# Title: Information Security @ Freshsales

**Objective:** To track and enhance information security related activities for Freshsales product

**Infosec Point of Contacts:**

| **Point of Contacts** | | | |
| --- | --- | --- | --- |
| Sections | SPOCs | Email | Team DL |
| AppSec Team | [Gopalakrishna Peeleti](https://confluence.freshworks.com/display/~gopalakrishna.peeleti)  [Siranjeevi Jayakumar](https://confluence.freshworks.com/display/~siranjeevi.jayakumar) | [gopalakrishna.peeleti@freshworks.com](mailto:gopalakrishna.peeleti@freshworks.com)  [siranjeevi.jayakumar@freshworks.com](mailto:siranjeevi.jayakumar@freshworks.com) | [team-appsec@freshworks.com](mailto:team-appsec@freshworks.com) |
| Infosec - GTM | [Senthilkumar Iyyappan](https://confluence.freshworks.com/display/~senthilkumar.iyyappan) | [senthilkumar.iyyappan@freshworks.com](mailto:senthilkumar.iyyappan@freshworks.com) | [team-gtminfosec@freshworks.com](mailto:team-gtminfosec@freshworks.com) |
| GRC Team | [Ramya Subramanian](https://confluence.freshworks.com/display/~ramya.subramanian) | [ramya.subramanian@freshworks.com](mailto:ramya.subramanian@freshworks.com) | [team-grcinfosec@freshworks.com](mailto:team-grcinfosec@freshworks.com) |
| SOC Team | [Nagamarimuthu Karuppiah](https://confluence.freshworks.com/display/~nagamarimuthu.karuppiah) | [nagamarimuthu.karuppiah@freshworks.com](mailto:nagamarimuthu.karuppiah@freshworks.com) | [team-soc@freshworks.com](mailto:team-soc@freshworks.com) |
| Incident Reporting | - | [security@freshworks.com](mailto:security@freshworks.com) | [security@freshworks.com](mailto:security@freshworks.com) |
| Director of Information Security | [Sriram Krishnan](https://confluence.freshworks.com/display/~sriram.krishnan) | [sriram.krishnan@freshworks.com](mailto:sriram.krishnan@freshworks.com) | - |
| Chief Risk Officer | [Kim Smathers](https://confluence.freshworks.com/display/~kim.smathers) | [kim.smathers@freshworks.com](mailto:kim.smathers@freshworks.com) | - |
| Bi-Weekly Sync Up Meeting -  Thursday between 5 p.m. and 5.30 p.m.  Attendees:- [Siranjeevi Jayakumar](https://confluence.freshworks.com/display/~siranjeevi.jayakumar) [Gopalakrishna Peeleti](https://confluence.freshworks.com/display/~gopalakrishna.peeleti) [Sriram Chandra Mouli Viswanathan](https://confluence.freshworks.com/display/~sriram.viswanathan) [Sudharshan Jayasampath](https://confluence.freshworks.com/display/~sudharshan.jayasampath) [Muthukumaran Murugesan](https://confluence.freshworks.com/display/~muthukumaran.murugesan) | | | |

| **Software Security Maturity Model** | | |
| --- | --- | --- |
| **Level 1** | **Level 2** | **Level 3** |
| 1. Coverity (SAST) and AdvisoryBot (SCA) scans are performed for all releases in the security staging environment    2. Security bugs with priorities P0 and P1 reported through security assessments and responsible disclosure programs are tracked to closure based on agreed SLA | 1. Coverity (SAST) and AdvisoryBot (SCA) capability are integrated into the product's CI to identify and track security bugs to closure in Freshrelease    2. P0 vulnerabilities are not introduced in the production  3. Security bugs with priorities P0, P1, and P2 reported through security assessments and responsible disclosure programs are tracked to closure based on agreed SLA | 1. Coverity (SAST) and AdvisoryBot (SCA) capability are integrated into the product's CI to identify and track security bugs to closure in Freshrelease  2. Authzchecker (DAST) is integrated into the product's CD pipeline to identify and track security bugs to closure in Freshrelease    3. P0 and P1 vulnerabilities are not introduced into the production  4. Security bugs with priorities P0, P1, P2, and P3 reported through security assessments and responsible disclosure programs are tracked to closure based on agreed SLA    5. Threat modeling/security design review is conducted by the respective product teams for features or functionalities that require security considerations |
| **P0 Vulnerabilities:**  1) Remote Code Execution  2) SQL Injection  **P1 Vulnerabilities:**  1) Cross-Site Scripting  2) Vulnerable third party components  3) Broken Access Control  **Product Team Action Items:**   1. To adhere to the defined SLA and close the reported issues 2. To provide the necessary information and access to the security engineering team, to implement the model | | |

