VERIZON CALNET 3 CATEGORY 7
Table of Contents

7.2.1.4.a DDoS Detection and Mitigation Features

Contractor's Summary description of service: DDoS Detection and Mitigation Features and related unsolicited services

Geographic Availability: Statewide

Service Limitations and Restrictions N/A

Change Charge Applicability: Change Charge Applicability varies by service and feature code. See Column E for change charge applicability.

A	B	C	D	E	F	G	H	I	J	K
Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of measure	Charge per change per item	Delegation Needed (Yes/No)	Required or Discretionary
1	DDoS Detection and Mitigation, 1 – 2 GB	DDSO1002	DDoS Detection and Mitigation Service as described in Section 7.2.1.3 for 1-2 GB of traffic flow.		$ 0	$2,123.80	Per Network	N/A	Yes	Required
2	DDoS Detection and Mitigation, 3 – 4 GB	DDOS3004	DDoS Detection and Mitigation Service as described in Section 7.2.1.3 for 3-4 GB of traffic flow		$ 0	$2,410.80	Per Network	N/A	Yes	Required
3	DDoS Detection and Mitigation, 5 – 6 GB	DDOS5006	DDoS Detection and Mitigation Service as described in Section 7.2.1.3 for 5-6 GB of traffic flow		$ 0	$2,927.40	Per Network	N/A	Yes	Required

7.2.2.3 Email Monitoring and Scanning Service Features

Contractor's Summary description of service: Email Monitoring and Scanning Service Features and related unsolicited services

Geographic Availability: Statewide

Service Limitations and Restrictions N/A

Change Charge Applicability: Change Charge Applicability varies by service and feature code. See Column E for change charge applicability.

A	B	C	D	E	F	G	H	I	J	K
Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of measure	Charge per change per item	Delegation Needed (Yes/No)	Required or Discretionary
1	Email Monitoring and Scanning Service, 1-49	EMLM0049	Email managed security services seat as described in Section 7.2.2.		$ 0	$1.95	Seat	N/A	Yes	Required
2	Email Monitoring and Scanning Service, 50-74	EMLM0074	Email managed security services seat as described in Section 7.2.2.		$ 0	$1.33	Seat	N/A	Yes	Required
3	Email Monitoring and Scanning Service, 75-99	EMLM0099	Email managed security services seat as described in Section 7.2.2.		$ 0	$1.18	Seat	N/A	Yes	Required
4	Email Monitoring and Scanning Service, 100-500	EMLM0500	Email managed security services seat as described in Section 7.2.2.		$ 0	$1.05	Seat	N/A	Yes	Required
5	Email Monitoring and Scanning Service, 501-1000	EMLM1000	Email managed security services seat as described in Section 7.2.2.		$ 0	$0.88	Seat	N/A	Yes	Required
6	Email Monitoring and Scanning Service, 1001 and above	EMLM1001	Email managed security services seat as described in Section 7.2.2.		$ 0	$0.84	Seat	N/A	Yes	Required

7.2.3.2 Web Security and Filtering Service Features

Contractor's Summary description of service: Web Security and Filtering Service Features and related unsolicited services

Geographic Availability: Statewide

Service Limitations and Restrictions N/A

Change Charge Applicability: Change Charge Applicability varies by service and feature code. See applicable service feature code line item description as how this change charge applies by service and feature.

A	B	C	D	E	F	G	H	I	J	K
Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of measure	Charge per change per item	Delegation Needed (Yes/No)	Required or Discretionary
1	Web Security and Filtering Service	WSFS0000	Web Security and Filtering service as described Section 7.2.3.		$ 0	$1.28	Per User	$ 0	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Contractor's Summary description of service: Security Information and Event Management (SIEM) and related unsolicited services

Geographic Availability: Statewide

Service Limitations and Restrictions N/A

Change Charge Applicability: Change Charge Applicability varies by service and feature code. See Column E for change charge applicability.

