SECURE COMMUNITY NETWORK

Request for Proposal

Managed Security Services

DUE DATE 28 Sep 2020

Table of Contents

1 Introduction and Overview

1.1 General

Secure Community Network (SCN) issues this Request for Proposal (RFP) for a Managed Security Services Provider to deliver services consisting of but not limited to:

- Managed Security Services. Provide real-time threat monitoring and alerting, analysis and actionable remediation recommendations to assist SCN in managing and securing its network operations, to include:
    - 24x7x365 Threat Monitoring & Alerting
    - Threat Intelligence
    - Vulnerability Management
    - Behavioral Detection & Analysis
- Proactive Security Services. Chief Information Security Officer-like services to guide, assess and test SCN's people, processes and technologies to ensure the confidentiality, integrity and availability of its data and information systems, such as:
    - Information Security Program Development & Governance
    - Cyber Posture Maturity Assessments
    - Risk & Business Impact Assessments
    - Regulatory & Privacy Compliance Readiness
    - Penetration & Vulnerability Testing
    - Cybersecurity Training
- Reactive Security Services. Response to and management of cyber events to determine what, when and how an event occurred, and recommend immediate actions to prevent further impact while recovering quickly, such as:
    - Cyber Incident Response
    - Forensic Investigations
    - Litigation Advisory & Expert Witness
    - Historical Breach Analysis
    - Ability to work directly with SCN's IT MSP during incident response & recovery

All of the above will hereafter collectively be referred to as the "Solution." "Proposal" shall mean the Vendor's bid to provide the services in response to this RFP. "Vendor" shall mean a recipient of this RFP who submits a proposal to SCN and includes any subcontractors to be used by the Vendor to provide the solution. "Agreement" shall mean the agreement that SCN executes with the awarded Vendor for the services hereunder.

SCN issues this request for a Managed Security Services Provider with the intent of having a third party monitor the SCN network for attempted breaches or potential threats.

The approach to the response to this RFP Solution must be agreed to and approved by the parties prior to the start of the engagement.

1.2 Confidentiality of Secure Community Network Information

This RFP, and all information provided to the Vendor in connection herewith, is SCN's confidential and proprietary information (the "Information"). The Vendor may not disclose this RFP, or any Information that SCN may provide the Vendor to assist the Vendor in developing a Proposal, to any other person or entity without the prior written approval of SCN. The submitted Proposal, and all information provided by the Vendor in connection hereunder, is Vendor's confidential and proprietary information (the "Information"). SCN may not disclose the Proposal, or any other Information that Vendor may provide to SCN regarding the Proposal, to any other person or entity without the prior written approval of Vendor. The parties may use the Information provided to it solely for the purpose of responding to and evaluating the response to this RFP. Neither party may disclose to any third party or person that it has received this RFP, the substance of this RFP, the response to the RFP or any SCN decision with respect to the Vendor's Proposal. Upon request, the parties shall return any Information provided by a party, and any copies thereof to such requesting party.

1.3 News Releases

Vendors who are submitting a proposal are not at liberty to discuss this RFP outside the SCN community. Neither party shall release the details of this RFP or subsequent contract without written permission from SCN.

1.4 No Contractual Relationship

Nothing contained in this RFP creates, nor shall be construed to create, any contractual relationship between SCN and any Vendor. SCN makes no commitment in or by virtue of this RFP to purchase any services from any Vendor, nor does receipt of any Vendor's Proposal place SCN under obligation to award the Agreement to that or any other Vendor. Such commitments may be made only in and through a written Agreement signed by both parties.

1.5 Primary Contract Relationship

SCN will contract with the Vendor of the winning proposal and Vendor will be known as the primary contractor. In the event of a subcontracting relationship, which has been approved by SCN and is being used by the primary contractor, the primary contractor assumes all responsibility for delivery, installation, maintenance, and support services that are supplied by the subcontractor.

