Meaningful Security Conversions Questions to ask vendors to gauge their commitment to "Secure Products" and Demand Security

Version 1.4

This document is a tool for operators to have meaningful ***security conversations*** with their vendors. Today's 'security reality' is harsh. The approaches used to secure our networks are failing. If we want to make progress, we need new meaningful conversations between vendors who sell "security solutions" and their customers who deploy/operator security solutions. This document provides two conversation tools for anyone who operates a network (the "Operator"). The first is a set of questions that be the foundation of a vendor-operator dialog. The second is a list of "Request for Purchase (RFP)" questions that can be put into an RFP. Both "conversation tools" can be used by anyone with an interest in security. No security expertise is required.

You do not need to be a security expert to ask these questions. In fact, it might be easier to not be a security expert. Ask the vendors to educate you. People with some level of security knowledge tend to over emphases that knowledge, not really knowing what they are missing. This method of dialog with multiple vendors will result in a better understanding of what you need to accomplish.

"Vendor-Operator" Security Conversations. The first tool is a list of guided "security conversations" questions. These questions can be used with an organization's vendors. The key is to have "meaningful conversations" that clears the path for insight, knowledge, and action.

- These conversations help the organization learn how their vendors would serve their security needs.
- These conversations are not one sided. The vendor benefits from these conversations, creating a reason to take time to do the security work that helps all their customers.
- The security questions also act as a "guiding principles" tutorial for both parties, providing conversation template that can be traced to international standards.

- None of the questions listed are unreasonable. They are all based on two decades of security conversations in the community. There is no point in asking vendors to do something that does not fit with their business processes. All the items listed in the guiding principles section are things that have been done in vendors who are serious about security. There is nothing in the list which is out of scope or cannot be done.
- All the items in the guiding principles are will enhance the vendor's products and solution - benefiting all their customers. So if there are items that require new investment, that investment will benefit the vendor's entire eco-system.

Vendor Security RFP Questions. The second tool is a list of RFP questions. RFPs are powerful tools to drive change in a vendor. All the requirements listed in a RFP are items that vendors have deployed in their operations. Like the guiding principles, these RFP requirements are not asking vendors to do anything which is out of scope of what they should be doing to secure their products. Any requirement that needs additional vendor investment will benefit all the vendor's customers.

Use of this Document

This document is one chapter of a new book on practical security. This is a living document, with new versions provided to help Operators have those conversations with vendors. It can be used by clients of GETIT and Barry Greene for their RFPs and vendor interactions. While this document is reviewed by the industry's top security professionals, some of the best ideas come from new people who are using these conversations in their own organization. Feel free to send suggestions. If you have suggestions, please e-mail Barry Greene bgreene@senki.org. PDF copies can be found at www.senki.org.

Conversation Guidelines

The appropriate role of these questions are for conversation purposes. They are designed to instigate a conversation between the vendor and their customers that lead to meaningful discoveries by both parties. A more resilient system can only be achieved through the dialog of discovery and action. Discover is the process of asking the questions from all your vendors. Each vendor conversation leads to new insight. This dialog will be an on-going

Reality Check: Vendors will not proactively dive into the extra work of securing their systems. It requires their customers to demand security best practices from their vendors. Do not be surprised if a vendor has big security issues if you - as an Operator - do not take the time to push

habit that should be made part of your normal organizational DNA. The dialog of action is the objective. Security only happens through action, both on the vendor's part and the operator's part. Both sides need to look at the insight gained through the dialog and take action.

Here are some "conversation guidelines" to get started:

1. **Get Executive Approval to Commit the Time.** The #1 security action a CxO can make is the allocation of time for their existing team to invest in security. It does not take millions of capital dollars to make a significant impact on the organization's security posture. It does take time allocated from people's work day to invest, converse, learn, and act on the security knowledge. Get the CxO approval to have these security conversations.

2. **Ask the questions in writing.** Start the conversation by requesting in writing to your vendor with the first questions, the meeting time, and meeting location. The objective should be a partnership conversation. As hinted throughout this document, there are no perfect security solutions. What is important is the dialog and action.

3. **Non-Disclosure Agreements (NDAs) Might Be Required.** The dialog and information exchanged shares details that are best controlled so that the bad threat actors do not have access. Mutual NDAs are not required, but are also not to be a surprised. What is key is that both partied view the exchange within the understanding that the threat vectors are real and impact each of there customers.

4. **Set up regular meetings with your vendors to have these conversations.** These conversations take time. Often, both parties - the vendor and the organization - needs time to prepare the materials. Other times both parties require time to think about what was presented. But, both parties need to be committed to consistent dialog. The big organization change comes with persistent and consistent action. It is recommended that regular weekly or bi-weekly meetings are set up until there is an agreed resolution.

