|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **OJT LITE TEMPLATE** | | | | **Completion sign-off** (Signature / Date) |
|  | **Name of Intern** | **Jonathan Ho** | **NP Internship Supervisor:** | Mr Andy Ng |  |
|  | **Dates of Internship** | **09/09/2024 – 24/01/2025** |
|  | **Company:**  **Department:** | **NCS Pte Ltd**  **Managed Security Services, Security Governance** | **Company Mentor:**  **Designation:** | Vijayendran Ramalingam  Security Governance Team Lead |  |
|  | **Job Designation** | **IT Security Officer (ITSO)** |
|  | | | | | |
| **#** | **Main Tasks** | **Task Elements** | **Knowledge, Skills & Attitude** | **Training Guidelines** | **OJT Hours** |
|  | Describe the main tasks (taken from the job description).  Begin with a verb (to indicate the desired learning outcome). | List the steps in each main task. | List the knowledge, skills & attitude needed to accomplish the main task. | Highlight the methods & training materials used to carry out the training. (You can use any of the following headers: Explain / Demonstrate / Provide / Show / Discuss etc) | List the estimated hours that the Main Task requires. |
| 1 | Process Review: Realignment of Security Deviation Template  (part of doc review) | * Review of process related documents (i.e. Vulnerability Management, Hardening Guide, Patch Management, Security Deviation Request templates) * Assessment of the Templates (i.e. Unique requirements, common information) * Revamp templates into a singular cohesive excel formatting with clear permissible inputs for relevant Value fields * Acquire approval from iSEC before implementation & any improvements/changes to be made via presenting the proposal and final product. | Knowledge:   1. Basic understanding of security and how systems work 2. Ability to work with different security tracks and partners (various tracks, PWC, iSEC) 3. Understanding of security tools:    * Rapid7: For finding system vulnerabilities    * AlgoSec: For checking security rules    * Archer: For managing risks   Skills:   1. Understanding of security guidelines (IM8) including:    * How to identify different types of risks    * How to assess their impact    * How to determine how likely they are to happen    * How to fix or manage these risks 2. Good grasp of procedures:    * Know which templates to use and when    * Combine multiple documents into one seamless Excel file    * Understand how to manage different versions of documents   Attitude:   1. Detail-oriented:    * Pays attention to small details    * Takes care in following current processes    * Makes sure documents are properly formatted 2. Good at managing change:    * Can create new versions of documents that maintain familiarity    * Helps others understand and adapt to new versions    * Makes transitions between different versions smooth 3. Ability to take feedback:    * Able to take feedback cohesively and improve the template based on stakeholder’s needs. | Explain   1. SOP is used as a guideline when we are doing the review process for each document at hand 2. Usage of established internal SOPs to better understand the template fields 3. Shadowing of colleagues at the start and learning the important points to look out for when creating the unified template 4. Presentation of PowerPoint slides to stakeholders involved helps in the alignment of expectations with all parties. | 1 week: 8hrs  Falls under the AlgoSec Process Enhancement Review. |
| 2 | Rapid7 (whitelisting processes) | * Creation of SOP for whitelisting procedures for Rapid7 * Need clarification from Supervisor | Knowledge  Understanding of criteria of certain rapid7 vulnerability logs and whitelist certain false positives as well as maintenance of current lists of whitelisted items.  Skills   1. Ability to navigate rapid7 vulnerability management. 2. Use of InsightIDR in threat detection and response as an SIEM 3. Attention to detail in creating the SOP as it is a new addition in the environment and a completely new SOP. 4. Ability to determine whether a vulnerability requires remediation or is a false positive in the environment and checking with the tracks to confirm these, creation of a form to fill up to whitelist certain false positives. 5. More clarification would be needed   Attitude   1. Attention to detail in the usage of the product, as we are mainly using it for threat detection in the environment. 2. Curiosity in exploring the different methods to create whitelists using GUI/CMD prompts. 3. Understanding the SOP’s formatting and providing users a smooth process in implementing new whitelists and provide templates for users to request for websites to be whitelisted. | Explain   1. Usage of Rapid7 to find vulnerabilities in the environment and what are the remediation measures that the application recommends. 2. Ability to first use the application and then view how many logs are redundant due to non-invasive false positives. 3. Able to create an SOP to locate and find the hits for the vulnerabilities and the relevant tracks for that vulnerability and either remediate or whitelist the vulnerability. | TBC |