1.6 Proposal Costs

Expenses incurred in preparing and presenting a Proposal is the sole responsibility of the Vendor and may not be charged to SCN in any way.

1.7 Evaluation of Proposals

The evaluation of all Proposals will be based on a single submission by each individual Vendor. This submission may include multiple alternative approaches for consideration by SCN provided that they meet the requirements of this RFP. No revisions or amendments to the proposal will be accepted after submission unless approved by SCN.

Once SCN has evaluated the submitted proposals, the preferred vendor will be contacted and requested to do a presentation of their solution for SCN executive management at its headquarters in Chicago, IL., or via videoconference. The preferred vendor will then be requested to deploy their solution to SCN for a no-cost trial period of 30 days for final evaluation in real-world conditions.

SCN will use some or all of the following criteria to evaluate Proposals (the order does not represent priority):

- The Vendor's ability to provide reliable services
- The Vendor's ability and willingness to aid in configuring the Solution to meet SCN's needs
- The services features and ability to support business and technical requirements

- The ability to integrate third-party software products and or services
- The level of complexity of the Solution
- The overall quality and presentation of the Proposal
- The price of the Solution
- The overall business case impact
- Any third-party evaluations of the vendor's services
- Industry standing and expertise

1.8 Basis for Award of Agreement

SCN reserves the right in its sole discretion and for any reason whatsoever, to accept, reject or terminate consideration at any time of any or all Proposals. SCN specifically reserves the right to contract with a Vendor that does not offer the services at the lowest price or with one or more companies that did not submit a Proposal and to modify the terms of the projected transaction or the specifications of the services at any time prior to execution of the Agreement.

1.9 Amendments to RFP

SCN reserves the right to amend, modify, or withdraw this RFP at any time. If the RFP is amended or modified, it will be in writing from SCN. Vendors are required to acknowledge all amendments in writing.

1.10 RFP Schedule

The schedule for this RFP is as follows:

RFP Issued:	08 Sep 2020
Vendor's Intention to Bid by:	11 Sep 2020
Last Date to submit questions:	16 Sep 2020
Answers provided by:	21 Sep 2020
Proposal Submission:	28 Sep 2020
Target for SCN Decision:	09 Oct 2020
Solution Implementation:	16 Nov 2020

1.11 Vendor Questions

Vendors should submit all questions about this RFP **in writing** by the date specified above to:

Primary Contact: Matthew Siegel, Operations Center Coordinator

msiegel@securecommunitynetwork.org

Backup Contact: Robert Graves, Regional Security Advisor

rgraves@securecommunitynetwork.org

It is SCN's intent to provide responses to questions to all Vendors where appropriate.

1.12 Acknowledgment of RFP Receipt

Within two business days of the receipt of this RFP Vendors must provide written or electronic acknowledgment of the receipt of this Request for Proposal and intention to respond. This communication should be addressed to the attention of the Primary Contact at the address noted above.

1.13 Election Not to Submit Proposal

In the event the Vendor elects not to proceed with submission of a Proposal to SCN, a letter denoting such intention should be sent to the Primary Contact at the above address. SCN would like to request that the Vendor provide rationale for the decision not to respond.

1.14 Proposal Submission

One (1) electronic copy of the Proposal must be delivered no later than 5 p.m. Eastern Daylight Time, to the Primary Contact listed at the above address on the "Proposal Submission:" date in the RFP schedule above.

Proposals should be in Microsoft Word or PDF. The Vendor's name should appear on the bottom of every page other than the cover page. Each page, other than the cover page, shall be numbered.

SCN reserves the right to reject Proposals received after the due date. Each Proposal shall constitute an offer, which remains valid for a minimum period of 90 days after the proposal submission date.

1.15 Form of Service Agreement

Vendor should submit a copy of their standard agreement form. When SCN completes its analysis and selects a Vendor, SCN will provide an agreement for execution by the successful Vendor. The Vendor must state its fee structure based on the contents of the RFP.

