

# Integrating Vulnerability Assessment and Remediation

## Guidelines to Maximize Performance and Benefits

In this article, Matt Mosher, Senior Vice President of Americas at Lumension Security will outline the process for successfully integrating vulnerability scanning and remediation capabilities to ensure organizations maintain a secure environment while complying with internal and external security policies.



## Integrating Vulnerability Assessment and Remediation

Over the last several years the explosion of vulnerabilities across all platforms and the shrinking exploit window has left traditional IT security and IT operations teams in a bit of a quandary.

Historically the two teams have been separated by a line akin to the one between church and state. The IT security team is tasked with ferreting out an increasing number of vulnerabilities that could potentially leave the infrastructure exposed. Once they've come up with their laundry list of problems they lob them over the fence to IT operations on the other side. IT operations is then asked to address these issues in between all of the other day-to-day activities involved in keeping the infrastructure running. That may have worked in the past, but today's problem is that security's laundry list continues to lengthen. Over the last three years Windows vulnerabilities have increased by 75 percent and Macintosh holes have skyrocketed by 228 percent, according to research done by McAfee. Meanwhile, the countdown to fix these flaws has been shaved to nearly nil.

"In 2006 we've seen a significant rise in attacks that take advantage of zero-day vulnerabilities, leaving a user or system unable to defend against the attack since no patch is available," noted Marcus Sachs in the end-of-year SANS Top 20 Report for 2006. So not only must IT operations staff fix more problems, but they also need to mend them in a shorter timeframe—all while still maintaining the same level of system availability and reliability as before.

Obviously, something's got to give, and it shouldn't be the security of the systems. Many experts believe that the only way to adapt to the new threat landscape is to develop a proactive set of methodologies that better integrates the two sides of the fence, eliminating the "us and them" mentality that is so pervasive in IT security and operations relationships at this time.

"IT organizations need to become more effective at running cooperative processes across IT security and operations," wrote Mark Nicolett and John Girard in a Gartner report. "The elimination of desktop, server and network vulnerabilities requires a coordinated effort between the IT security and operations groups."

### No More Scan-and-Patch

The first step to establishing a more cooperative relationship between IT security and operations is to change the organizational mentality about vulnerability scanning and remediation. Part of the reason why the old model isn't working anymore is because it was never an efficient way to run vulnerability management program in the first place, says Paul Zimski senior director of market and product strategy for Lumension Security.

"What you ended up getting into is this constant scan and patch syndrome, where you have one team scanning, another team patching, the other team scanning. It is sort of the rinse-wash-repeat cycle," he says "You're constantly playing catch-up, you're constantly chasing your own tails, finding new and resurrected old problems and hoping they get resolved."

It is imperative that organizations move away from the scan-and-patch mindset. Not only is it a reactive method of security, but also not every problem can be fixed with a patch. Some may be fixed through a patch, but others problems might best be solved through a configuration change or a policy change. Because of this, administrators need to develop the approach to these risks into a process.

Instead of chasing down each individual vulnerability one-by-one, this process-oriented approach should focus on enforcing policies that mitigate risks to the organization's assets, prioritized by system criticality and the importance of associated business needs. Organizations need to ask themselves what desired state of security they wish to enforce. By focusing and calibrating resources on this single issue, they can achieve a higher level of efficiency with fewer resources because they don't have two different teams finding and enforcing different problems without any common ground.

This increased level of efficiency should help organizations reap the reward of an overall infrastructure that is more hardened against attacks. In fact, a recent Gartner report noted that implementing an integrated vulnerability management program can help to reduce successful external attacks by up to 60 percent.

A vulnerability management program will vary from business to business, but there are a few

traits common to the best. First, the organization must involve the right stakeholders throughout the entire process. Second, it must set a mandatory security baseline and policies to enforce them. And third, it must utilize tools and methods that will enable all IT groups to work cohesively in maintaining the baseline.

All three of these developmental elements can go a long way toward achieving the ultimate goal of bringing risks down to a level that the organization can live with. In the end an organization needs to come to terms with an acceptable level of risk, one that balances the health of the network with the health of the business.

### Stakeholder Involvement

In order to do it right, whoever is setting mandatory baselines and policies must not only understand the business, but also how IT infrastructure enables the business. Because no single person should be expected to have that level of understanding all on their own, it is best to organize a committee with a diverse membership to drive the vulnerability management program's development. Non-technical representatives from various business units can provide insight into the most strategic divisions and business processes. Members from IT operations can shed light on which systems directly enable those key processes. And IT security members can inform the committee on how to balance the availability and effectiveness of those systems against the threats from the outside.

All of these insights together should help the committee to develop a minimum level of security that the organization is comfortable with and to begin defining IT policies to ensure this baseline is maintained.

Once the initial work is done, the committee may want to meet on a periodic basis to reevaluate business priorities and the threat landscape to ensure that the chosen level of risk and policies are still in line with expectations across the organization.

This committee will lay the foundation for the vulnerability management program, but more cooperation is necessary from those actually implementing and enforcing policies. A smaller working group can help facilitate this. While this group will

still need a diverse set of stakeholders, its size can be scaled down. This group should be composed of more technical members than the larger committee. These professionals should be able to come to a consensus as to the nuts-and-bolts plan for shielding or mitigating risks.