|  |  |  |
| --- | --- | --- |
| Security Issues - Dashboard & SLA Compliance | | |
| **List of items** | **Description** | **Fresh release / Confluence Page** |
| Unresolved Security Issues | This filter provides a list of security issues unresolved in Freshmarketer |  |
| Risk Accepted Security Issues | This filter provides a list of risk accepted security issues in Freshmarketer |  |
| SLA Breached Security Issues | This filter provides a list of SLA breached security issues in Freshmarketer |  |
| Security Vulnerability Dashboard | A real-time dashboard that provides deep insight on a security status/trend for all projects in Freshworks Org | [Security vulnerability Dashboard - Power BI Link](https://app.powerbi.com/groups/me/reports/432c83d2-8451-4f18-8419-72e318021236/ReportSectione32c80e56e7dfaac3b22)  [About Security vulnerability Dashboard - Confluence Page](https://confluence.freshworks.com/pages/viewpage.action?pageId=237166630) |
| Freshworks Vulnerability Scoring System ( FVSS) | A common scoring system to rate the severity of the security bugs | [Freshworks Vulnerability Scoring System (FVSS) Link](https://freshdesk.github.io/security/severity-calculator/)  [About FVSS - Confluence Page](https://confluence.freshworks.com/display/SEC/Freshworks+Vulnerability+Scoring+System) |
| Security SLA | Service Line Agreement for fixing security issues  P0 (Urgent) - 1 day  P1 (High) - 15 days  P2 (Medium) - 45 days  P3 (Low) - 60 days | [About SLA - Confluence Page](https://confluence.freshworks.com/display/SEC/Freshworks+Vulnerability+Scoring+System) |

|  |  |  |  |
| --- | --- | --- | --- |
| CI-CD Tools Integration | | | |
| **Tools** | **Confluence Page** | **Implementation Status** | **Runway Job** |
| Coverity | [Coverity Integration](https://confluence.freshworks.com/display/SEC/Coverity+Integration) | **Yes** | <https://freshsales.runwayci.com/job/Coverity-PR-Freshsales/> |
| Coverity Enabled Repos | [Coverity Integration](https://confluence.freshworks.com/display/SEC/Coverity+Integration) |  | [Repos](https://docs.google.com/spreadsheets/d/12y5mduupu-ur4n0RQxRah2XDpSkgVA0W08gQCiZ49Dw/edit?usp=sharing) |
| AdvisoryBot | [AdvisoryBot Configuration](https://confluence.freshworks.com/display/SEC/AdvisoryBot) | **Yes** |  |
| AdvisoryBot Enabled Repos | [AdvisoryBot Configuration](https://confluence.freshworks.com/display/SEC/AdvisoryBot) |  | [Repos](https://docs.google.com/spreadsheets/d/1n8esNhGUPn63s2VApW5jBaD_nanMPp6_2hZGq0NxPuU/edit#gid=0) |
| Trivy | [Trivy Integration](https://confluence.freshworks.com/display/SEC/Container+Image+Security+Using+Trivy) | **Yes** | <https://freshsales.runwayci.com/job/Trivy-image-scanner/> |
| Authzchecker | [Authzchecker Configuration](https://confluence.freshworks.com/display/SEC/AuthzChecker) | **No** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Security Awareness & Training | | | |
| **Training** | **Timeline** | **No. of Participants** | **Presentation Drive** |
| Security Focus QA Training |  |  |  |
| Security Check List for QA |  |  | [QA Security Checklist](https://docs.google.com/spreadsheets/d/1LZaorCg0CKPSxfPiheEnLpVJAl3N6PjhxXoA2IFJNDQ/edit?usp=sharing) |
| Security Focus Dev Training |  |  |  |
| Security Best Practices | - | - | [Ruby](https://confluence.freshworks.com/display/freshsales/Security+Best+Practices) |
| Tech Stack | - | - | [Freshsales](https://confluence.freshworks.com/display/freshsales/Secure+Architecture+Deliverables+-+Tech+Stack+Collection) |
| Network Architecture |  |  | [Architecture](https://docs.google.com/document/d/1AfHS2cMBrWi72m9FLGaZXW7qda5OQmzNV3kjlAwMfz8/edit?usp=sharing) |
| External Security Bug Program | - | - | [https://www.freshworks.com/security/responsible-disclosure/](http://Responsible%20Disclosure%20Policy)  <https://hackerone.com/freshworks?type=team> |