5. **Use all the best practice for effective meetings.** Set a clear agenda before the meeting. Ensure the NDA is signed before the meeting. Designate a note taker to publish notes. Share copies of the materials before the meeting (not after). Ask everyone to allocate time to read and review the materials provided by the vendor before the meeting. All of this and other "meeting BCPs" are important to gaining the most from these security dialogs. Effective meetings are what makes a dialog into a meaningful conversation.

6. **Get responses in writing from your vendors.** The writing process is not a burden for the vendor. The questions asked in the checklist applies to all their

customers. Every question asked is a question that would be asked by other customers.

7. **Do not expect perfection.** No vendor has everything covered. There are always big gaps. These conversation questions is a collection of deployed expectations based on multiple vendors, ISO standards, IETF Guidelines, FIRST guidelines, and other materials. Given this, it would be a surprise to find any one vendor who has all items in this conversation list covered.

8. **Ask for the Vendor's Security Resolution Plan.** How will they fill the gap. Some gaps may take a long time to rectify, which is OK if the vendor is committed to change. The resolution plan is the most important part of the dialog. It is a document that leads to action within the vendor. If several of the vendor's customers are asking for the same thing, the result is a business case for action within the customer.

9. **Build an Operator Action Plan.** As the Operator uses the conversations to learn about security, they will gain insight into how to build more security-resilient organization. For example, a vendor's security team would need to call the Operator. Who in the Operator do they call? What actions will that team take to remediate the issue? If an emergency patch is required to fix a security vulnerability, does the Operator have plans to push through "emergency patches?" These will be the sort of actions that the Operator will need to implement to leverage the full benefit of these vendor-Operator security conversations.

Guiding Principles to Demanding "Security" from Vendors

Conversation Phase 1 – Review the Vendor's Vulnerability Management Process

The first phase of the "security conversation" is how the vendor will respond to security vulnerabilities. There is ***no*** possibility of creating a totally secure system. Vulnerabilities and risk will be found. How the vendor respond when vulnerabilities is the first conversation organizations need to have with their vendors. How a vendor will react to a vulnerability reported and facilitate the deployment of the fix is a key element for all organizations. Vendors with immature vulnerability management processes are a risk to the organization. These questions will be a facilitation tool. The organization does not need security experts to ask the questions. The response from the can be measured with common sense.

> ***Reaction First, Proactive Next. Some might question why the ability to react to a security issue should be the top of the list. This is a core element from crisis management that is used within the security community. If there is no way to create "perfect security," then the ability to react to risk, manage risk, and priorities risk should be the first items to be addressed. They should also be the first items for an Operator to ask when exploring their vendor's security capacity.***

✓ **Does the Vendor have a Vulnerability Management Process?** Never, ever expect any vendor to have a perfectly secure system. It will never happen. Brilliant, economically motivated cyber-criminals are digging into systems looking for zero-days that are beyond the scope of most vendors (and operators and white hat security penetration teams). Expect the discovery of an advanced persistent threat (APT) inside your organization. When this happens, how the vendor responds is critical. Many vendors will dismiss or hide the problem. Most vendors will not have a vulnerability management process (especially new vendors and vendors outside the US and Europe). Do not wait for a vulnerability's announcement on the news and exploited to harm customers. Understanding the vendor's response to these crises is critical to the operability stability of the operator. Given that, vendors should be able to present to their customers their vulnerability management process. The first conversation starts with the vendor presenting to their customer explaining their process. This provides a baseline for all the subsequent conversations.

✓ **Check the vendor's website. See if they have a "/security" page with information about how to report a security vulnerability and their security team.** Each company should have a public, easily accessible page that allows anyone easy access. For example, www.example.com/security would list he security team details, how to reach them, their phone number, and PGP keys. Too many companies have been blindsided with vulnerabilities reported via "full disclosure" ("full disclosure" is where a 'finder' of the vulnerability reports it publicly without coordinating with the vendor). Vendors who do not have this simple public contact list are an indication of their ability and interest into the security of their products.

✓ **Check if the vendor has a published vulnerability disclosure policy.** The vendor should have a publicly accessible and policy on their corporate vulnerability disclosure process. The vulnerability disclosure process will meet industry expectations for responsible disclosure. This make is clear to everyone what their vulnerability disclosure policy will be when someone finds a

vulnerability and reports it to the vendors. The absence of a vulnerability disclosure policy is a test to understand the quality of the vulnerability response team inside the vendor.

✓ **Does the vendor have a Security and Vulnerability Response Team that is available 7x24, 365 days a year with English as the primary language of business?** "Availability" shall be via E-mail (using PGP) and phone. Availability should be tested with all vendors. The operator should ask for an initial briefing call with the Security and Vulnerability Response Team. Ask for a run through with all the policies, procedures, tools, and approaches used by the vendor to ensure their products are as secure as possible. That first call will provide a gauge of the vendor's security maturity.