2 SCN's Current Business Environment

2.1 SCN Overview

The Secure Community Network (SCN), a nonprofit 501(c)(3), is the official safety and security organization of the Jewish community in North America. Founded in 2004 under the auspices of The Jewish Federations of North America and the Conference of Presidents of Major American Jewish Organizations, SCN works on behalf of 146 federations, the 50 largest Jewish nonprofit organizations in North America and over 300 independent communities as well as with other partners in the public, private, nonprofit and academic sectors to ensure the safety, security and resiliency of the Jewish people. SCN serves as the Jewish community's formal liaison with federal law enforcement and coordinates closely with federal, state and local law enforcement partners on safety and security issues related to the Jewish community. SCN is dedicated to ensuring that Jewish organizations and communities, as well as life and culture, can not only exist safely and securely, but also flourish.

SCN's team of law enforcement, homeland security and military professionals proactively works with communities and partners across North America to develop and implement strategic frameworks that enhance the safety and security of the Jewish people. This includes developing best practice policies, emergency plans and procedures; undertaking threat and vulnerability assessments of facilities; providing critical, real-world training and exercises to prepare for threats and hazards; offering consultation on safety and security matters; and providing response as well as crisis management support during critical incidents. Through its Operations Center and Duty Desk, SCN analyzes intelligence and information, providing timely, credible threat and incident information to both law enforcement and community partners.

SCN also partners with select entities to provide co-branded security services to its partner organizations in the Jewish community. SCN may seek such a partnership with the selected vendor.

The purpose of this request for proposal is to help SCN identify technical solutions available to meet its business needs for protecting proprietary data and systems from unauthorized access. It is soliciting input from a select group of vendors to present their design for a comprehensive solution to ensure the confidentiality, integrity and availability of SCN data.

This document includes a profile of the current environment, from a business perspective as well as a technical point of view and includes detailed information. High-level business requirements have been defined, indicating the immediate focus for this initiative as well as the long-term strategy.

2.2 SCN Organization and Structure

SCN operates as distributed organization. Its headquarters is located in Chicago, IL, and consists of executive management and leadership staff, the Operations Center, and Duty Desk. The Chicago staff currently consists of 12 persons, working principally from network connected devices and occasionally working remotely from SCN-owned devices or from personal devices (e.g. smartphones). The headquarters staff is anticipated to continue to grow over the next 12 – 24 months.

SCN's operational staff works from remote locations around the country. Some are embedded in partner organizations and connect to SCN systems via the partner's devices and network, while others work from stand-alone sites and connect from SCN-owned devices. All operational staff routinely connect to SCN's Microsoft Office365 cloud server remotely from SCN-owned devices and personal devices (e.g. smartphones). At this time, remote staff do not directly connect to the primary network at the Chicago, IL headquarters. The operational staff is currently 18 persons and is anticipated to continue to grow over the next 12 – 24 months.

2.3 Business Requirements

As part of SCN security best practices, it has been deemed vital for SCN to implement, maintain and monitor appropriate security measures. This is to:

- Provide protection for our internet-facing applications and client services
- Prevent any internal damage to our network from the outside
- Set a best practice standard for Cybersecurity in the Jewish community

This should encompass a 24x7x365 service that:

- Positively identifies security incidents based on log information from sources including, but not limited to, firewalls, Intrusion Detection/Prevention systems, Active Directory servers and domain controllers, DNS, endpoint anti-malware, and cloud-based web proxy
- Proactively alerts on potential attacks using appropriate threat intelligence resources and techniques with recommendations for measures to implement in order to prevent potential attacks
- Performs triage of events and reporting of incidents for further investigation

Services should include development and administration of an organizational information Security program and standards aligned with industry best practices to proactively to identify, manage, and avoid risks. Additionally, SCN and/or Vendor must be able to identify and declare an incident and the Vendor must provide incident response support to enable SCN to be able to conduct its business. These services will enhance our security posture and reduce our risk of a security breach.