A	B	C	D	E	F	G	H	I	J	K
Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of measure	Charge per change per item	Delegation Needed (Yes/No)	Required or Discretionary
1	SIEM, 1 – 15 Devices	SIEM0015	SIEM service as described in Section 7.2.4.		$ 0	$1,887.57	Initial Deployment	N/A	Yes	Required
2	Each additional device	SIEA0015	Each additional device above 15.		$ 0	$126.53	Device	N/A	Yes	Required
3	SIEM, 16 - 40 Devices	SIEM0040	SIEM service as described in Section 7.2.4.		$ 0	$5,060.94	Initial Deployment	N/A	Yes	Required
4	Each additional device	SIEA0040	Each additional device above 40.		$ 0	$125.84	Device	N/A	Yes	Required
5	SIEM, 41 - 100 Devices	SIEM0100	SIEM service as described in Section 7.2.4.		$ 0	$12,652.34	Initial Deployment	N/A	Yes	Required
6	Each additional device	SIEA0100	Each additional device above 100.		$ 0	$126.53	Device	N/A	Yes	Required
7	SIEM, 101 – 250 Devices	SIEM0250	SIEM service as described in Section 7.2.4.		$ 0	$31,527.98	Initial Deployment	N/A	Yes	Required
8	Each additional device	SIEA0250	Each additional device above 250.		$ 0	$126.66	Device	N/A	Yes	Required
9	SIEM, 251 - 1000 Devices	SIEM1000	SIEM service as described in Section 7.2.4.		$ 0	$85,276.80	Initial Deployment	N/A	Yes	Required
10	Each additional device	SIEA1000	Each additional device above 1000.		$ 0	$85.19	Device	N/A	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

11	SIEM, 1001 - 2500 Devices	SIEM2500	SIEM service as described in Section 7.2.4.		$ 0	$213,191.99	Initial Deployment	N/A	Yes	Required
12	Each additional device	SIEA2500	Each additional device above 2500.		$ 0	$85.28	Device	N/A	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Verizon Vulnerability Management (VVM) Service is a solution that automates network auditing and vulnerability management across an organization, including network discovery and mapping, asset management, vulnerability reporting and remediation tracking. Driven by our comprehensive KnowledgeBase of known vulnerabilities, VVM Service enables cost-effective protection against vulnerabilities with one scanner appliance deployed in the customer environment. The Verizon's Cloud Platform core scanning technology is inference-based. It begins by creating an accurate inventory of the operating system, protocols, ports and services with an IP Address in the customer environment. This IP Address inventory is then used to developed vulnerability expert system specific to the IP Address, which chooses the appropriate set of vulnerabilities to test based on the IP Address profile. The result is a customized scan of each target. Customer does not need to have an understanding of the systems on the network or obtain specific credentials to perform vulnerability scanning. An example is VVM will only launch applicable modules and specific vulnerability checks on listening applications (i.e. Microsoft 10 will have only Microsoft 10 vulnerability checks attempted, Apache will have only Apache vulnerabilities checks, etc.). Web Application Scanning is an additional layered on service feature outside this base VVM service.

During a Scan, VVM performs a user configurable TCP, UDP, and RPC port scan followed by a set of modules called Service Discovery. Service Discovery takes each port that is identified as open or filtered as part of the port scan modules and intelligently determines the application type, vendor, and version through a combination of banner detection and intelligent active packet/service testing. VVM Cloud Platform is able to more accurately determine IP address inventory of what "service" is actually running on a given port.

Another feature of VVM service is Verizon Payment Card Industry Compliance (PCI) which is included at no additional charge. PCI Compliance (PCI) module provides organizations storing cardholder data a cost-effective and highly automated solution to verify and document compliance with PCI Data Security Standards. The reports PCI Compliance scan produces to the customer provides the tools necessary to support their PCI compliant environment. This provides the customer the ability to use these reports available with the Verizon PCI scanning service to stay current to identify PCI scanning compliance (e.g. PCI Data Security Standards quarterly reviews). Verizon PCI Compliance service is an authorized PCI DSS scanning vendor which can document false positives and provide official quarterly scanning reports. The PCI module supports simple PCI workflow to identify gaps in compliance and allow customers to focus on areas to remediate.