✓ **Does the vendor participate with industry vulnerability and incident response teams?** As mentioned, the only way the industry can respond to the aggressive cyber-criminal threat is via aggressive collaboration. No vendor can work in isolation. Collaboration with their peers, their customers, security researchers, and law enforcement has proven to be the best defense. Operators can "test" to see if their vendors are collaborative by checking on their industry participation. For example, all vendors selling equipment and software to the Internet and telecommunication industry should be part of the Forum of Incident Response and Security Teams (FIRST) www.first.org. FIRST is one key industry groups for vulnerability and industry response. Just being a member of FIRST requires a community audit of the vendor's processes and procedures. If the vendor is not a member of FIRST, ask "why" and "when."

✓ **Does the vendor participate with the national vulnerability and incident response teams?** While many vendors might be a member of industry groups, few put the extra effort into the national Computer Emergency Response Teams (CERTs). These groups are as critical to vulnerability management as the national groups. All operators should have some relationship with their national CERTs or other vulnerability coordination bodies. These could be national CERT Teams or special interest groups like that Information Sharing and Analysis Centers (ISAC) community (see http://www.isaccouncil.org/memberisacs.html). The operator's vendors should have some relationship with these local security and vulnerability response teams. That relationship is an excellent test of the vendor's security maturity.

✓ **How would the vendor notify our organization about a security vulnerability?** Do you get action alert E-mail directly from the vendor or do you read about the vulnerability from the morning news? How your organization gets notified

of the vulnerability is critical to the whole process. Some vendors will have their System Engineering (Sales Engineers) walk into the customer and brief them in person. This is an extreme example, but indicative of the level of effort needed by the vendor to communicate during a crisis. Reviewing these processes before a vulnerability happens is strongly advised. Note: Phase 4 of the security conversation will get into deep details of how the vendor interacts and notifies their customer. During the first phase of questions, the objective is to get the quick answers.

Conversation Phase 2 – Review the Vendor's Security Development Lifecycle

The security development lifecycle (SDLs) are all the activities used during the product development to minimize security risk. SDLs do not eliminate risk, but they do reduce risk. The "risk reduction" is two-fold. The first is the risk to the shareholders of the vendor. Products which have reduced security risk have less chance of impacting the company's profitability through preventable security vulnerabilities. The second risk reductions are to the vendor's customers. Risk are inherited from the vendor into the Operator by selection of that vendor to be used in their operation. This "inherited risk" give the vendor's customers the ability to ask in-depth questions on what they are doing with their SDL to reduce inherited risk.

The follow are some excellent questions for an Operator to have with their vendors to gain an understanding of the vendor's SDL. Note that you do not have to be an expert to ask these questions. Common sense is common for everyone. Ask, listen, and learn. Then ask more questions.

Demand the Vendor provide their Security Development Lifecycle (SDL) process. This vendor presentation will normally be under a nondisclosure agreement with the details confidential. But, each vendor with an SDL should have the ability to brief their customers, explain how the SDL process works, explain how the SDL process is evolving over time, and explain how the customer can engage with the SDL process. What should an operator look for in a mature SDL? There are books, papers, and guidelines in the industry that cover best practices for SDLs. Here are some of the core items to seek in your vendor's SDL:

- **How is the vendor's SDL integrated into the vendor product development processes?** Security "after the product development" is an afterthought. It never works. Effective SDLs are an integrated part of the normal product development process. Look for the vendor's SDL presentation to first present

their product development process, then how the SDL integrates with that process.

- **How does the SDL process allow for rapid vulnerability fixes?** "Zero Day" vulnerabilities are often in the "active exploit" mode. That means these reported vulnerabilities need to have the fixes defined, integrated, tested, and deployed in hours - days - not weeks - months.

- **Does the SDL process use a form of Root Cause Corrective Action (RCCA)?** When a vulnerability is discovered, there are two phases to the "fix." Phase one is to get the vulnerability fixed to mitigate the potential active exploitation. Phase two uses an RCCA process to find out how the vulnerability got through all the checks. The RCCA is essential to find more potential issues. The RCCA is then used to update the tools, processes, and test to prevent a repeat of the Root Cause. The RCCA goes beyond "regression testing" and looks for the underlying causes, fixing those causes, and making impactful improvements.

- **Does the vendor's SDL include regular Static Analysis Testing?** How the results of the static analysis testing is used to improve the resiliency and security of the code? Static analysis testing is one of the many tests to check on the quality of the code. There are open source static analysis tools, vendor specific tools, and commercial tools. A commercial example of static analysis is Coverity (www.coverity.com). Many vendors will use static analysis testing, get overwhelmed with the volume of errors, and take no action. Ask the vendors how many bugs were fixed each quarter; as a result, of their static analysis testing. Remember, this sort of testing is about code stability and security. It catches coding mistakes that could lead to outages.

