LESSONS LEARNED IN VULNERABILITY MANAGEMENT

InquisIT

www.inquisitllc.com

INTRODUCTION

Cybersecurity risk has taken over as the number one topic keeping CIOs and CISOs up at night. Whether it be because of user error, emerging zero-day threats, or persistent attacks against perimeter infrastructure, there is no doubt that agencies are under constant attack from foreign and domestic threats. Never before has it been so critical that agencies stay at the forefront of technology while maintaining patch management, configuration management, awareness programs, and overall vulnerability management in alignment like a finely tuned engine.

How do agencies outpace cyber threats? The answer is simple – Manage your vulnerabilities! Well, it's easier said than done.

Federal agencies are required to manage vulnerabilities on their network, but often are not provided with all the necessary information on how to execute. Policies are sufficient for heavy brush strokes coming down from The Department, but more and more frequently the operational components of Vulnerability Management programs lead teams into peril. Having infinite options on when and how to run the program (and with what tools) can lead to a 'paralysis by analysis' effect, leaving SOPs in draft form for way longer than necessary.

Unfortunately, there is no one universal 'silver bullet' for the best way to structure the optimal Vulnerability Management program. Much of an effective program is more an art than a science, and requires constant tuning based on lessons learned.

If you have been delegated responsibility for building out a program for your agency, hopefully these hard-earned lessons give you some ideas to think about in terms of preparedness and technical capability.

ALWAYS BE THREAT MODELING

ADAPT SCANNING STRATEGIES AROUND YOUR ENVIRONMENT

If you are fortunate enough to come into a Vulnerability Management program at the beginning, then you certainly have your work cut out for you.

At InquisIT, our engineers have never stepped into any two agencies with the exact same functional requirements. Whether networks are Linux heavy, entirely Windows, something in-between, host a variety of appliances, one-off GOTS infrastructure, or middleware systems, performing thorough analysis up-front is key. What is critical is taking a thorough inventory of what you have and who is responsible for it. Automated tools are the most helpful (eg. Nmap, BigFix, SCCM), but supplementing with old-fashioned emails and tag-up sessions could uncover some endpoints which would otherwise go unseen.

In addition to technical inventorying, understanding the chain of command and setting forth a communications strategy with responsible parties (aka. the 'soft skills') is a commonly overlooked component of any Vulnerability Management program. Scanning systems and generating reports are great, but potentially worthless if the engineer is incapable of communicating risk in real-world terms.

Aside from laying out the repercussions of an exploit, taking operational processes into account is a common hang-up which could drive a wedge into an otherwise successful Vulnerability Management program. Take into account when peak hours for each system are, when patch management cycles take place, or when releases are being integrated for the best results. Remember, setting scans to run on production systems at peak hours during the busiest time of the season could put a bad taste in everyone's mouths and (even in 2019) cause some unintended performance impacts.

NOT ALL DEFICIENCIES CAN BE SCANNED FOR

A missing best-practice security configuration is raised to senior leadership. The discovery leads to some sour looks, uncomfortable meetings, and lines of questioning such as "Why didn't your scanner discover that we weren't doing X, Y, or Z??". The fact of the matter is, a scanner can present you with technical findings all day long. However, unless you look outside the console and put the findings together in a context that makes sense for your organization, you are missing out on the big picture.

Oftentimes this encounter will be seen when lower-severity scan findings are ignored. These categories often fill scan reports with self-signed certificates, SSL or TLS versioning, weak cryptographic algorithms, SMB signing enforcement, Network Level Authentication, IKE/IPSEC configurations, or otherwise difficult to interpret findings which fall into the 'organizationally defined' category of remediation. Many of these findings are Low or Medium severity because they require a prerequisite to be exploited (such as being behind the organization's firewall, establishing man-in-the-middle positions, etc.). Remember though, the most sophisticated cyber-attacks historically chain together more than one low-level vulnerability to tip the scales in their favor.

Knowing what a finding means in the grand scheme of things is where the rubber meets the road. Don't rely entirely on your tool to put the pieces together for you, and don't ignore findings which require executive input. Perform the research and determine if there is a logical process in which the finding can impact your organization. Always be threat modeling.

DON'T LET A TOOL OWN YOU

A major faux-pas for any Vulnerability Engineer is aligning tightly with only one scanning tool or vendor. As technology professionals, we understand that for every area worth being in, there is more than one product to meet your needs. The highly competitive nature of cybersecurity in particular lends itself well to an influx of new vendors meeting in the space and vying for you to get your hands in their consoles. Why sell yourself short and swear that only one vendor has the 'best' product? We are not talking about your favorite brand of sneakers, after all.

Keeping focus on only a single product 'puts the blinders on' in terms of evaluation criteria. Some vendor products are fantastic in some areas, but miss the mark entirely in others. For example, a tool's threat intelligence capabilities are more critical than ever as quick analysis of security posture becomes more important. Some products have no capability here whatsoever.