The VVM Cloud Platform has standard template-driven reporting engine enables customers to easily mine scan results in a similar way that a SQL report writer queries a SQL database. Customer has the option for standard reporting or customized reports based on the customer needs and limits of vulnerability scan information collected available on the web based portal interface. Roles based access are available, controlled by the customer, for the flexibility of the access levels required to get reporting information to appropriate personal at no additional charge.

Customer must provide Internet Access for scanner appliance collection and reporting via the web based portal. Verizon will provide unlimited scanning on the number of IP's in the customer's service with this service. Scans are scheduled via the Verizon Portal on demand or recurring scheduled. Ad-hoc scans are also apart of good business practice to follow-up on vulnerable areas discovered to confirm progress and remediation of issues found. The customer will choose the amount of IP Addresses to have the vulnerability scan service. The customer would need to order additional quantities, should they require more IP Address to be scanned. Verizon will pre-configure the scanner appliance based on the customer service. Customer may also purchase add-on cloud scanner for use in Amazon or Microsoft cloud environments. Customer is responsible for the installation of the scanner appliance on their network. Additional customer installation instructions are available at https://www.qualys.com/docs/qualys-scanner-appliance-user-guide.pdf?_ga=1.158192435.887113033.1420830694. Verizon provides on-line training via instructor-led lead net-conferencing for tool and setup of the service. Customer is responsible for all remediation to include: discovering and categorizing assets for VVM, schedule scanning of systems to detect vulnerabilities, Prioritizing assets by business risk, Remediating vulnerabilities through patching software or other methods, Informing the security team, auditors, and management with reports, and continuously repeating these steps for ongoing security.

VVM Customer Care provides the option to obtain support services from Verizon that enable the Customer to optimize their existing VVM service investment and ensure a high level of vulnerability protection.

The Verizon VVM Customer Care package includes:

- Set-up Assistance. Assist in set-up activities for VVM service after customer has provided the necessary information about their current environment such as:
  - Names, responsibilities and contact info of relevant stakeholders
  - Approximate number of IP addresses to be scanned
  - Internal and/or external IP addresses
  - URLs to be scanned
  - List of Application/s to be scanned

In Set-up Assistance, Verizon will, upon request and upon behalf of the customer, set up the VVM service. This activity is essential to providing the basis of providing Vulnerability Reporting for the customer environment.

- Operational Assistance. Verizon will perform duties and responsibilities typically performed by the Customer including:
  - Vulnerability Scanning. Verizon will proactively scan targets for our comprehensive KnowledgeBase of known vulnerabilities in the Customer's environment. Per Customer request, Verizon will review and analyze scan results prior to delivery to Customer. Verizon will regularly perform four distinct types of scanning, each of which can be deployed together or separately:
    - External scanning - Focuses on assets exposed directly to the Internet. External scanning provides an external attacker's view of the Customer network perimeter and highlights the level of risk the Customer is exposed to from attacks from the Internet.
    - Internal scanning - Focuses on the Customer's internal network to find vulnerabilities within the enterprise. This type of scanning is important as large number of attacks exploit weaknesses in the internal hosts once they gain a foothold in the network.
    - Authenticated scans - Verizon will utilize login credentials to the assets themselves to run host-level checks on the targets. This form of scanning produces the most meaningful results, as it can find issues such as weak passwords, missing patches or configuration weaknesses in addition to software vulnerabilities.
    - Policy Scanning Module – If the Customer elects to purchase the optional Verizon Policy Compliance (VPC), Verizon will provide operational assistance and system management support to enable Customer to utilize this policy scanning module. The primary purpose of this Care module is for Verizon to map VPC to the required security standard the Customer wishes to apply. Verizon can analyze device configurations, web application and access control information from Customer networked devices (IP Address) based on the VVM scan. Verizon will work with the Customer to use VPC as a means to provide proof of compliance demanded by auditors across multiple compliance initiatives. In addition, Verizon will support Customer efforts to remediate the compliance gaps and modify/refine policy.
    - Web application scanning - Verizon will search for typical vulnerabilities in web applications that can be exploited by attackers. This form of scanning is especially useful for Internet-facing web applications, which are typically constantly under attacks. (Note: this type of scan is offered only when the Verizon Web Application Scanning module is purchased.)