- **Does the vendor use Test Driven Development (TDD) in their software deployment?** TDD is an approach to coding use in Agile Development. The essence of TDD is to first code a test for the new function before coding the function. Yes, this seems backward - writing the test before the function. But, the decades of TDD application demonstrates that the disciple of first figuring out how to test the function before writing the function forces quality into the code. The result in the industry code that is higher quality, fewer bugs, and fewer security issues! Ask the vendor if they are using TDD. Seek to find out if they are using it in all their software This will include microcode for their hardware (ASIC, FPGA, NP, etc.) and elements in network equipment (control plane and management plane elements). TDD now has industry consensus to

the empirical impact to the quality of software development – specifically with the prevention of security vulnerabilities.

- **Does the vendor use Dynamic Analysis Testing (DAST) in the vendor's development process?** Dynamic Analysis Testing (DAST) is different from static testing. While static testing pulls in source code to look for issues, dynamic testing pulls in the compiled software image. Dynamic testing made huge gains over the last decade. The revolution of virtualized environments makes it easier to load a compelled version of the code into a simulator designed to dynamically test the image. Issues fond via DAST cover security, stability, robustness, and for some performance. DAST will undercover issues that will not be seen with static analysis. There are problems in code that is a result of code interaction. Two modules might interact in a way that causes a vulnerability or instability. These interactions are hard to identify with static analysis, but are more easily seen after the code is compelled and tested. Vendors who care about the quality of their code should have both static and dynamic analysis testing. There are now open source tools available as well as tools built specific by the vendor for their unique environments. A good commercial example to explore would be Veracode (www.veracode.com). They provide a baseline example of a dynamic testing tool used extensively in the industry.

- **Does the vendor use the industry vulnerability classification and enumeration tools?** The industry puts a lot of effort into common tools to normalize the risk of a vulnerability. These tools include the Common Vulnerability Enumeration (CVE), Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), and several other tools being developed. The operator should first ask if the vendor knows about these tools. Then ask who they use these tools in their Security Development Lifecycle (SDL) processes. For example, The CVSS system has been used in several vendors to put a metric on the risk a reported vulnerability has to their customers. The CVSS risk value then drives the coding priority in the company. The higher the CVSS risk, the faster the vulnerability gets fixed, tested, and deployed to the customers. CVSS puts an empirical metric to drive the internal processes. This CVSS value is then used to determine how the vulnerability will be disclosed to operators. The higher the number, the more risk to the customer. A CVSS priority will govern the speed of field testing and deployment of the fixed code. Another example is the use of CWE in static and dynamic analysis testing. Many times these tests produce huge reports. Vendors often do not know where to start. In response, the industry has a top CWE list. CWE metrics allows the static and dynamic testing vendors to put a CWE value to each of their finding. The CWE value can then be used to triage the list of issues and prioritize limited coding

resources on the most critical CWE items. Overall, vendors who are engaged and can explain how they are uses these tools in their SDL processes are must more engage with the security of their products.

- **Does the vendor have Regression, Stress, Performance, and Compliance System Testing?** Some might ask "isn't this basic?" Yes, it is basic. But operators would be surprised to find that major vendors do not have a structured system to test. Any operator who is serious about the resiliency and security of their operations should have details of the vendor's regression, stress, performance, and standards compliance testing. This information would be presented under an NDA. It is a mark of a mature synergy between a vendor and their customer to have conversations around on the improvement of the testing environment based on their joint operational experiences. For example, an issue found in the network that was missed in all prior testing would be added to the vendor's regression and stress test. This will ensure that this issue is not repeated. It is also used for other products the vendor launches. How does this test impact security? Most of these test suites are systems test. They test the product in a production simulation. These systems oriented test are the logical follow-on to the static and dynamic testing.

- **Does the vendor use of fuzz testing in their quality processes?** Fuzz testing pressure test an element in unexpected ways. Normally engineers who write a test are ensuring that the element under test is working as expected. Fuzz testing is the opposite. It is designed to send the unexpected. If an element in the protocol is four bytes in a specific location of a packet, then the fuzz test will send 4 bytes offset before - mismatching the location. It is interesting how systems respond when they receive information that is unexpected. Some of the most damaging security vulnerabilities have been found during fuzz testing. Others vulnerabilities have been found in crash core dumps - where the "bug" that cause the crash could if easily be found if a fuzz tester were used on the protocol. The operator should have a conversation with the vendor if fuzz testing is used and how it is used with their product.