Knowing where some products excel versus others is a critical piece of any pilot program and may even require an investment in more than one single scanning tool. You will encounter situations where false positives need to be validated. Products which excel at network vulnerability scanning are commonly prone to false positives with web applications (eg. blind SQL injection or cross-site scripting discoveries) which will need to be validated by a proxy web tool. Aside from manual testing, it is always worthwhile to have an alternate tool to validate these findings.

DEFINE THE SCHEDULE AND STICK TO IT

Vulnerability Management programs only truly work when they are predictable. The most obvious point here is that the sooner findings can be delivered to the appropriate Asset Owner, the better. Aim to give appropriate time for engineers to include any new pieces of software into the testing process, get any new code changes into the pipeline early, or seal up any configuration changes before a malicious party takes advantage. As we all know by now, nothing goes out to production untested.

In addition to the obvious points, keeping a routine schedule helps all parties know at how, and with what frequency, to expect hearing from you. Developing the schedule early gets everyone involved in the routine. Aligning that routine with a championed policy is even better to establish its legitimacy. After all, being told a change needs to take place and actually acting on the request can be two separate and distinct things.

What this means for the VM teams out there is that you need to determine at an organizational level what you are scanning on weekly, monthly, or quarterly intervals, and who needs to be notified of the activity. Performing scans without letting Asset Owners know is typically considered a bad practice. Next, establishing remediation timeframes which are appropriate for your organization based on severity (eg. Critical findings resolved within 7 days).These timeframes should be established well in advance and made known. Finally, determine when remediation scanning will occur to validate if any changes are effective, and ensure the Asset Owners are aware of when and how to notify you that it is time to re-run a scan.

Aside from vulnerability scans, configuration and compliance management shouldn't be forgotten. At this point, all federal agencies must align with a configuration baseline such as DISA STIG or CIS Benchmarks. Knowing that automated systems exist on the network to enforce these settings is one thing, but performing periodic checks to ensure compliance is another. What if machines are placed in the wrong OU and not receiving Group Policy settings? What is your organization's percentage of tolerable deviation, and at what point do engineers act to get machines back in line? How long do they have to act on the findings? These are critical questions which should be ironed out well ahead of time.

SET REALISTIC AND MEASURABLE GOALS

An unfortunate truth for all organizations is that there is no such thing as an invulnerable network. This can be a hard pill to swallow for some in senior leadership, since the expectation for private and public sector environments alike is that there be no single vulnerability that can lead to compromise. In reality, if there were such a thing as a perfect network, everyone would be doing it, and cybersecurity as an industry wouldn't exist!

What is key is to set realistic and measurable expectations, understand your organization's security goals, and put emphasis on prioritizing your findings. One of the easiest ways to convey value in any program is to find metrics which are effective in communicating and driving the program. This helps to identify that the program is successful, while setting a real goal to strive towards.

Metrics can be notoriously difficult to establish for Vulnerability Management programs. The reasons vary, including the fact that CVEs are published daily, vendors are not in alignment with severity ratings, or time frames in which scans are run could change results significantly. Try reporting progress to senior leadership the day before versus the day after Patch Tuesday! Defining real, actionable metrics which steer the security program is the key to success in reporting.

As mentioned earlier, understanding your organization's processes is key to understanding the 'pulse' of your environment. Identifying the metrics which convey value to your stakeholders is subjective and requires clear context. For example, knowing the total number of Critical and High vulnerabilities across the board absolutely has value, but keeping numbers on Criticals/Highs which have existed on the network for over 30 days is much more impactful.

Find out what is most important for your organization and determine a way forward to report on it!

METRICS TO CONSIDER FOR YOUR PROGRAM

TOTAL HIGH/ CRITICAL VULNERABILITIES OLDER THAN 30 DAYS

If a host has a vulnerability which is highly scored and has existed longer than 30 days, it is likely outside of your organization's patch cycle.

PATCH MANAGEMENT EFFECTIVENESS OVER TIME

Similar to above, but broader in scope. The total percentage of vendor patches successfully deployed between patch release and the conclusion of your patch cycle.

TOTAL BASELINE COMPLIANCE PERCENTAGE

A snapshot in time of how compliant your organization is with DISA STIG/CIS Benchmarks, or another configuration baseline.

TOP 10 EXPLOITABLE HOSTS ON THE NETWORK

A list of the most vulnerable hosts, as determined by your primary scanning tool or analysis.

MEAN TIME TO REMEDIATION

The mean time between discovery of a category of vulnerabilities on your network, and when it was found to be resolved.

CONCLUSION

Establishing an effective Vulnerability Management process is undoubtedly difficult and goes beyond simply deploying patches. There are equal parts balancing technology, effective communication, and diligent reporting which make the process function properly.

Much of this requires continuous improvement and can never be ‘set it and forget it’ despite initial expectations.

Adopting lessons learned from others experienced in the space as well as with your own teams is the best step towards refining this process, hardening your agencies network, and keeping you a step ahead of those pesky hackers!