| 3 | AlgoSec Automation/Process enhancement for Ruleset and Policy review processes. | * Perform assessments, monitor firewall logs and review rulesets and policies as well as finding improvements (if any) from the existing SOP (both internal and official) * Identify multiple actionable plans and strategies to present to the respective stakeholders to align expectations of the processes and pre-requisites involved. | Knowledge  Thorough understanding of solution’s numerous applications and the automation functions that come out of the box.  Skills  Ability to utilize both GUI and command line solutions for automating  Identification of the pre-requisites and other miscellaneous requirements required in the automation: i.e. credentials needed, permissions, email and SMTP servers.  Attitude  Curiosity to explore the numerous ways to implement the automation in the environment.  Attention to detail to ensure that all necessary implementations are in place to allow this automation such as setup of an email forwarder in the intranet, relevant mailing lists, IPs and firewall rules to allow these, etc. | Explain   1. Locate and find ways to implement automation for rule review processes such as auto forwarding logs weekly. 2. Automatic analysis of risky rules, remediation plans provided in Algosec firewall analyzer, and forwarding these in a format that would be easy to use for reports. 3. Set up of mail forwarders, raising SRs to set up the email servers, producing an initial plan on the processes and prerequisites involved to ensure a smooth implementation. 4. Automating location of firewall rule owners such that rule owners are tagged to tracks and team owners to find for simpler review processes. |  |
| 4 | Warrant of Fitness (WoF) tracking/tracker handling and miscellaneous processes | * Need clarification from Supervisor | Review of hardening artefacts and warrant of fitness(WoF), and approve the WoF, and submit review checklist and approval status regularly to all the relevant tracks.  Upload hardening guides based off identified IM8 clauses, relevant industrial standards, most notably: ISO27001.  Knowledge  Thorough understanding of different OS, software like cyberark, hardening procedures according to IM8 clauses and appropriate remediation/ mitigation measures to recommend to tracks when needed.  Ensure the artefacts are all up to standards such as if all the software packages are approved, OS mentioned is hardened accordingly such as OS patching had been done, such that it is compliant to the IM8 Clauses/ to our approved hardening guides.  Ensure that the RSA netwitness artefacts, SIEM artefacts are provided with actual captures of administrative event logs shown in the SIEM. Ensure that the splunk artefacts are also logged into the system.  For disaster recovery only for the applicable systems, ensure the DR is properly setup.  Other stuff like Imperva, Tripwire, carbon black, CyberArk,,Banffcyber, etc, are to have artefacts submitted in the report.  Skills  Ability to utilize check and formalise reports to submit to higher ups.  Able to identify the IM8 Clauses relevant to the deviations and how to implement the correct remediation or mitigation efforts for the environment to assist teams to raise for that deviation for the device.  Attitude  Attention to detail is important as specific clauses and industrial standards need to be upheld in the environment as security is crucial with the sensitivity of the data being handled. | Would need more clarification on these, specific roles and functions not explicitly given out. | TBC |
| 5 | eTRS SOC compliance implementation | * Need clarification from Supervisor | No specific details given, would require clarification on tasks. | TBC | TBC |