- **Does the vendor have documented risk assessments for all elements, protocols, systems, and solutions?** Part of an SDL is the risk assessment process. Features and functions of the product should include the capability to mitigate risk. How would the operator know if they vendor is performing these risk assessments? Ask for a review of the risk assessment. There are several approaches the vendor can use for these risk assessments. Some vendors like the ITU X.805-risk assessment process attempts to illustrate this in detail. Other vendors use simpler attack trees to explore all the vectors for

risk. Some will develop their own methodology that is tune to their solution's environment. All of these are A-OK. The core principle the operator should look for is the existence of a risk assessment and how that impact the capabilities of the product.

- **Does the vendor use specific security testing tools for their Unit Under Test (UUT) testing?** There are many open source and commercial security testing tools on the market. These solutions range from full organizations to commercial tools. For example, the Open Web Application Security Project (OWASP) is focused on tools practices, and best practices to promote robust web security. These tools are open source and often free to use. Contrast this to the mature market of specific commercial security testing solutions (Spirent aka Mu Dynamics, IXIA, and Codenomicon, Veracode, Qualys, Cigital, Imperva, Fortify, Trustwave, etc.). These companies are worth interacting with to see how they would test the vendor's product in an operational environment. Operators with the means can consider using these tools in their own testing and evaluation. Others can review the tools and then ask the vendors to use them in their testing.

Conversation Phase 3 – Review the Vendor's Healthy Interaction & Transparency

Once you understand the vendor's SDL processes; it is appropriate to ask the tougher questions. These questions will determine vendors who are "OK" with their product security commitment from the vendors who are "all in" in their commitment. It should not matter if you ask these questions to the vendor directly or through your local reseller.

✓ **Will the vendor's Security and Vulnerability Response Team review postmortem on past vulnerabilities with our organization?** Vendors who have a long track record of security will have a history of vulnerabilities. The vendor's security team should be willing to review with customers past vulnerabilities, how they were found, what was done to fix, the code, what was learned, and how improvements were applied. This conversation is an excellent measure of the vendor's commitment to security. As mentioned before, in today's environment it would be impossible to have perfect security. What can be done is continuous improvement to minimize as much of the risk as humanly possible.

✓ **Does the vendor bring in 3rd party penetration test and security auditors?** All security professionals know that the biggest danger is myopic thinking. Internal security teams will fixate on what is known. The internal security team will often miss out on things that might be obvious to someone else. Some vendors mitigate this narrow thinking by investing in their teams. Sending them to a range of security conferences helps them keep a broader view of the risk. But many times this is not enough. Regular 3rd party penetration test and security audits are an effect means to review a vendor's full SDL process. The operator should ask if the vendor pulls in these 3rd party security audits, how they are used to improve the processes, and if they will continue with the practice. It would not be appropriate for the operator to asked details of the 3rd party findings. What is more important is the level of commitment by investing in these 3rd party audits.

✓ **Will the vendor be open to a joint table top exercise?** Table top exercises are tools used in the security incident response community to test the processes and procedures. Operators asking their vendors to be part of a tabletop exercise is a critical to the robustness of their operations. For example, one large on-line web site did a robust table top exercise with all their vendors where they simulated a combined DDOS attack with the exploitation of a zero-day attack. The exercise tested all the processes and procedures. Lessons were learned. All the processes were updated. Nine months later this large on-line company's alarms were triggered a week before a major news event. They knew they were going to get hit with a major DDOS attack. They also saw the scans looking for what could be a zero-day attack. This vendor activated their emergency response procedures, pulled in all the vendors, and prepared for what was going to be a major attack during a major surge of customer traffic. As it turned out, all the preparation mitigated the attack, found a vulnerability, fixed the problem and maintained services throughout the customer surge. This is one of many examples where an operator preparing with compressive table top exercise were able to keep services operating at 100% in the middle of a major attack. It works. Ask the vendors if they have the willingness and capabilities to participate.

✓ **Will the vendor be willing to open their code to an operator driven source code audit?** What? Why would Operators (our customers) want to look at our source code? Why would any vendor allow that to happen? Simple. The cyber-security risk is not just a cyber-criminal risk. It is now a nation state risk. Vendors and governments are now asking their vendors to open their internal processes to operator driven reviews. These reviews are under very tight NDAs

with additional contractual agreements to protect intellectual property and liability risk. These operator driven audits are happening in the industry. The vendor should expect their customer to ask. Operators who are worried about Nation State cyber-security risk should first do all of the above, then build the capacity for this type of security audit.

✓ **Will the vendor publish the "reporter" of a security vulnerability in their security advisory?** A leading indicator of a vendor's security maturity is their policy on providing credit. Mature vendors with a thoughtful security policy will provide credit to the people who "report" and "find" security vulnerabilities. This "giving credit" policy is good for all parties. It encourages responsible vulnerability reporting and disclosure in the community.