3 SCN's Current Technical Environment

The following information is provided to give Vendor information concerning SCN's technical environment, for the purposes of submitting a Proposal for the services requested:

Security Monitoring – Security Technology

Type	HA or SA[1]	Performance	No. of hosts
NG Firewalls	SA	Small/Medium/Large[2]	1

3.1 Security Monitoring - Infrastructure

Type	Criticality[3]	Platform	No. of hosts
Windows endpoints	–	–	2
Mac endpoints	–	–	28

3.2 Cloud Monitoring

Type	Nr.
Office 365 users	40 users

[1] High Available (cluster of 2 nodes) or Stand Alone.
[2] Small: < 4Gbps throughput, Medium: 4-10 Gbps, Large >10 Gbps
[3] Providing critical security logs. High: like Active Directory, Proxy. DHCP, Proxy, AV etc. Low: the rest.

4 Response Format

SCN requires Vendor to organize its Proposal in the following order:

- **Executive Summary:** Provide an overview of the solution, including differentiators and value provided by the solution. Vendors should limit the Executive Summary to a maximum of three pages.
- **Responses to Questions:** Provide concise responses to the Questions listed in the following sections, presented in the exact order as arranged in this document. Vendor must follow numbering sequence, use the same section titles and answer all questions in order for Vendor Proposal to be considered.
- **Pricing:** Provide detailed pricing for the proposed solution.
- **Supplemental Information:** Any information that Vendor deems relevant to the proposed solution can be included as an Appendix. Please note: Do not include information unless it directly relates to the solution proposed in Vendor Proposal.

Vendor Proposals must adhere to the above-stated format in order to be considered.

5 Vendor Profile

5.1 Primary Business Purpose

5.1.1 Please provide a brief statement of your organization's primary business purpose.

5.2 Corporate History

5.2.1 Please provide a brief history of your company, to include details of ownership.

5.3 Management Team

5.3.1 Please provide brief biographies of your management team.

5.4 Services Offered

5.4.1 Are you willing to co-brand your solution with SCN to create a mutually beneficial agreement for SCN to provide your solution to its partner organizations? Please describe similar arrangements you have made with customers in the past.

5.4.2 Describe the services offered by your organization, including any optional services that might be of interest to SCN.

6 Business Attributes

Business attributes are one element of SCN's requirements. They comprise characteristics, policies, processes and procedures that need to be described in a qualified RFP response and include:

- **Financial Viability**
- **Managed Service Viability**
- **Security Vision and Investment**
- **Security Practices**

6.1 Financial Viability

6.1.1 **Provide information about your company's financial stability. If your company is public, include an annual report and supporting financial statements. If your company is private, include supporting documentation to demonstrate a stable, profitable, sustainable business model.**

6.1.2 **Provide detail on any venture funding you have received, including the sources of the venture funding.**

6.2 Managed Service Viability

6.2.1 **What is your company's core business strategy? What are your primary lines of business in terms of revenue? Where do security services fit into your business strategy?**

6.2.2 **Describe any recent industry analysis (e.g., Gartner, Forrester) and awards your company has won.**

6.2.3 **Describe any industry-relevant certifications your company holds (e.g., SOC1, SOC2).**

6.2.4 **Identify your top three competitors in the Managed Security Services sector and identify what differentiates you from each.**

6.2.5 **Provide the number of Managed Security Services clients at the end of last year, current, and projected at the end of this year. Only include clients for Device Management, Security Monitoring, SIEM, Log Management and Vulnerability Scanning services.**

6.2.6 **Identify three references from among your current clients and provide contact information for each. (SCN will execute appropriate NDAs before receiving client information.)**

6.2.7 **Provide details on how long you have offered each of your Managed Security Services.**

6.2.8 **Describe your most recent fiscal year's Managed Security Services growth rate over the prior fiscal year.**

6.3 Security Vision and Investment

6.3.1 **Describe your company's vision and direction for developing new technologies in support of your Managed Security Services.**

6.3.2 **Describe, in detail, your company's investment approach to technology research and development as it relates to solving security challenges and improving client ROI.**

6.3.3 **Provide details on your level of investment in research and development.**

6.3.4 **Provide examples of innovation and enhancements to your service architecture and/or service offerings.**

6.4 Security Practices

6.4.1 Provide detail on your internal security policy and procedures, documenting any industry standards (ISO 17799, CobiT, etc) that you have adopted or follow.

