Hyper-Automation Candidates in Security Operations Center

Remember the days when customers would call their banks or customer care to find the status of money debited/credited, credit limit, billing dates etc.? The calls were answered by customer care associates. Over the years, we have seen that all of this information is rendered by an Interactive Voice Recording system and there is very little-to-no human interaction for most of the simple queries you may have for a service provider. There has been a drastic change in the back ground where a machine is doing the job that, who knows, how many customer care associates were doing. The changes behind the screen is not visible to the customer, however the customer still gets the requested information.

Let's now try to relate that to our cyber security life and draw a parallel.

Based on the survey conducted by Black Hat in Aug 2016 *"… nearly three-quarters (72%) of respondents felt it is likely that their organizations would have to deal with a major data breach in the year ahead. Approximately two-thirds of respondents said they did not have enough staff, budget, or training to meet those challenges"*. The gap between what we expect will happen and what we need to do is widening.

A team from Wipro participated in Black Hat and DefCon conferences. Reputed and established vendors were showcasing their capabilities and were vying against each other to tell how their product fares better than others in the market. Stall after stall, more and more jargons, dashboards and survey results were thrown at us. A portion of the estate at the Black Hat business hall was allocated to "Innovation City", where little known organizations were bustling with people. We ran into two vendor booths, Phantom and Demisto. Phantom and Demisto, call themselves *Security Orchestration / Incident Response Platform* and they both functionally do the same thing. They automate tasks that are simple, flow based and repeatable. Tasks that rely on standard operating procedures or on playbooks can be digitized and can be accomplished by running scripts.

Let's consider an example of a phishing email which keeps the security team busy. Once there is a trigger on a phishing email, we can have the platform perform the following tasks automagically:

- Send an awareness email to the phishing mail recipient warning of the phishing attempt
- Search our environment for other users who may have received the phishing mail with similar attributes
- Check the URL / attachment contained in the email for reputation against Threat Intel subscription sources
- Block the suspicious URL on proxy servers once it is confirmed malicious
- Remove the email from the user's inboxes and inform the users of the phishing attempt

All of this happens with the existing environment in a non-disruptive manner. It thus relieves an analyst of mundane jobs and gives more elbow space for the analyst to contribute higher up in the value chain.

So, do these *Security Orchestration / Incident Response Platforms* address the challenge of shortage of resources and having to deal with an incident or a breach in the near future? To a great extent, yes! Efforts and tasks accomplished with a tool are more measurable than tasks accomplished manually. Hence usage of these tools in an organizations would make tasks accountable, auditable and because it is automated, it becomes efficient in terms of time. Apparel and merchandise is delivered to customers via drones, driverless

cars, robotic and remote surgery are all a reality today. There is no reason why Security Incident Response should not take the next big step, automation!