✓ **Does the vendor have an active bug bounty program?** Bug bounties are an evolution of a vendor or service provider working with the community to find problems before they become a problem. Bug Bounties are normally run by a company that specializes in managing the bug bounty. This "outsources" some elements of the security management, but assures that someone is looking at who is reporting the vulnerabilities to the vendor. A Keyword search on "Bug Bounty" will highlight companies who either manage bug bounties or sponsor bug bounties.

✓ **Will the vendor provide the required "GPL" documentation based on requests for all open source software used in the organization?** Whine a vendor uses open source forward in their product, that vendors must comply with the open source license to use that open source. There are several different open sources licenses in used in the industry. The range "use it however you choose" to "if you modify it you must submit the changes publicly." Open source compliance is something that can be used gauge the level of vendor maturity. If they do not know how to manage the open source software in their product, then they most likely are not managing their own code in their product. As a minimum, the vendor should provide a list of all the open source software using throughout their product. Using open source is a good thing. Using open source that does not match license and practice creates preventable risk.

✓ **How does the vendor manage open source security vulnerabilities?** Open Source is highly encouraged, but open source is also being maintained. Part of that maintenance will fix security vulnerabilities. As the industry has seen with [1], each vendor who uses Open Source needs to have workable plans to fix

[1] Heartbleed was a OpenSSL Vulnerability discovered through proactive security testing in April 2014. https://en.wikipedia.org/wiki/Heartbleed

vulnerabilities with all the open source used in their products. This question is another data point to help measure the security maturity of the vendor.

Phase 3 are some of the toughest security questions to ask vendors. It will push most vendors. Many times the vendors will not have answers because they do not have processes, procedures, nor tools to address the questions the Operator is asking. This is hard work, but it will only get done if the Operators who buy and deploy these solutions ask the questions. Otherwise, there will be no "justification" for the vendor to allocate time/resources.

Conversation Phase 4 – Joint Vulnerability Reaction Plan

Vulnerabilities are inevitable. The speed of reaction by the vendor and the operator will determine the window of risk to the business. If an organization wishes to rapidly respond to vulnerabilities, they must proactively invest in a joint reaction plan. This phase of the security conversation is more intensive. It will get into planning that might turn into contract and service level agreement (SLA) conversations. Notice that conversation on the reaction plan is after much longer conversations that inform both parties.

- ✓ **How will the vendor disclose a normal security vulnerability to our organization?** This is a redundant question but worth reviewing again. There will be more insight from each of the vendor conversation and within the own organization as the Operator reviews their own processes.
- ✓ **Does the vendor have a phased disclosure process for notifying customers before the full public disclosure?** Some vendors will have segments of their customers who will be exposed to attack once the vulnerability is publicly disclosed. This window of vulnerability has posed life impacting risk on the industry. The time it takes for a vulnerable to be "weaponized" by a threat actor is now hours vs weeks. The time it takes to weaponize is determined by the motivation of the threat actor. For example, a cyber-criminal DDOS extortionist who sees a new vulnerability useful to their DDOS extrusion racket will be highly motivated to weaponize and use the vulnerability to increase their cash flow. Knowing this "window of exposure risk," some vendors will create a phased disclosure process. This phased disclosure will notify some customers before other customers. This process is customized per vendor and the dialog with their customers. The key for the "security conversation" is to have the conversation and understand the vendor's process (if it exist).

- ✓ **What are the upgrade plans for each vendor element in the organization? Can the upgrades be done with minimal impact to the organization's business?** A fix for a vulnerability is of no use if it cannot be deployed. This means the vendor and the organization needs to have an upgrade path and plan for each of the vendor's elements in the network. This might be software, hardware, M2M elements, IoT elements, or any other part of the network that requires an "upgrade/patch" to fix a vulnerability.

  It is advised that the organization exercises the upgrade plans. How long will it take? Will there be impacts on the business? What will it take to "certify" the new upgrade? These are all questions that need to be answered in this conversation.

- ✓ **We buy the vendor's equipment through a 3rd party/reseller. How will we work with the vendors to review our reaction processes?** Many organizations cannot buy directly from the vendor. They need to go through a local reseller. The reseller should not be a barrier to the ongoing "security conversations."

Phase 5 – Cryptography – The Toughest Questions

How a vendor handle cryptography is some of the hardest questions for the vendor and the Operator to address. Honestly, most of the time you will have both sides talking past each other as "crypto novices" try to communicate with each other. Many do not like this truth to be pointed out. But it is needed for people to get into meaningful and productive conversations around the vendor's use of cryptography. But, these questions need to be addressed by both parties. Not addressing them will expose the both organizations to preventable risk.

Conversation Guidelines for Cryptography Conversations

Acknowledge that Cryptography is Critical. Organizations cannot assume that there is no-one sniffing the wire, accessing the files, or using other means to access information. Crypto is a critical part of an organization's defense It will increase over time as our technology become more widespread.