6.4.2 Have you had an independent review of your MSSP infrastructure and service (ISO compliance review, SAS 70 review)? If so, please provide details. If not, describe your plans to have a review performed in the future.

6.4.3 Do you perform internal reviews over your MSSP infrastructure and service? If so, please provide details. If not, would you grant us the right (or a third party on our behalf) to audit your operations and determine the appropriateness of implemented safeguards?

6.4.4 Describe your business continuity/disaster recovery policy.

6.5 MSS Infrastructure

6.5.1 Do you maintain full, dedicated Security Operation Centers (SOCs) to support your MSS services?

6.5.2 Describe your SOCs, including details on the following points:

- Do you own and manage your SOCs?
- Where are your primary SOCs located?
- Where are your secondary SOCs located?
- Are all of your SOCs operational 24x7x365?

6.5.3 Describe how you limit service interruption if a SOC goes offline.

6.5.4 Describe security safeguards around the SOCs.

6.5.5 Do you permit an onsite SOC visit? If so, what is the process for planning the visit?

6.5.6 What percentage of your staff is directly involved with delivering MSS services and managing MSS client accounts?

6.5.7 Describe your company's annual staff retention rate for positions used to support the SCN account.

6.5.8 Identify the number of employees versus contractors.

6.5.9 Describe your company's staffing approach. What are your classifications for support (Example: Level 1, Level 2, etc.) Clearly define each level of support and the functions performed. (Example: Level 1 support monitors events, incident escalation, documentation, etc.)

6.5.10 What qualifications and certifications are required for your SOC staff?

6.5.11 Describe your approach to background checks or screening you perform on employees, contractors, consultants and vendors associated with any aspect of your managed services offering.

6.5.12 Please provide any additional information on your company or services which may be of value in our decision-making process.

7 Service Attributes

7.1 Security Monitoring

7.1.1 **Describe the technical architecture for your MSS services.**

7.1.2 **How does your monitoring technology integrate into our environment? What bandwidth is required?**

7.1.3 **Do you use any commercial SIEM technologies for event collection, correlation or analysis activities?**

7.1.4 **Provide a listing of devices (IDS, firewalls, routers, etc.) you support as part of your monitoring service. Please provide categories of devices as well as specific vendors technologies you support. Describe your preferred collection method used to gather security logs or events from devices. Describe other non-preferred collection methods that you support.**

7.1.5 **How scalable is your monitoring solution? Provide the current event load across your client base. How does your platform manage spikes in traffic growth?**

7.1.6 **How flexible is your monitoring platform? Can you support custom application logs? Explain the process and timeframe for supporting new event sources.**

7.1.7 **What data do you analyze from collected logs?**

7.1.8 **Rank potential event sources in order of recommended priority.**

7.1.9 **Describe your ability to monitor technologies via their native APIs.**

7.1.10 **Do you require SCN to maintain certain versions of the technologies you monitor?**

7.1.11 **Do you require implementation of a log collection or consolidation device on our network, if so, provide detail.**

7.1.12 **Describe the communication data flow between monitored devices on our network and your monitoring facility. Include the format, protocol, direction of communication and bandwidth implications. Describe how the confidentiality of the communications is protected across public networks.**

7.1.13 **Describe your methodologies for the following:**

- **Filtering of data gathered**
- **Normalization of data received**
- **Identification of suspicious activity**
- **Validation of security events**
- **Trend analysis of security events**
- **Retention of event data**