Verizon will analyze the vulnerabilities reported by the scanner and interpret and prioritize based on factors such as the severity, availability of exploit code, and business criticality of the affected asset.

- Scanning recurrence (Frequency) – Verizon will work with Customer to develop and execute an appropriate scan schedule.
- Monitor compliancy requirements. Verizon will monitor Customer's adherence to applicable compliance requirements and assist with compliance adherence planning.
- Vulnerability remediation and patch management - Verizon will oversee the vulnerability/patch management process, assign vulnerabilities to the designated asset owners for remediation, and communicate recommended remediation steps. Verizon's guidance will adhere to three primary methods of remediation:
  - Patching: Apply a security patch or software update from the vendor to repair the vulnerability.
  - Configuration adjustment: Adjust the configuration of the software to remove the vulnerability, such as changing passwords, modify permissions or change firewall rules.
  - Software removal: Removing and uninstalling the vulnerable software to eliminate the vulnerability and the associated risk.

Once the asset owners report that the vulnerability has been remediated across the environment, Verizon will conduct a specific verification scan to ensure that the chosen remediation method has been efficiently implemented and all attack vectors for a given vulnerability have been successfully eliminated.

- Monitoring and reporting – In addition to scanning for vulnerabilities, Verizon Customer Care staff will monitor the asset database and associated criticality of data to ensure the tracking process is providing current and accurate information. Verizon will provide the Customer a regular vulnerability report highlighting the current threats the Customer is exposed to by leveraging resources using the VVM tool service.
- Network documentation management – Verizon will develop and update Network Layout descriptions on a periodic, as needed basis.
- Continuous Improvement and Knowledge Transfer. Verizon will continuously improve the service based on feedback from the Customer, the results of the vulnerability scans and the feedback from Key Performance Indicators monitoring. The improvements may include changes in the processes or practices, or modification in the scanning infrastructure or configuration. Verizon will continually work with the Customer to build the body of knowledge so that the Customer can achieve self-sufficiency when desired.

Verizon VVM Customer Care will also apply to the other modules (such as Verizon Policy Compliance Service and Verizon Web Application Scanning) should they be purchased as add on options to VVM service.

7.2.4.2 Security Information and Event Management (SIEM)

A	B	C	D	E	F	G	H	I	J	K
Line item #	Feature Name	Contractor's Product Identifier	Feature Description	Feature Restrictions, Limitations and Additional Information	Non-Recurring Charge per item	Monthly Recurring Charge/item per unit	Unit of measure	Charge per change per item	Delegation Needed (Yes/No)	Required or Discretionary
13	Vulnerability Management ≤ 256 IP's	VVMS0256	Provide Vulnerability Management Scanning up to 256 IP's as described above		N/A	$554.78	Scan Up to 256 IP's	N/A	Yes	Required
14	Vulnerability Management ≤ 512 IP's	VVMS0512	Provide Vulnerability Management Scanning up to 512 IP's as described above		N/A	$682.92	Scan Up to 512 IP's	N/A	Yes	Required
15	Vulnerability Management ≤ 1,024 IP's	VVMS1024	Provide Vulnerability Management Scanning up to 1,024 IP's as described above		N/A	$1,109.98	Scan Up to 1,024 IP's	N/A	Yes	Required
16	Vulnerability Management ≤ 1,536 IP's	VVMS1536	Provide Vulnerability Management Scanning up to 1,536 IP's as described above		N/A	$1,707.91	Scan Up to 1,536 IP's	N/A	Yes	Required
17	Vulnerability Management ≤ 2,048 IP's	VVMS2048	Provide Vulnerability Management Scanning up to 2,048 IP's as described above		N/A	$1,878.73	Scan Up to 2,048 IP	N/A	Yes	Required
18	Vulnerability Management ≤ 3,072 IP's	VVMS3072	Provide Vulnerability Management Scanning up to 3,072 IP's as described above		N/A	$2,049.57	Scan Up to 3,072 IP's	N/A	Yes	Required
19	Vulnerability Management ≤ 10,000 IP's	VVMG0000	Provide Vulnerability Management Scanning up to 10,000 IP's as described above		N/A	$11,104.16	Scan Up to 10,000 IP's	N/A	Yes	Required
20	Scanner Appliance Installation	VSAN0000	Scanner Appliance Installation provides the customer to have the option for Verizon to install the scanner appliance in the customer environment. This Scanner Appliance service installation option is available for the VVM service or Additional Scanner Appliance. VVM Service and Additional Scanner Appliance have pre-configured scanner appliance shipped where the customer is responsible for installation into their premise environment.		$3,000.00	N/A	Per Appliance	N/A	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