More informal than the committee, this group can be a good liaison between IT operations and security to keep the communication flowing. This is critical once the baseline and policies are set and the two teams must get their hands dirty to enforce them.

### Baselines, Policies and Methodologies

When developing a security baseline and associated vulnerability management policies, it is important to operate under the assumption that the business isn't seeking perfection. The goal isn't necessarily to lock things down into this magic state. It's just to mitigate enough risk that you are providing a good balance between security and business enablement.

Many organizations collectively have some idea of a minimum acceptable level of security running around in the back of the mind of their leadership. The vulnerability management committee should be able to help these leaders articulate their ideas and then come to a consensus about the levels of risk they are comfortable accepting. Once they have done that, then they can develop baseline policies outlining when and where these risk levels should be maintained.

A vulnerability management program can't get off the ground without that baseline and those policies. Similarly, though, these standards mean nothing if the IT shop can't reliably enforce them.

The initial ramp-up phase of enforcement may seem a Herculean effort. Undeniably, it will be a lot of work, but the eventual payoff will be a much easier maintenance load in the long run. Once you get to that point of vulnerability management what you are really doing is spending your ancillary efforts on what's come up new and not spending too much time on old threats. It becomes challenging to address emerging threats if organizations don't have a hold on what they're already dealing with.

One of the most difficult logistical problems start-

ing out during the ramp-up phase is that often the systems most at risk are the ones the organization can least change. For example, an organization can't install a patch on a back-end financial system without considerable planning and testing. If there is a critical vulnerability on that system, then it might make sense to make some kind of low-impact configuration change that could lower the severity of the vulnerability to a level accepted within the baseline.

It is up to IT security and operations to be pragmatic and determine the methods by which they can realistically solve those types of problems. As the teams continue to work together to enforce policies, the procedures they agree upon will eventually gel into an overall vulnerability assessment and remediation methodology that works for their business. The more they refine this methodology, the easier it gets to manage vulnerabilities holistically.

### Tools To Aid The Process

Of course, in order to truly hone an auto-enforceable environment an organization can't depend on policies and processes alone. It also needs tools that can facilitate those best practices.

One of the fundamental dilemmas facing organizations in the process of integrating vulnerability assessment and remediation is the fact that most tools were developed in specialized silos borne out of that old-school separation of church and state. Analysts with Gartner particularly find fault with comprehensive assessment tools, which they accuse of finding problems with little thought put into fixing them.

“Although the ability to discover and evaluate the security state of systems is required by the IT security organization, the output of vulnerability assessment tools is overwhelming and is not organized properly to drive the work of mitigation,” Gartner analysts wrote in a recent report. “Vulnerability assessment tools need to provide better analysis and guidance related to mitigation actions that will eliminate the largest number of critical vulnerabilities.”

On top of this, assessment and remediation tools also have a clash of nomenclature. Because these sets of tools grew up separately, they aren't built to speak in the same 'language' about spe-

cific vulnerabilities. In other words, most vulnerability assessment tools refer to a single vulnerability with vulnerability codes commonly used by security professionals while most remediation solutions will refer to that same vulnerability with completely different vulnerability codes used by operations staffers. Rarely are these codes cross-referenced.

Again, Gartner emphasizes that these tools must bridge that gap to enable better cooperation between the two teams. “Vulnerability assessment products should evaluate an environment with respect to security configuration policies and provide a cross-reference of associated vulnerabilities,” Gartner's analysts wrote.

Ideally, then, an organization should look for an integrated assessment and remediation solution that links nomenclature and organizes assessment reports in such a way that both user groups can execute their functions seamlessly. This involves a truly integrated solution where from a single interface you can really get a baseline understanding of your entire environment, identify where the biggest security areas are, and make informed decisions about what you want to resolve and enforce.

Such a tool set can also go a long way to enabling compliance efforts. Right now, many enterprises are having a hard time muddling through comprehensive vulnerability scanning reports and marrying them with often-incomplete remediation reports and presenting them in an understandable fashion to the auditors.

“You can't get true compliance reporting from separate scanning and patching technologies because you're only getting a portion of whole the situation from each tool,” Zimski says. “You need to get a single compliance report based off the two technologies that can composite the network and agent centric views in a fully-integrated solution.”

That way, a business can not only show the regulators that it knows where the vulnerabilities are, but also what it has done to mitigate risk posed by them.

### Synergy of Integration

By leveraging these integrated technologies and

implementing a holistic methodology to managing vulnerabilities, organizations can encourage their IT security and operations staffs to work together. This can help break the vicious and reactive scan-and-patch cycle that too many businesses remain mired in today.

In the end, the best implementation of these strategies will combine assessment and remediation to create a vulnerability management program that is stronger than the sum of its two parts.

“When you take vulnerability assessment and remediation and combine the two, you really get something new,” Zimski says. “It is a different way to bring the stakeholders in an organization together, working more cohesively and collaboratively on fixing a problem. And when you get that, what you end up having is these strong baselines that are enforcing your policies as well as a rapid response for dealing with emerging threats.”

**Lumension Security™, Inc.**  
15580 N. Greenway-Hayden Loop, Suite 100  
Scottsdale, AZ 85260

[www.lumension.com](http://www.lumension.com)