White Paper

Getting the Most Value from Your Vulnerability Management and Compliance Programs

Overview

Enterprise Vulnerability Management (VM) and Compliance programs reach their full potential when they are built on well-established foundational goals that address the information needs of all stakeholders and tie their output back to these enterprise goals. Today's enterprise-class, state-of-the-art VM and configuration auditing solutions may well be up to the task of supporting these programs, but technology is only one essential ingredient. Effective programs are also supported by robust workflow processes that cross organizational boundaries to implement a "closed-loop" model, spanning detection through remediation. Overcoming typical obstacles such as organizational resistance, incomplete coverage of your network and gaps in measurement are keys to program success.

As a CISO/CSO/VP of Security, anticipating these obstacles and planning how to deal with them will determine whether or not your VM or Compliance program will meet the expectations set by your enterprise. We discuss several solutions to the most common problems encountered before, during and after the initial deployment of your VM or Compliance solution. Careful consideration of these items will help to make your VM and Compliance program more effective.

Revisit Your Program Goals

Your VM or Compliance program is well underway—you've installed the technology, trained your staff, and are even generating some reports and metrics. But the pace of your deployment has slowed down. It's now time to review the reasons you implemented a VM or Compliance solution in the first place. Are you seeing the results you anticipated?

An ideal VM or Compliance program should:

- Scan all of your assets at a frequency that allows rapid detection of new vulnerabilities, rogue devices, and compliance violations, based on the criticality of those assets to your business
- Have no impact on production operations
- Have content that is continuously updated as new vulnerability checks and compliance coverage are developed
- Provide actionable reporting across all organizational levels and groups
- Be fully integrated with remediation and verification processes and workflows to enforce accountability within the program
- Provide accurate and objective measurements of risk across your enterprise and show reduction in risk over time.

In short, your VM or Compliance program must be viewed by executives, operations staff, and other stakeholders as the source of truth that measures the vulnerability and compliance posture of your entire organization; and a cornerstone of a unified security architecture that fully supports enterprise risk reduction efforts.

It's About Reducing Risk

The overall effectiveness of your VM or Compliance program will be measured primarily by the reduction of risk within your organization. Because risk is inherently intangible and not absolutely quantifiable (until an incident or event occurs), it is a complex and difficult metric to calculate. Effective measurement of risk must bring together several components, including the adequacy and frequency of vulnerability or compliance scanning, quality and timeliness of reporting, and effectiveness of followup remediation and verification actions suggested by the output of the VM/Compliance tools and processes. Large organizations with complex IT departments commonly experience inconsistencies or gaps within these components and associated data reconciliation problems, making the performance of risk reduction efforts more difficult to evaluate.

Consider Your Scanning Regimen (Coverage, Frequency and Depth)

From a coverage perspective, are you scanning everything you should be and at the appropriate frequency? Remember, your network is only as secure and compliant as the least secure asset connected to it. Enterprise VM and Compliance solutions provide automated scanning, and many companies configure these solutions for continuous scanning of their entire enterprise. However, without a complete understanding of all the networks within your enterprise, you may not be covering all known assets, let alone discovering new

ones. Integrating your VM and Compliance tool with a robust and reliable asset management system—ideally through automated means—will help to ensure you are scanning all the networks in your enterprise.

Many organizations lack asset management systems that can provide a reliable source of configuration data for the VM or Compliance solution. In these cases, router and firewall configuration files or the network engineering group can provide a comprehensive list of networks to be scanned to assess their vulnerability or compliance posture. Be aware that in some cases, network devices may block scan traffic to connected endpoints, resulting in interrupted scans that contain incomplete vulnerability and compliance information for filtered endpoints. Discovery of new or transient assets beyond just servers and laptops is most effectively supported using a solution based on agentless technology.

Periodic reviews of scan results might reveal seemingly empty networks or networks comprising hosts without any reported vulnerabilities or compliance issues. These are likely indicators of filtering, either at the network or host level. While firewalls are an important component of defense-in-depth security, they should not be configured to interfere with legitimate security or compliance evaluations. A vulnerability or compliance issue that has been blocked from detection by your VM or Compliance solution still exists and presents undesirable risk to an organization.

Frequency of scanning is another important aspect to consider when measuring the effectiveness of your program. Configuring your VM or Compliance tool to scan a network once a year is less effective than performing weekly or daily scans, and can result in delayed detection of important vulnerabilities or compliance issues. With most automated tools, updating the solution to include results of the most recent vulnerability and compliance checks is critical.

