401 – Security Solution Expert Notes

**Section 1: Threat Analysis**

|  |
| --- |
| * 1. Analyze external threat research to determine potential impact to an organization |
| * 1. Analyze threat modeling data to determine risk profiles of the infrastructure and applications |

***Threat Research/Threat Modeling***

* F5 Labs <https://www.f5.com/labs>
* OWASP Top 10 <https://owasp.org/www-project-top-ten/>
* <https://support.f5.com/csp/article/K52596282>

**Section 2: Architect Solutions**

|  |
| --- |
| 2.01 Determine the correct solution to mitigate a given threat |
| 2.02 Determine the correct control to address a compliance or business requirement |
| 2.03 Determine the appropriate security framework for an application |
| 2.04 Explain the justification for a proposed solution |
| 2.05 Determine when BIG-IQ is required for centralized management and visibility |

***Security Framework***

* <https://www.f5.com/services/resources/white-papers/f5-big-ip-platform-security>
* <https://www.f5.com/services/resources/white-papers/the-f5-security-for-service-providers-reference-architecture>
* <https://www.f5.com/content/dam/f5/corp/global/pdf/white-papers/big-ip-system-security-wp.pdf>
* <https://www.f5.com/solutions/application-security>
* <https://www.youtube.com/watch?v=qSlLH5Tq9PA>

***BIG-IQ Centralized Management and Visibility***

* <https://www.f5.com/products/automation-and-orchestration/big-iq>
* <https://www.f5.com/pdf/products/big-iq-datasheet.pdf>
* <https://www.youtube.com/watch?v=YZ6dZa512j8>
* <https://www.youtube.com/watch?v=QAPeSOd7O40>
* <https://clouddocs.f5.com/training/community/big-iq-cloud-edition/html/>
* <https://www.f5.com/services/training/free-training-courses/getting-started-with-big-iq-centralized-management>

***Compliance/Business Requirement***

* <https://support.f5.com/csp/article/K51230228>
* <https://www.f5.com/company/policies/export-compliance>
* <https://www.f5.com/pdf/solution-guides/maintaining-governance-risk-and-compliance-and-streamlining-the-audit-process.pdf>

***FIPS***

* <https://support.f5.com/csp/article/K52534643>
* <https://support.f5.com/csp/article/K91841023>
* <https://support.f5.com/csp/article/K49272430>
* <https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-platforms-fips-administration-13-1-0/1.html>
* <https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/f5-platforms-fips-administration-13-0-0/1.html>

**Section 3: Operation and Implementation**

|  |
| --- |
| 3.01 Apply procedural concepts required to configure F5 technology to provide network layer DOS protection |
| 3.02 Determine the appropriate protection against known bad actors |
| 3.03 Determine the appropriate settings to mitigate web fraud |
| 3.04 Articulate architectural requirements for outbound SSL visibility |
| 3.05 Apply procedural concepts to configure network firewall protection |
| 3.06 Troubleshoot F5 technology to address functionality or performance issues |
| 3.07 Verify a configuration is functioning as intended to mitigate a vulnerability |

***AFM***

* <https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/big-ip-afm-getting-started-14-1-0/03.html>
* <https://techdocs.f5.com/en-us/bigip-15-1-0/big-ip-system-dos-protection-and-protocol-firewall-implementations/about-afm-dos-protection.html>
* <https://support.f5.com/csp/article/K49869231>

***ASM***

* <https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/asm-implementations-13-0-0/1.html>
* <https://support.f5.com/csp/article/K29359407>
* <https://www.f5.com/services/resources/white-papers/protecting-against-application-ddos-attacks-with-big-ip-asm-a-three-step-solution>

***IP Intelligence***

* <https://www.f5.com/pdf/products/ip-intelligence-service-ds.pdf>
* <https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-implementations-13-1-0/8.html>
* <https://support.f5.com/csp/article/K13875>
* <https://www.f5.com/services/resources/white-papers/dynamic-perimeter-security-with-ip-intelligence>
* <https://techdocs.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-implementations-12-1-0/7.html>

***WebSafe***

* <https://www.f5.com/pdf/products/websafe-mobilesafe-datasheet.pdf>
* <https://clouddocs.f5.com/training/community/fps/html/class1/module1/module1.html>
* <https://clouddocs.f5.com/training/community/fps/html/class1/class1.html>

***MobileSafe***

* <https://www.f5.com/pdf/products/mobilesafe-datasheet.pdf>
* <https://techdocs.f5.com/en-us/bigip-15-1-0/fraud-protection-service-big-ip-configuration/configuring-a-mobile-security-anti-fraud-profile/overview-configuring-a-mobile-security-anti-fraud-profile.html>

***DataSafe***

* <https://techdocs.f5.com/en-us/bigiq-7-1-0/big-iq-fraud-protection-service/configuring-f5-datasafe-profiles.html>
* <https://techdocs.f5.com/kb/en-us/products/big-ip_asm/manuals/product/bigip-datasafe-configuration-13-1-0/1.html>
* <https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-datasafe-configuration.html>

***Silverline***

* <https://www.f5.com/products/security/silverline>
* <https://www.f5.com/pdf/products/f5-silverline-web-application-firewall-datasheet.pdf>
* <https://www.f5.com/pdf/products/silverline-ddos-datasheet.pdf>

***SSL Orchestrator***

* <https://www.youtube.com/watch?v=GQx5a2bVrTs>
* <https://www.youtube.com/watch?v=AadhUC5FNGs>

**Section 4: Security Response**

|  |
| --- |
| 4.01 Analyze logs or other data sources for security incidents |
| 4.02 Determine the appropriate proactive security response plan |
| 4.03 Determine the appropriate incident response plan given specific attack details |

***ASM Logs***

***AFM Logs***

***BIG-IQ Logs***

***F5 SIRT***

* <https://www.f5.com/content/dam/f5/corp/global/pdf/agility/agility2018/The-F5-SIRT-And-You.pdf>
* <https://devcentral.f5.com/s/articles/introducing-the-f5-security-incident-response-team-sirt-25076>
* <https://www.f5.com/labs/articles/cisotociso/making-the-most-of-a-security-incident>

**Honorable Mentions:**

<https://www.youtube.com/playlist?list=PLzhiuUd6nZKj_-tshSblw4Q3PA-fuQ9Vs>