7.1.14 **Describe how you correlate traffic between IDS, firewalls, network devices, and other devices you are monitoring. Include details on:**

- **Event-Linking Correlation**
- **Asset-Based Correlation**
- **Anomaly Detection**
- **Meta-Event Correlation**
- **Fraud Data and Blacklist Data Integration**
- **Global Scale and Intelligence**
- **Early-Warning Systems**

7.1.15 **Describe your approach to correlation of data across your managed service clients and devices, regardless of type or function.**

7.1.16 **Describe your ability to correlate event data to asset criticality information.**

7.1.17 **How do you gain visibility into anomalous activity and how is that activity analyzed?**

7.1.18 **Do you integrate external intelligence into the monitoring process? If so, describe what intelligence is used, how it is obtained and how it impacts the analysis process.**

7.1.19 **Describe your approach to reducing false positives.**

7.1.20 **Describe the manner in which your company prioritizes client notification based on potential event impact.**

7.1.21 **Describe the type of notification and communication included as part of your MSS service. Please include the timing associated with each type of notification.**

7.1.22 **Describe any service limitations or thresholds that we would be charged additional fees for exceeding. How many incidents can be escalated before additional fees are charged? If services are charged hourly, describe the timekeeping mechanism in place, and how visibility will be provided to SCN?**

7.1.23 **Describe your ability to create custom correlation rules.**

7.2 Device Management

7.2.1 **Describe your managed service capabilities.**

7.2.2 **How long has your MSS organization been performing device management/monitoring?**

7.2.3 **Describe how your company provides security and technical support (e.g. deployment, incident response, forensics, etc.)?"**

7.2.4 **Do you have special relationships with the product and platform vendors of the products you will deploy?**

7.2.5 **Do you currently have a device configuration check-up procedure? And how often would you do this?**

7.2.6 **Do you currently have a pre-deployment testing procedure in place? If you do, please explain briefly.**

7.2.7 **Describe your process and quality assurance for making device changes. Describe your general device management quality assurance measures.**

7.2.8 **Describe how you will work with our IT MSP to effectively manage security policies and related hardware (firewalls, etc.).**

7.2.9 **Can you support our change management procedures? If so, how do you reconcile that with your standard operating procedures?**

7.2.10 **What visibility does the client have into device policies and configuration?**

7.2.11 **How many change requests are we allowed in a given month for managed devices?**

7.2.12 **Describe the troubleshooting process. If a customer or vendor device is functioning improperly, explain the process to return to normal operations. How do the processes differ?**

7.2.13 **Describe your approach for implementing a managed/monitored IDS/IPS solution for a client.**

7.2.14 **How do you assure timely operating system, firmware, patch, and signature upgrades/updates? What is your procedure for performing these changes? Include description of quality assurance measures.**

7.3 Managed Detection and Response

7.3.1 **Do you have your own Endpoint Detection and Response (EDR) technology? If not, do you rely on third-party technology for EDR?**

7.3.2 How does your EDR technology possess the capabilities to apply threat intelligence and behavioral analytics? Can that information be correlated against other security telemetry?

7.3.3 Explain how your EDR technology is supported internally. Does your staff understand adversarial threat behavior and how to incorporate that into threat intelligence?

7.3.4 Describe your company's Incident Response capabilities? Do you have an incident response practice? How long has it been offered?

7.3.5 How do your services incorporate Incident Response findings into the solution?

7.3.6 Describe your incident response staff. What types of experience/credentials does your company possess? Are they well versed in handling complex cyber incident response cases, with an understanding of legal and compliance implications?

7.3.7 Describe the technology that comprises your MDR solution. Does it include intellectual property? If so, describe the intellectual property, how it was developed and how is it updated?

7.3.8 Does your MDR solution include IDS and/or log forensics? If so, describe.

7.3.9 Does your MDR solution incorporate cloud? If so, describe.

7.3.10 Describe your global threat visibility capabilities. How do you stay updated on current and emerging threats? How is that information incorporated into your MDR solution?