| 6 | Firewall Log Review processes | * Review and monitoring of firewall logs * Review and compilation of rules that are to be disabled, deleted, removed, etc. * Email respective rule owners, clarification of rule deletion, modification, and others to confirm the actions (deletion, etc) are correct/okay. * Compilation of firewall review summary tables such as the number of rules unused, removed, temporary, special, etc. * Update relevant firewall team members, network team members, etc of the rules and changes to be made. | Knowledge   1. Knowledge and familiarity in reviewing firewall rule logs and being able to identify anomalous rules based on a set criteria such as risky ports without valid reasons for usage of the ports in service requests. 2. Able to spot incorrect implementation of firewall rules by the firewall team such as wrong users, ports, name, etc. 3. Knowledge on reporting standards such as how to format the report, wording of why rules are anomalous, root cause/fish-bone analysis of how anomalous rules had been implemented, 4. Ability to review   Skills   1. Understanding of the Breakglass safe and storage management process    * How to tally records of Breakglass check-in and check-out logs.    * How to escalate the record if an anomaly is found.   Attitude   1. Attention to detail for reviewing older logs which do not have an up-to-date service request ID, which requires manual checkups of the new rule owners |  | 50 hours |
| 7 | Breakglass BAU & update of SOP processes (Administrative account review) | * Review the check-in and check-out dates of the physical Breakglass records and compare them with Breakglass records that are stored in database. * Ensure that record Account ID (e.g.: ID, domain, servers, envelope/package ref, number of accounts or items) are correct. * Ensure that both records align with one another and raise any anomalies with higher ups. | Knowledge   1. Knowledge and familiarity of the Breakglass security procedure.   Skills   1. Understanding of the Breakglass safe and storage management process    * How to tally records of Breakglass check-in and check-out logs.    * How to escalate the record if an anomaly is found.   Attitude   1. Detail-orientated    * Pays attention to small details 2. Careful to spot any errors in reviewed documents | Explain  Demonstrate   1. Check that Service Request for the breakglass procedure can be found on the Service Request platform. 2. Ensure that the requester name and request ID are correct. 3. Compare the check-out dates and check-in dates of the Breakglass envelope on the physical file as well as the Service Request platform. 4. If check-in / check-out dates are misaligned, we need to raise the issue to higher ups to reconcile the error. | BAU at end of each month |
| 8 | Application log reconciliation for all tracks within DC3 architecture - under damien | * Need clarification from Supervisor |  |  |  |
| 9 | Automation (TBC) | * Not much efforts being engaged in this portion currently, will update once more details are provided. | TBC | TBC | TBC |
| 10 | GITSIR | * Review of CVEs related to the environment and roll out of updates/mitigation/remediation efforts for all the affected devices. * Update to client personnel for confirmation of the related CVEs, any additional remediation or mitigation efforts needed, estimation of the remediation timeline, etc. | Knowledge:   1. Knowledge and familiarity in the vulnerability scanning and vulnerability assessment process.   Skills:   1. Ability to identify the systems and teams that have the OS, applications, Software, etc. That are affected by the CVEs that have updates that came out. 2. Assist teams with remediation/mitigation efforts for CVEs that are not addressable with updates, such as when applications are not up to date with current versions 3. Usage of IM8 clauses in helping deviation efforts for the devices affected. Such as the possible deviation that needs to take place.   Attitude:   1. Detail-orientated, pays attention to the CVEs addressed by the updates, and which applications still require mitigation efforts according to the proposed IM8 timelines |  | A BAU task,  Roughly 3hours/week |
| 11 | Vulnerability Assessment | * Review of OS vulnerabilities picked up by vulnerability scanner for various environments * Email respective teams about the vulnerabilities * Compilation of responses to vulnerabilities (i.e. Seeking deviation, remediated, false positive) | Knowledge:   1. Knowledge and familiarity in the vulnerability scanning and vulnerability assessment process.   Skills:   1. Understanding of the vulnerability assessment process    1. How to identify asset owners and relevant track leaders for vulnerabilities   Attitude:   1. Detail-orientated, pays attention to small details 2. Careful to spot any errors in reviewed documents | Explain   1. After vulnerability scan has been performed, the scan results are sent out to the various asset owners, whose systems have vulnerabilities detected. 2. After receiving the replies from the asset owners, proceed to advise the asset owners (if applicable) to take the necessary steps to remediate the vulnerability. (i.e. Advising asset owners to upgrade to the latest version of their respective systems) |  |