is there anything that pops up that is communicated with Mark and team)
  + What AD Domain Controller events are monitored by the WCS team?
  + Are logs sent to Splunk? Understanding Splunk as a whole.
  + Any concerns with the logging activities?
  + What triggers log reviews? (Alerts) - Through email, phone calls etc. Walk us through an event that took place. Who gets alerted
  + What actions are taken to remediate alerts? Timeframe.
  + What corporate standards are being leveraged?

Attendees:

Machine generated alternative text:
Oluwaseyi Mafi 
Host, me 
Ann Marie 
Bianca Moon 
David Kaemmerer 
Emely Santos 
James Rose 
Jeffrey Harris 
Joseph Rocha 
Mark Ostrowski 
Michael Shanahan 
Nicole 
Ryan Evans 
Ryan Greene 
Saurabh Dilip Saxena 
Terri Ann Quiambao 
Todd Savoy 

And Tyrell Jarett

**AGENDA:**

**What events are logged? Sign-ins? Etc. If failed attempts are repeated multiple times, are log failures recorded and identified? (From an AD perspective, is there anything that pops up that is communicated with Mark and team)**

Jim: We run Splunk, and SCUM for monitoring active directory. We have

* + OS level monitoring, CPU.
  + Second part and most critical, SCUM monitoring. Microsoft has a monitoring package. Specifically looking at active directory data and Alerting.
  + The last part. Event logging. Goes to Splunk, the collecting application that runs in the main cores. That's how we retain things. We use the events for alert driving purposes.

Mark: If a domain controller is not replicating properly, SCUM picks it up.

**Is this Automated?**

Mark: There is a team of engineers responsible for the SCUM environment. All the alerts are configured by the SCUM team through the scum console. CPU memory, hard disk, it will occur there. And the SCUM is the active directory monitoring application while Splunk is for monitoring all the security ingestions, and events that are triggered.

**What team monitors Splunk?**

Underneath global security. Infrastructure monitoring. **The most important logs are security logs, Authentication, account lock outs**.

**Any communication with the global security team?**

Mark: We monitor specific event. We can look at where there might be issues. A service account getting locked out for whatever reason, we look into that using our dashboard, looking into the account and help troubleshoot the issues. These areas include:

* + Troubleshooting issues in Active directory
  + Also, on the security end if we have to do investigation from the security end, issues like who is using it, what desktop, etc. **For security event, it is monitored by the SOC team**.
  + Event of domain controller, Mark is always alerted. And his team is also alerted.

**What mode do these alerts come in as?**

**Do you follow any SLAs?**

 Mark: Done through emails. As soon as we get alerted, we get on top of them. We look at the Splunk logs like the SOC team does as well. Is the domain controller overloaded compared to the other domain controllers? We are looking at the health of our environment using Splunk.

**How quickly do you resolve these issues?**

We ingest all the security logs within Splunk. We can see all authentication request. We utilize Splunk as a tool. Looking at problems and addressing. We also look for suspicious activities. Splunk is used in multiple different ways.

Julie: We use Splunk for environmental analysis and incident response. Based on the alerts we receive, we determine the response. The nature of the alert will dictate the response time.

**Any issues?**

Julie: No issues so far. It's an ongoing activity. No outages or concerns.