Without a consistent update process, the technology will not be able to detect the latest vulnerabilities or compliance issues. From a quality assurance perspective, these updates should be treated much like antivirus signature file updates in that they should be tested prior to being used on critical production networks and systems.

Depth of scanning refers to whether or not you are performing authenticated scans, i.e. using credentials to access the internal configuration of systems on your network. While authenticated scanning is the norm in compliance and configuration auditing, many VM programs have not yet progressed to this stage. Unauthenticated vulnerability checks are generally not intrusive. In the unlikely event that such scans disrupt production services, this should be logged as a vulnerability on the affected system. After all, any device or malicious user who sends identical traffic would have the same undesirable effect on the affected systems. Anomalous or unanticipated network traffic should never be allowed to have a deleterious impact on any system.

However, the difference between non-authenticated vs. authenticated vulnerability scans can be likened to the difference between your doctor making a diagnosis merely based on external observations of symptoms vs. performing a diagnostic test such as an MRI or CT scan. Scanning with credentials is necessary to identify all the vulnerabilities present on a system. When you first activate authenticated scanning, be aware that your VM solution will present you with significantly more information (and vulnerabilities). This can be overwhelming for your security team, and certainly discouraging for individuals responsible for remediating the vulnerabilities on affected systems. Take appropriate steps to work with program stakeholders to help them prioritize remediation efforts.

Address Specific Information and Reporting Needs of Stakeholders

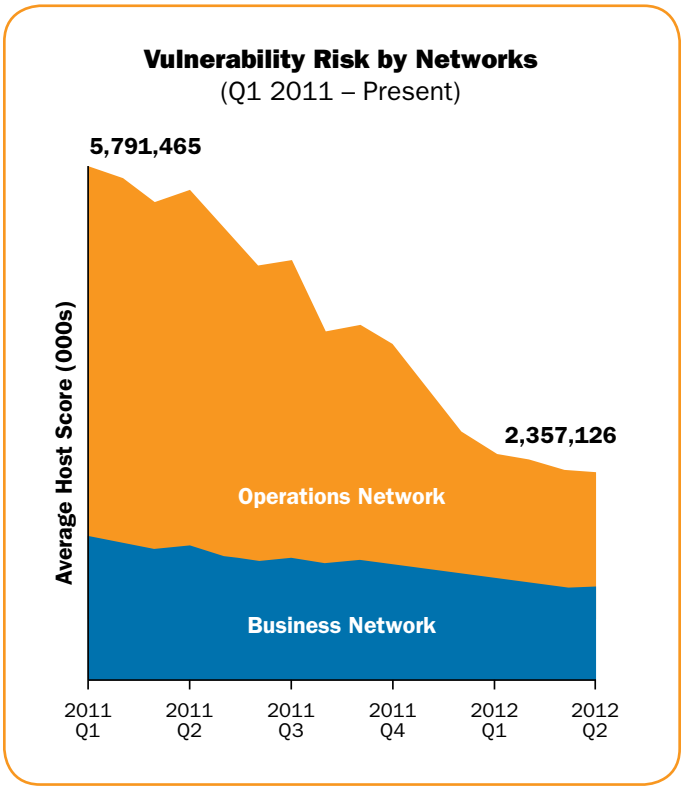
Audience-specific reporting is critical to the continued success of VM and Compliance programs and their effectiveness as a key part of your organization's overall risk management strategy. There are multiple consumers of vulnerability and compliance reports, from security and operations practitioners responsible for remediation of any findings to executives and even your Board of Directors. Each group will likely require different information, and it is important that each type of report provides meaningful, actionable data to its target audience. Your program should provide targeted and actionable information to stakeholders at the frequency they demand.

Top 10 Vulnerable Hosts (point in time)		
Hostname	Score	Number of Vulnerabilities Present
oldmail.example.com	402,487	16
sql72-old.example.com	363,889	12
hmi4.ops.example.com	318,050	14
laptop34.clients.example.com	226,538	8
dev82.example.com	192,416	8
legacydev.example.com	185,598	10
guest734.example.com	136,283	6
finance23.example.com	111,320	12
cardreader-tampa.example.com	103,208	2
win2k.example.com	9,190	14

Interactive Reports Help Prioritize Remediation for Operations Staff

Security and operations staff need access to the technical details of the vulnerabilities and compliance findings for which they are responsible to remediate. They will generally need this information in a format that allows correlation by system, system type, and vulnerability—this is where automated, interactive reports can provide a benefit. With detailed vulnerability or compliance information at hand, security and operations can determine the priority of remediation, and get timely feedback and objective verification of their efforts.