21	Additional Scanner Appliance	VASA0000	Additional Scanner Appliance provides the customer to have the option for an additional scanning appliance deployed in the customer environment. Benefits to additional scanners include reducing scan times by keeping the scanner appliance close to the assets, load sharing, and redundancy for customer internal, non-internet facing assets. Customer is responsible for the installation of the scanner appliance on their network.		N/A	$213.12	Per Scanner	N/A	Yes	Required
22	Cloud Scanner Appliance	VASA0001	Cloud Scanner Appliance provides the customer the option of scanning their Amazon Elastic Compute Cloud or Microsoft Cloud environment. Benefit to additional cloud scanners include reaching elastic cloud environments that could not be reached from the customer's enterprise network. Scanner Appliance Installation (VSAN0000) can be used should customer require assistance with installation of the Cloud Scanner Appliance on Amazon or Microsoft network.		N/A	$213.12	Per Scanner	N/A	Yes	Required
23	Vulnerability Management Customer Care ≤ 512 IP's	VMCC0512	Vulnerability Management Customer Care to include up to 512 IP's as described above. Monthly efforts not to exceed 44 hours of activities.	VVM Customer Care can only be ordered with VVM Service and not ordered as a standalone service.	N/A	$6,945.40	Up to 512 IP's	N/A	Yes	Required
24	Vulnerability Management Customer Care ≤ 1,536 IP's	VMCC1536	Vulnerability Management Customer Care to include up to 1,536 IP's as described above. Monthly efforts not exceed 88 hours of activities.	VVM Customer Care can only be ordered with VVM Service and not ordered as a standalone service.	N/A	$13,890.80	Up to 1,536 IP's	N/A	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

25	Vulnerability Management Customer Care ≤ 3,072 IP's	VMCC3072	Vulnerability Management Customer Care to include up to 3,072 IP's as described above. Monthly efforts not exceed 132 hours of activities.	VVM Customer Care can only be ordered with VVM Service and not ordered as a standalone service.	N/A	$20,836.20	Up to 3,072 IP's	N/A	Yes	Required
26	Vulnerability Management Customer Care ≤ 10,000 IP's	VVMR0002	Vulnerability Management Customer Care to include up to 10,000 IP's as described above. Monthly efforts not exceed 176 hours of activities.	VVM Customer Care can only be ordered with VVM Service and not ordered as a standalone service.	N/A	$27,781.60	Up to 10,000 IP's	N/A	Yes	Required

Verizon Security Policy Compliance (VSPC) Service is a layer on service to Verizon Vulnerability Management (VVM). VSPC enables organizations to analyze device configurations, web application and access control information from their networked devices (IP Address) based on the VVM scan. VSPC provides an organization to reduce the risk of internal and external threats, while at the same time provide proof of compliance demanded by auditors across multiple compliance initiatives. VSPC provides an efficient and automated workflow that allows IT security and compliance professionals to include:

