Team: Team 08

Inject Number: 35

Inject Duration: 180 Minutes

Inject Start Date/Time: Sat, 16 Mar 2019 16:39:13 +0000

From: CISO

To: IT Team

Subject: D101 - DNS Logging and Review

Due to a recent audit finding, we have been instructed to log our DNS traffic to a central repository (logging service software as approved by your company) and retain those logs for 30 days. Perform a cursory review of this traffic in attempt to identify suspicious activity and indicators of compromise. Document your solution and findings with screenshots and include any other pertinent details. Reply in a business memo with your findings.

Objectives:
*Enable Logging on your DNS server and provide evidence of this
*Send those logs to a searchable logging solution and provide evidence of this
*Review these logs to look for IOCs (indicators of compromise); summarize your findings with a conclusion in regards to having observed suspicious traffic or not

Thank you.

CISO