Acknowledge that Crypto Conversations are specialized. People who have not invested in the time and effort to learn will get lost. In fact, "crypto experts" who have not spent recent time in the field will often need crypto-refresh to think within

that specialized mind-frame. This should not stop vendor-operator dialogs on cryptography. Everyone needs to be asking these questions.

Constantly Revisit the Crypto Conversations. Breaking crypto is something criminal and state actors actively pursue. In addition crypto professionals proactively try to break systems before the bad actors find ways to do it. Given this level of "active investigation," Operators should be revisiting their vendor's "crypto strategy." These conversations are not one time meetings.

Cryptography Questions to Prime the "Meaningful Conversation"

Note: Version 1.4 is the beginning "meaningful cryptographic questions." More will be added in future versions.

What Cryptography is supported? Start with the basics. Get them to list out what the vendor things is the full list of cryptography usage. This might be a complete list it might be an incomplete list. There are times when parts of the organization do not know what other parts of the organization are doing, even through its is all on the vendor's product.

What is the list of cryptography certifications that the vendor supports? Where is its supported in their software? This list would be the second question that would help lay the foundation for the vendor's crypto strategy.

What is the vendor's "Crypto Strategy?" Will the vendor support back doors to support various demands for access to cryptographic access? How does the vendor manage the requirements from places like US, China, UK, and other countries? It is important for the vendor to be transparent. Crypto transparency allows for each organization to accurately measure risk.

How does the vendor manage the software signing keys within their organization? All the vendor's code should be signed. How they handle the certificate within their organization is a good indicator of the crypto maturity.

How does the vendor test their cryptographic implementations? As mentioned, there is concerted interest by multiple parties to break crypto implementations. These "investigations" target the cryptographic algorithm, the implementation, the vendor's specific implementation, the supporting protocols, the configuration, the operation, and the key management. Given this, vendors should have some sort of proactive testing practice where they are one of the "investigators" on their own implementations to find problems before the bad actors (or a University grad student who is working on their thesis).

How does the vendor manage their keys wishing their implementation? Many times the "theory" of good cryptography breaks down with the key management. There are many times where poor key management allows private keys to be pushed out into the public. Asking "how the vendor manages keys" help understand what might be missing with the vendor's solution. For example, ask what would happen if the Operator needed to push out need keys ASAP because of some type of staff change. How would that work? Can it work?

Conversation Phase 6 - Review Industry Certification

Finally, look at the vendor's Acceptance Test Plans and Solutions Certification Plans. Does the vendor include security as part of their acceptance - certification test plans? Vendor deploying their solutions are driven to get the solution up, running, tested, and in production. Testing for security is normally not part of the acceptance testing that the operator nor vendor require. Security is an "afterthought." It might be months later when the security team come into review and find major configuration issues that have left the solution vulnerable to attack. One of the truest tests of a vendor's commitment to security is to see it practices in all parts of the company in all phases of the product's lifecycle. Even with the deployment teams who are working hard to get the system up and running.

Time for Action

There is no security without action. It is like Yoda's wisdom, "there is no try, you either do or do not." Security is no different. It only comes from action. Talking is not action. Everyone in the Operator who is part of these vendor security dialogs

are going to learn. They are going to think. They are going to reflect. They are going to think of things they can do right now to make their organization a more secure and resilient organization. It is vital for the team who are facilitating these conversations to take action. That is action should be on both sides of the conversion. The vendors need to constantly seek ways to build more resilient products. The Operator need to find rational solutions that minimizes security risk to their organization.

Security Requirements to include in an Request for Purchase (RFP)

The following questions are designed to be cut and pasted into the RFP document.

Security Requirement	Justfication
The vendor shall be required to be a member of the Forum of Incident Response and Security Teams (FIRST) www.first.org.	
The vendor shall have a Security and Vulnerability Response Team that is available 7x24, 365 days a year with English as the primary language of business.	
The vendor is required to have publicly accessible and published policy on their corporate vulnerability disclosure process The vulnerability disclosure process will meet industry expectations for responsible disclosure.	
The vendor will deliver their detailed vulnerability management process that has the complete life-cycle of the vulnerability report to the risk assessment process, to the processes to rapidly fix the vulnerability to the customer disclosure phases.	
All vendor claims of that their product is “secure” must have a 3rd party report and validation to support the claim for “security.”	