- Define policies that describe how an organization will provide security and integrity
- Provide proof that the policies have been operationalized
- Give documented evidence that the organization has discovered and fixed any security policy compliance lapses

VSPC automatically maps this information to customer's internal security policies and external regulations in order to document compliance. VSPC provides the ability to report on current compliant status and remediate the compliance gaps via the Verizon Portal. VSPC provides compliance posture with internal security and regulatory policies to include:

- Reported in understandable format, easily accessible by business stakeholders
- Workflow and exception management allows organizations to easily produce compliance reports for internal configuration and regulatory requirements
- Security Policy Controls are mapped back to common framework templates for standards such as CIS, COBIT, FFIEC, HIPAA, ISO 17799, ISO 27001, ITIL, NERC, and NIST 800-53

VSPC is available on the Verizon Portal for customer reporting. Customer selects the number of IP's to enroll into VSPC subscription (a subset of the IP subscription for VVM). A standard template is then selected for the VSPC Library, or a custom template can be built to reflect customer own standards. The VSPC module utilized the latest VVM detailed inventory database to report on level of compliance using the standard or customized templates available on the Verizon Portal. The VSPC reporting system will provide reports from very detailed to high level executive views of compliances status to support a range of decisions from remediation to boardroom planning. Roles based access are available, controlled by the customer, for the flexibility of the access levels required to get reporting information to appropriate personal at no additional charge. Verizon provides on-line training via instructor lead net conferencing.

27	Verizon Policy Compliance (VPC) ≤ 32 IP's	VPCS0032	Provide Verizon Policy Compliance Scanning up to 32 IP's as described above.		N/A	$170.41	Scan up to 32 IP's	N/A	Yes	Required
28	Verizon Policy Compliance (VPC) ≤ 64 IP's	VPCS0064	Provide Verizon Policy Compliance Scanning up to 64 IP's as described above.		N/A	$213.12	Scan up to 64 IP's	N/A	Yes	Required
29	Verizon Policy Compliance (VPC) ≤ 128 IP's	VPCS0128	Provide Verizon Policy Compliance Scanning up to 128 IP's as described above.		N/A	$341.24	Scan up to 128 IP's	N/A	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

30	Verizon Policy Compliance (VPC) ≤ 256 IP's	VPCS0256	Provide Verizon Policy Compliance Scanning up to 256 IP's as described above.		N/A	$682.91	Scan up to 256 IP's	N/A	Yes	Required
31	Verizon Policy Compliance (VPC) ≤ 1,024 IP's	VPCS1024	Provide Verizon Policy Compliance Scanning up to 1,024 IP's as described above.		N/A	$1,366.24	Scan up to 1,024 IP's	N/A	Yes	Required
32	Verizon Policy Compliance (VPC) ≤ 2,048 IP's	VPCS2048	Provide Verizon Policy Compliance Scanning up to 2,048 IP's as described above.		N/A	$1,707.91	Scan up to 2,048 IP's	N/A	Yes	Required
33	Verizon Policy Compliance (VPC) ≤ 3,072 IP's	VPCS3072	Provide Verizon Policy Compliance Scanning up to 3,072 IP's as described above.		N/A	$2,305.82	Scan up to 3,072 IP's	N/A	Yes	Required

Verizon Web Application Scanning (VWAS)
Verizon Web Application Scanning (VWAS) is a layer on service to Verizon Vulnerability Management (VVM). VWAS allow organizations to discover, catalog and scan any and all of an organization's web applications. VWAS scans and analyzes custom web applications and identifies vulnerabilities that threaten underlying databases or bypass application access controls. It utilizes behavioral and static analysis to detect malware and monitor web sites that can be scheduled on the Verizon Portal with unlimited monthly scans.