7.3.11 Describe your MDR solution workflow. Include types of sources monitored, how alerts are correlated, how false positives are eliminated, the investigative process, how conclusions are reached and how customers are notified, if required.

7.4 Log Management

7.4.1 Describe your approach for collecting, indexing and retaining raw log data.

7.4.2 How long have you been offering log management services?

7.4.3 What tools do you use to monitor and manage log data?

7.4.4 What log sources are supported?

7.4.5 How is log data protected from tampering or misuse?

7.4.6 How scalable is your solution? How much log data can be retained?

7.4.7 What log reporting is available?

7.5 Vulnerability Scanning and Management

7.5.1 Describe your vulnerability scanning and management solutions.

7.5.2 Do you offer web application scanning and testing for database vulnerabilities?

7.5.3 Do you offer any solution that allows the client to scan for devices that are occasionally connected or maybe not be available when the scan is executed?

7.5.4 Do you offer any solutions that allows the client to satisfy the various compliance mandates?

7.5.5 Describe your vulnerability scanning architecture

7.5.6 Where do you source your vulnerability checks?

7.5.7 Describe any dashboard capabilities to provide visibility to all hosts and assets, their ongoing status, and alerting on changes.

7.5.8 How are vulnerabilities confirmed? What is the process to escalate and/or prioritize identified vulnerabilities?

7.5.9 Is vulnerability data used in the monitoring process? In what ways?

7.5.10 What vulnerability reporting is available?

7.5.11 How are vulnerability scanning reports delivered?

7.5.12 What are the qualifications of your vulnerability management team?

7.6 Cloud Services

7.6.1 How do your cloud technology services assist in increasing our overall security posture?

7.6.2 Explain how your solution handles the ephemeral nature of the public cloud.

7.6.3 How do your monitored and managed cloud solutions enable correlation across Public Cloud and On-Premise environments?

7.6.4 Describe the technical architecture for your Managed Security Services in the cloud, including whether an agent is installed.

7.6.5 What log and event data sources from Cloud Service Providers (CSPs) are supported?

7.6.6 Do you have existing agreements with various Cloud Service Providers to perform intrusive and non-intrusive vulnerability management assessments?

7.6.7 Do you offer ancillary cloud security services such as Consulting, Technical Testing, Incident Response or Threat Remediation in the cloud?

7.6.8 What maturity level do you have within each of the major cloud service providers? Be specific and detailed in both level of expertise and experience. With each service please provide knowledge level of IaaS, PaaS, and automated deployment capabilities and tools used.

7.7 Advanced Threat Services

7.7.1 Describe your managed service for endpoint security.

7.7.2 How is the solution deployed, and what are the bandwidth implications?

7.7.3 Are your endpoint managed services “always-on,” or do they rely on periodic scanning?

7.7.4 Describe the endpoint threat prevention, detection and response capabilities.

7.7.5 What visibility do your advanced threat services provide into what is happening in our organization?

7.7.6 In the event of an alert, do your advanced threat services provide remediation recommendations and context that we wouldn’t get from the security technology alone?

7.7.7 How long are telemetry and events retained?

7.7.8 What operating systems are your endpoint agents supported on?

7.7.9 Do your advanced threat services provide prevention, visibility and incident response guidance?

7.7.10 Does your solution assist in regulatory compliance?

7.7.11 Can your solution detect zero-day threats?

7.7.12 Do you have threat intelligence embedded into the solution?

7.7.13 Do you offer services that complement each other to provide stronger defenses?

7.7.14 In the event of a compromise, will you help us remediate?

7.8 Level 2 Analysis Services

7.8.1 What type of support do you provide beyond standard Level 1 analysis (correlation, filtering, notification of events)?

