**Prehľadová tabuľka kategórií požiadaviek a funkcionalít TIP** – anglická verzia

|  |  |  |
| --- | --- | --- |
| **Category** | **Description of requirements listed as minimum requirements/functionality:** |  |
| **Integration** | **Requirements for Integration:**   * Security stack - SIEM * Security stack - MISP * Integration and Export IOCs via STIX/TAXII 2.1 * Function to select which IOCs will be integrated |  |
| **TI Platform**  **(TIP)** | **Requirements for TI Platform category:**   * Provide user management with RBAC * MFA * Communication over HTTPS * Allow the creation of alerts via email or API calls * Audit Log |  |
| **Threat Intelligence** | **Requirements for Threat Intelligence category:**   * Library must be easily searchable and filterable * Provide a library of reports on attackers * Provide a library of malware reports * Provide a library of reports on significant incidents * Information filtering options (MITRE Matrix) * Allow to request RFIs on a variety of topics * Monitor threats on the dark web * Monthly intelligence reports (global and local, focusing on Slovakia and the EU) * Monthly geopolitical reports (global and local with a focus on Slovakia and the EU) * Its own source of threats |  |
| **Brand Protection / Brand Abuse** | **Requirements for Brand Protection and Brand Abuse category:**   * Monitor open and closed sources on the Internet * Monitor mentions of our organisation, projects, brands * Monitor sensitive data on the Internet (possible data leaks) * Monitor the registration of typosquat domains (and certificates) * Perform removal or help with removal of the websites (website/domain takedown) * Monitor possible threats to important people * Capability to detect exposed access keys * Capability to detect leaked credentials * Detect phishihng websites * Monitor leaked or sensitive data on github, pastebin, etc. * Monitor internet presence of VIP/Executives |  |
| **The Third Party** | **Requirements for The Third Party category:**   * Assess the risk of the supplier/third party supplier * Warning function of a possible third party vendor compromise |  |
| **Vulnerabilities** | **Requirements for Vulnerabilities category:**   * Ability to enrich vulnerabilities with additional information * Prioritizing vulnerabilities * Highlight critical vulnerabilities in specific products |  |
| **Alert Management** | **Requirements for Alert management category:**   * Alert is descriptive enough to investigate by analyst * Alert provides enough recommended actions to remediate * Recommended actions are actionable through via TI platform * Alert is tagged by MITRE TTPs * Alert has relevant IOCs parsed out from the source * Possibility to assign alert to different TI analyst * Posibility to tag an alert by custom tags * Create notes and save attachments * Posibility to filter on alert and posibility to export alerts based on defined * Perform bulk actions on alerts like (whitelist, tagging, status change, etc.) * Save alert filters for later usage * Query on alert data * Create new detection logic * Modify build-in detection logic * Whitelisting option in detection logic (multiple whitelisting options should be provided) * Create automation workflows on alerts * Find/explore potential threats related to the organization * Run default reports on alert date * Run custom reports on alert data * Schedule reports on alert data |  |
| **Threat Library** | **Requirements for Threat Library category:**   * Various kinds of reports and analyses like (CVEs, TTPs, Sumaries) * MITRE techniques description and link to related items. * Threat intelligence news feed * Threat intelligence news summary * Overview of existing items * Item realitionship (TA, malware, campaigns) * Item show related IOCs * Item IOC can be pivoted down to IOC page * Item can be exported in various formats (JSON, PDF, etc.) * Item IOC can be added to blockilst feed * Item show related vulnerabilities * Item shows related MITRE techniques * Item can be bookmarked * Item can be custom-tagged or tagged * Item contains reference to external sources |  |
| **Filtering** | **Requirements for Filtering category:**   * Filter based on (source country, target country, business sector, first-seen, MITRE technique, common TTPs, vulnerabilities, content category) * Search with usage of regex and wildcards * Advanced searching via query * Searching by pre-setting of own tags/topics |  |
| **Feeds** | **Requirements for Feeds category:**   * Consume custom feeds * Allows adding of STIX/TAXII server * Allows adding of MISP server * Enable/disable per threat feed * Assess confidence of every threat feed (IOC if one feed is available) |  |
| **IOCs** | **Requirements for IOCs category:**   * List and filter IOCs * Search of IOCs can be done using wildcards * Platform supports # (hashtags) of IOC types * Tags/custom tags can be used to search IOCs * Whitelisting of IOCs * Export of IOCs in CSV format * Export of IOCs in STIX format * Export of IOCs in MISP format * VirusTotal analysis on top of IOCs, separate virustotal subscription is not needed * Parsing of IOCs from (pdf, html, word) documents is supported and can be included in threat feed * Parsing of IOCs from emails is supported and can be included in threat feed |  |
| **APIs**  (Available in standard programming language - python, javascript, golang) | **Requirements for APIs category:**   * Supports API for IOCs * Supports API for searching/filtering * Supports API for Alerts * Supports API for processed intelligence * Easy management of API tokens * Comprehensive API documentation |  |
| **Dashboards** | **Requirements for Dashboards:**   * Custom dashboards * Situation awareness dashboard * Dashboards base on, alerts, IOCs, threats, vulnerabilities |  |
| **Documentation** | **Requirements for Documentation:**   * Documentation is avalaibale in EN or SK language * Documentation is available for each platform feature. * Ducumentation is updated together with new platform version/feature |  |
| **Others** | **Requirements for category Others:**   * 24/7 support for the platform |  |