VWAS Service is available on the Verizon Portal for customer reporting. Customer defines the Uniform Resource Identifiers (URL) target(s) to enroll into Web Application Scanning subscription portal. The web application scanning module identifies on vulnerabilities via the Verizon Portal to include these methods:

- Crawl web applications (Intranet, Internet)
- Fully interactive User Interface with flexible workflows and reporting
- Identify web applications' handling of sensitive or secret data
- Customize: black/white lists, robots.txt, sitemap.xml and more
- Supports these authentication schemes to include Basic, Digest, HTTP Negotiate, HTML Form-based, Single Sign On, and Client SSL Certificates
- View reports with recommended security coding practice and configuration
- Supports scanning HTML web applications with JavaScript and embedded Flash
- Comprehensive detection of custom web application vulnerabilities including Open Web Application Security Project (OWASP) Top 10 Vulnerabilities
- Differentiates exploitable fault-injection problems from simple information disclosure - Profiles custom web application behaviors
- Configures scanning performance with customizable performance level

VWAS Service excludes: Manual application code review and Manual penetration testing.

Verizon provides on-line training via instructor lead net conferencing.

34	Verizon Web Application Scanning (VWAS) 1 URL	VWAS0001	Provide Verizon Web Application Scanning for 1 Uniform Resource Identifier (URL) as described above.		N/A	$170.41	1 URL	N/A	Yes	Required
35	Verizon Web Application Scanning (VWAS) ≤ 5 URL's	VWAS0005	Provide Verizon Web Application Scanning up to 5 Uniform Resource Identifier (URL) as described above.		N/A	$298.53	5 URL's	N/A	Yes	Required
36	Verizon Web Application Scanning (VWAS) ≤ 10 URL's	VWAS0010	Provide Verizon Web Application Scanning up to 10 Uniform Resource Identifier (URL) as described above.		N/A	$426.66	10 URL's	N/A	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

37	Verizon Web Application Scanning (VWAS) ≤ 25 URL's	VWAS0025	Provide Verizon Web Application Scanning up to 25 Uniform Resource Identifier (URL) as described above.		N/A	$853.73	25 URL's	N/A	Yes	Required
38	Verizon Web Application Scanning (VWAS) ≤ 50 URL's	VWAS0050	Provide Verizon Web Application Scanning up to 50 Uniform Resource Identifier (URL) as described above.		N/A	$1,494.37	50 URL's	N/A	Yes	Required
39	Verizon Web Application Scanning (VWAS) ≤ 100 URL's	VWAS0100	Provide Verizon Web Application Scanning up to 100 Uniform Resource Identifier (URL) as described above.		N/A	$2,562.07	100 URL's	N/A	Yes	Required
Pre-Implementation:										
40	Network Security Consultant I	NTSC0001	Pre-implementation site survey and network security design. Provides basic consulting skills to include planning, standards based data protection assessments, design, integration, development, configuration for non-complex pre-implementation activities. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Site Survey – Facility site survey required for successful design and implementation. Network Security – Consulting for planning, standards based data protection assessments, design, integration, development, configuration Services supporting network security.	$153.00	$0.00	Per Hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

41	Network Security Consultant II	NTSC0002	Pre-implementation site survey and network security design. Provides advanced consulting skills to include planning, standards based data protection assessments, design, integration, development, configuration for non-complex pre-implementation activities. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Site Survey – Facility site survey required for successful design and implementation. Network Security – Consulting for planning, standards based data protection assessments, design, integration, development, configuration Services supporting network security.	$200.00	$0.00	Per Hour	$0.00	Yes	Required
42	Senior Network Security Consultant	NTSS0000	Pre-implementation site survey and network security design. Provides advanced consulting skills across multiple disciplines. Conducts assessments and design for complex installations involving multiple technologies. Provides advanced consulting skills to include planning, standards based data protection assessments, design, integration, development, configuration for complex pre-implementation activities involving multiple technologies. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Site Survey – Facility site survey required for successful design and implementation. Network Security – Consulting for planning, standards based data protection assessments, design, integration, development, configuration Services supporting network security.	$245.00	$0.00	Per Hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

