**Rámcový protokol pre implementáciu** –anglická verzia

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  | **Framework protocol for implementation - MISP and TIP setup - List of activities that will fulfill the SaaS delivery** | | | | |
|  | **Partial installation of the service** | **Subcategories of the implementation sequence** | **List of activities to fulfill the deployment of the installation category** | **Date and Signature of the person responsible for the Customer - CSIRT - ORKIB:** | **Date and Signature of the responsible person on behalf of the Supplier:** |
|  | **Main** | **Subcategories** |  |  |  |
|  | **MISP** | MISP | * Integration MISP into the customer´s environment * Setting up sightings view / report * Addition organization's requirements to increase coverage and detection |  |  |
|  | * Normalizing inputs and feed into MISP |
|  | MISP to MISP (can be done in the category Others) | * Design setting how to process a link from non-public to public |
|  | MISP a SIEM (can be done in the category Others) | * Meet the organisation requirements to increase coverage and detection * SIEM integration check * Integration in the form of tagging - content for SIEM |
|  | **Integration** | Integration | Connect threat intelligence platform |  |  |
|  | Integration | Enable data connector |
|  | Integration | Connect threat intelligence upload API |
|  | Integration | Connect to STIX/TAXII feeds |
|  | **TI Platform** | TIP\_TI Platform | Setting up user managment with RBAC with SSO |  |  |
|  | TIP\_TI Platform | Setting up RFI on topics |
|  | TIP\_TI Platform | Setting the source of threats |
|  | TIP\_TI Platform | Setting up the Monthly intelligence reports and Monthly geopolitical reports |
|  | **Threat Intelligence** | TIP\_Threat Intelligence | Setting and overseeing the Possibility to assign alert to different TI analyst |  |  |
|  | TIP\_Threat Intelligence | Testing if Items / Threat Library - provide kinds of reports and analyses like (CVEs, TTPs, Sumaries) |
|  | TIP\_Threat Intelligence | Testing if Items / Threat Library - Item realitionship (TA, malware, campaigns) |
|  | TIP\_Threat Intelligence | Testing if Items / Threat Library can be exported in various formats (JSON, PDF, etc.) |
|  | **Brand Protection / Brand Abuse** | TIP\_Brand Protection | Setting of this part of TIP part in question will take place based on a checklist from the CSIRT.sk (Subject to both Quality and Quantity requirements) |  |  |
|  | TIP\_Brand Abuse | Setting of this part of TIP part in question will take place based on a checklist from the CSIRT.sk (Subject to both Quality and Quantity requirements) |
|  | **The Third Party** | TIP\_3th Party | Setting of this part of TIP part in question will take place based on a checklist from the CSIRT.sk (Subject to both Quality and Quantity requirements) |  |  |
|  | TIP\_3th Party | Setting of this part of TIP part in question will take place based on a checklist from the CSIR.sk T (Subject to both Quality and Quantity requirements) |
|  | **Vulnerabilities** | TIP\_Vulnerabilities | "Enrich Vulnerabilities" - Setting of this part of TIP part in question will take place based on a checklist from the CSIRT.sk (Subject to both Quality and Quantity requirements) |  |  |
|  | TIP\_Vulnerabilities | "Enrich Vulnerabilities" - Setting of this part of TIP part in question will take place based on a checklist from the CSIRT.sk (Subject to both Quality and Quantity requirements) |
|  | TIP\_Vulnerabilities | "Enrich Vulnerabilities" - Setting of this part of TIP part in question will take place based on a checklist from the CSIRT.sk (Subject to both Quality and Quantity requirements) |
|  | **Alert Management** | TIP\_Alert Managment | Review of (1/2) requirements that are defined for the AM category in príloha č.3 Špecifikácia požiadaviek pre TIP |  |  |
|  | TIP\_Alert Managment | Review of (2/2) requirements that are defined for the AM category in príloha č.3 Špecifikácia požiadaviek pre TIP |
|  | **Filtering** | TIP\_Filtering | Setting up / review of the function searching by pre-setting of own tags/topics / based of the predefined requirements from CSIRT.sk |  |  |
|  | TIP\_Filtering | Setting up / Testing the filter functions based on (source country, target country, business sector, first-seen, MITRE technique, common TTPs, vulnerabilities, content category) |
|  | **IOCs** | TIP\_IOCs | Setting up / Testing for Ability to list and filter IOCs |  |  |
|  | TIP\_IOCs | Setting up Whitelisting / based of the predefined requirements from CSIRT.sk |
|  | **Dashboards** | TIP\_Dashboards | Create and sett up custom dashboards |  |  |
|  | TIP\_Dashboards | Review of platforms dashboards base on: alerts, IOCs, threats, vulnerabilities |  |  |
|  | **Documentation** | TIP\_Documentation | Review and handover of EN or SK language documentation |  |  |
|  | TIP\_Documentation | Checking comprehensive API documentation / confirmation from the CSIRT.sk that they can proceed on the basis of this documentation |
|  | **Others** | MISP to MISP | Sync user, test & preview, flow control, setting up MIST to MIST - design how it would be done from private to public - IOCs flow |  |  |
|  | Feeds to MISP | Options, overlaps, setting up free feeds integration, open source, etc. |