Security Requirement	Justfication
The vendor will produce documentation on their product development process that includes measure to ensure the security of the network element, feature, function or system. This would include: • **Regular Static Analysis Testing and how the results of the static analysis testing is used to improve the resiliency and security of the code. An commercial example of static analysis is Coverity (www.coverity.com).** • **Test Driven Development (TDD) using the vendor's software deployment cycle for all software, from microcode to unit software, to control plane, to full systems integrations solutions. TDD now has industry consensus to the empirical impact to the quality of software development – specifically with the prevention of security vulnerabilities.** • **Use of dynamic testing in the vendor's development process for all software and applications. Veracode (www.veracode.com) is a commercial example of a dynamic testing tool used extensively in the industry.** • **Use of the Common Vulnerability Enumeration (CVE), Common Vulnerability Scoring System (CVSS), and Common Weakness Enumeration (CWE) in their processes and procedures.** • **Extensive use of fuzz and vulnerability testing in their quality processes.** • **Documented penetration test on all network elements, protocols, systems, and solutions.** • **Document and present the vendor's full Security Development Life Cycle (SDLC), how long has the process been implemented, and provide examples of three serious security issues the SDLC process prevented.)**	
The vendor shall have all network elements tested with known industry leading security test equipment. The minimum equipment will be Spirent (aka Mu Dynamics), IXIA, and Codenomicon (http://www.codenomicon.com/). The vendor shall use the comprehensive security, saturation, and fuzz test for all network elements. The reports shall be provided.	
The vendor shall be required to obtain an 3rd party security analysis and penetration test organization to validate the security of the network, systems, and solution. The 3rd party will be selected by The Company whose cost will be covered by the vendor.	

Security Requirement	Justfication
Proposed solution shall have capability to detect, identified, block, and giving alert when their proposed solution is attack from external and internal threats. The blocking shall not have an operational impact on the network element.	
The proposal solution shall have tools that detect malware infecting The Company's customers. The solution shall provide the capability to walled garden the customers and other communication tools to facilitate the customer ability to know and remediate their malware infection.	
All proposed Security solutions must be upgradable, allowing for new signatures and profiles. These updates shall be at no-cost to The Company.	
Vendor shall provide solution where actively protect system from fraud access that may lead unauthorized access and revenue loss.	
All network elements that is access by the staff shall be configured to use an internal Authentication, Authorization, and Auditing (AAA).	
All network elements in the vendor's proposed solution shall be able to integrate to an internal Authentication, Authorization, and Auditing (AAA) server. This will be used for all staff, tools, and Bots to log into and manage the network elements. Kerberos, TACACS+ or Diameter are the three accepted AAA protocols. Other newer AAA solutions that meet the requirements can also be acceptable.	
The vendor shall supply a redundant internal AAA solution to manage access to all network elements. The AAA server must be completely secure and redundant.	
All network elements shall be configured for Network Time Protocol (NTP) and Precision Time Protocol (PTP). All security and event logs on the network element shall use the time from PTP.	

Security Requirement	Justfication
Vendor will provide user log server, where all action done by user in each network element will be store off-line on a secure logging infrastructure.	
The vendor shall provide security monitoring and security remediation capabilities on all third party partner connections to their solution. This includes APIs and other integration interfaces.	
The vendor shall provide a vulnerability scanning tool that would regularly scan all network elements to ensure there are no known vulnerabilities. The vulnerability scanning tool's will provide reports and recommended remediation. The vendor shall maintain the signatures through the life of the solution's contract. Qualys (www.qualys.com/)and NESSUS (www.tenable.com) are examples of commercial vulnerabilities scanners.	
The vendor shall have a documented and demonstrated security process that includes how the company secures their network, how they build secure products, and how they react to incidents that impact their products and their customers.	
The vendor shall have a publicly view able website that list all public security policies and practicers. This is normally a "/security" page with information about how to report a security vulnerability and their security team.	

Security Requirement	Justfication
The vendor shall supply their development lifecycle that includes all testing. This would include items listed in (Figure) but have special details with the following: • **The software engineering code management.** • **Validation of the security and integrity of the signed codes - including the build processes used to protect the code from non-authorized insertion of code.** • **Feature/Function Testing done on each version of the software** • **Regression Testing (with the policy of which bugs get added to the regression test and how many test are added each cycle)** • **Performance Testing** • **Stress Testing (including is you perform any fuzz/ boundary testing)**  **Typical Vendor Software Development Cycle Interlocked with their Customer**	
The vendor shall have an Internet accessible to to access, submit, and review all software and hardware bugs. This tool shall be secure, with all Network Staff at The Company ability to access the Bug Tool as any time. Access to the Bug Tool shall be part of the total support package. The Bug Tool will have the functionality to perform "bug scrubs" on each version of software.	

Security Requirement	Justfication
The vendor shall arrange for quarterly software roadmap reviews. These reviews will present the next years software feature roadmap for the next year, provide training on new features, and functions, and receive feedback on the road map priorities from The Company.	
The vendor should provide technical certification reports on all software quarterly. These will be written reports that highlight any issues that might require upgrades.	
The vendor should provide immediate vulnerability disclosure reports with software fixes within 30 days from the time of first report of the vulnerability.	