43	Principal Network Security Architect	NSPA0000	Pre-implementation site survey and network security design. Provides highly advanced consulting skills across multiple disciplines. Conducts assessments and design for complex installations involving multiple technologies. Provides advanced consulting skills to include planning, standards based data protection assessments, design, integration, development, configuration for complex pre-implementation activities involving multiple technologies. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Site Survey – Facility site survey required for successful design and implementation. Network Security – Consulting for planning, standards based data protection assessments, design, integration, development, configuration Services supporting network security.	$295.00	$0.00	Per Hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

Implementation:										
44	Network Security Consultant I *(normal business hours, Mon-Fri, 8am-5pm)*	NSCN0001	Implementation network security consultant performs basic on-site installation, assessments and tests interoperability with other products. During normal business hours, Mon – Fri 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Implementation professional service combines a well-trained, well-equipped integration team with a highly skilled support organization to seamlessly install, provide network integration and performs recurring standards based assessments to the customer environment. VZ engineers have extensive experience with numerous technologies, environments, product interoperability testing and manufacturers' equipment to perform installation activities.	$153.00	$0.00	Per Hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

45	Network Security Consultant I *(outside normal business hours, Sat/Sun)*	NSCO0001	Implementation network security consultant performs basic on-site installation, assessments and tests interoperability with other products. During outside of normal business hours, Sat, Sun & Holidays. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Implementation professional service combines a well-trained, well-equipped integration team with a highly skilled support organization to seamlessly install, provide network integration and performs recurring standards based assessments to the customer environment. VZ engineers have extensive experience with numerous technologies, environments, product interoperability testing and manufacturers' equipment to perform installation activities.	$229.00	$0.00	Per Hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

46	Network Security Consultant II *(normal business hours, Mon-Fri, 8am-5pm)*	NSCN0002	Implementation network security consultant performs advanced on-site installation, assessments and tests interoperability with other products. During normal business hours, Mon – Fri, 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Implementation professional service combines a well-trained, well-equipped integration team with a highly skilled support organization to seamlessly install, provide network integration and performs recurring standards based assessments to the customer environment. VZ engineers have extensive experience with numerous technologies, environments, product interoperability testing and manufacturers' equipment to perform installation activities.	$200.00	$0.00	Per Hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

47	Network Security Consultant II *(outside normal business hours, Sat/Sun)*	NSCO0002	Implementation network security consultant performs advanced on-site installation, assessments and tests interoperability with other products. During outside of normal business hours, Sat, Sun & Holidays. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Implementation professional service combines a well-trained, well-equipped integration team with a highly skilled support organization to seamlessly install, provide network integration and performs recurring standards based assessments to the customer environment. VZ engineers have extensive experience with numerous technologies, environments, product interoperability testing and manufacturers' equipment to perform installation activities.	$305.00	$0.00	Per Hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

48	Network Security Project Manager *(normal business hours, Mon-Fri, 8am-5pm)*	NSPN0001	Network Security implementation project manager coordinates project resources including customer staff and other VZ resources. The project manager defines the project responsibility assignments. During normal business hours, Mon – Fri 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Project management for complex network security solutions. Project Management includes the statement of work, master schedule and site schedules, project acceptance criteria, and other key deliverables that support the customer overall plan. VZ project managers define the project responsibility assignments for successful project implementation.	$153.00	$0.00	Per Hour	$0.00	Yes	Required

7.2.4.2 Security Information and Event Management (SIEM)

49	Network Security Project Manager *(outside normal business hours, Sat/Sun)*	NSPO0001	Network Security implementation project manager coordinates project resources including customer staff and other VZ resources. The project manager defines the project responsibility assignments. During outside of normal business hours, Sat, Sun and Holidays. Only to be sold in conjunction with the support of services specifically listed in Category 7.	Project management for complex network security solutions. Project Management includes the statement of work, master schedule and site schedules, project acceptance criteria, and other key deliverables that support the customer overall plan. VZ project managers define the project responsibility assignments for successful project implementation.	$229.00	$0.00	Per Hour	$0.00	Yes	Required