7.8.2 Describe how your Level 2 service works.

7.8.3 Which security event sources are supported?

7.8.4 What are the support hours for this service?

7.8.5 Will dedicated resources be provided to deliver this service?

7.8.6 How scalable is your solution?

7.8.7 Describe the qualifications and certifications of the staff delivering this service.

7.9 Threat Intelligence

7.9.1 Do you have a dedicated research team focused on threats and vulnerabilities?

7.9.2 What information sources do they source for intelligence?

7.9.3 How is intelligence analyzed and validated?

7.9.4 How is intelligence used in the management and monitoring of client devices?

7.9.5 What visibility do clients have into this intelligence?

7.9.6 What is the level of integration between the research team and SOC operations?

7.9.7 What services does your research team support? Is supporting research their only role?

7.9.8 How is this team modeled? What is their mission?

7.9.9 Provide examples of how proactive threat research has been used to protect clients.

7.9.10 Provide samples of research briefs or write-ups from research staff.

7.9.11 Provide "net effect" examples of how security responders, researchers and analysts have worked together to protect your clients.

7.10 Incident Response

7.10.1 Please describe the format of your Incident Response services.

7.10.2 What are the services that are available as part of the IR service?

7.10.3 Is there a minimum upfront financial commitment required for your IR services?

7.10.4 Describe how your IR integrates into the MSS services being proposed.

7.10.5 Indicate the experience of your IR consultants.

7.10.6 Describe how you integrate and apply Threat Intelligence into your IR services.

7.10.7 Describe how the hours can be utilized in the event no cyber incidents occur during the service period.

7.10.8 What is the false positive rate of incident alerts in the last 12 months?

7.10.9 What was your average detection and response time for incidents in the past year?

7.11 Portal and Reporting Features

7.11.1 Describe your company's user portal functionality.

7.11.2 How do users connect to the portal?

7.11.3 Does your portal feature mobile access?

7.11.4 How many users can the portal support?

7.11.5 Can access to the portal be limited by job function?

7.11.6 Does the portal feature customizable dashboards?

7.11.7 Describe your standard reporting process. How frequent will we receive standard reports? Do you have web-based reporting capability?

7.11.8 Do you have asset-based reporting allowing SCN to create and group assets, assign criticality and view event, scanning and all other information using asset views?

7.11.9 What standard reports are available?

7.11.10 Are compliance reports available? If so, which regulations are supported?

7.11.11 Do you support ad-hoc reporting requests? Describe the process for requesting ad-hoc reports. Provide the timeframe for turnaround of ad-hoc reporting.

7.11.12 In what formats can reports and data be exported?

7.11.13 How can reports be shared?

7.12 Service Level Agreements and Account Management

7.12.1 Describe your service level agreements.

7.12.2 Explain the expected working relationship, roles and responsibilities between your security staff, SCN's staff and SCN's IT MSP staff.

7.12.3 Describe your problem escalation process.

7.12.4 Indicate the frequency of meetings or teleconferences to review performance, issues, threat environment and responses. Explain the types of analyst and account management support provided during those meetings.

7.12.5 Describe how you measure and report client satisfaction, including frequency.

7.12.6 What is your process for adding new services or technologies?

7.13 Service Implementation

7.13.1 Describe your approach to implementing services.

7.13.2 What client resources are required to support implementation?

7.13.3 What is the typical implementation timeframe?

7.13.4 How do you ensure minimal impact or disruption to the client?

7.13.5 What steps do you take to ensure full and complete implementation?

7.13.6 Detail the handoff process once services are established.

7.13.7 What training is necessary to client staff to introduce them to the services?

7.13.8 How do you handle implementing services across widespread, geographically dispersed facilities?

7.13.9 What options are available for implementation? Remote installation? Onsite field engineers?

7.13.10 Describe the level of IT and security skills needed by client staff to implement and operate your solution.

8 Pricing

8.1.1 **Please provide pricing estimates for the proposed for a 12-month period. Please ensure all costs are reflected, including "implied" or non-explicit costs. Include descriptions of any volume discounts or economies of scale, especially for services based on number of users, identities or instances.**