Security managers generally require more analytic reports that summarize the state of vulnerabilities or compliance posture across classes of systems or networks. For instance, a manager might want to compare the set of vulnerabilities in the San Francisco office with the set of vulnerabilities in the Toronto and Munich offices to determine whether or not remediation efforts are being performed consistently across the organization. It may also be useful to compare the compliance posture of UNIX servers to Windows counterparts, to see which systems are being patched in a more timely manner. Finally, a manager might want to look at the vulnerability scores of the entire organization over time in order to determine the overall effectiveness of the configuration and patch management programs.



Analytic Reports Show VM or Compliance Posture Across the Enterprise

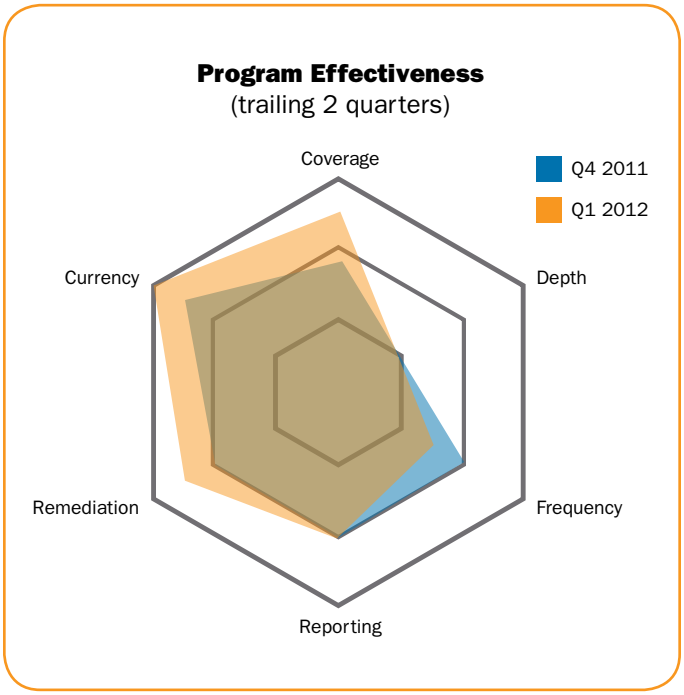
For executives and board members, simpler reports summarizing the state of the VM or Compliance program expressed as a risk or program maturity metric are beneficial and are often included as part of an overall security or IT briefing. When included in other business operations reports, this information must be high level, allowing at-a-glance understanding of the overall risk and compliance posture. In addition to providing a quick answer to the question "How secure and compliant are we?", the accuracy of the information must be unassailable in the event questions arise.

"Traffic-light" reporting (where the overall posture is given a red, yellow, or green rating) is common, however this simple signal should be accompanied by high-level summary or component metrics, especially showing change in risk or compliance posture over time. For example, the overall status of the program, represented by a single color could comprise underlying coverage, reporting, and remediation metrics, each of which contribute to the overall rating.

A more comprehensive way to represent the effectiveness of your VM and Compliance program is to use a capability maturity model, similar to the SEI-CMM. For VM and Compliance programs, six key metrics can be used to assess effectiveness. We have already discussed scanning regimen, and three of the metrics refer to that—coverage, frequency and depth. The other three metrics are reporting, remediation, and currency. While the scanning regimen metrics can be easily derived from your VM or Compliance solution, the others can be more subjective and will require alternative and possibly more manual methods of measurement, e.g., a simple 1-5 scale that answers the following key questions for each metric:

- How timely, targeted and relevant is the information you are providing to your stakeholders?
- Are VM and compliance findings being remediated in a timely fashion?
- How current is your VM and Compliance solution with respect to software releases and content?

A spider graph is an effective visual tool to indicate how well your program is performing on each of these six key metrics, and can also be used to track improvements over time.



Simplified Reporting Provides a Quick Snapshot of Overall Program Effectiveness for Executives

Report generation needs to be automated. This saves valuable time and effort, and results in more objective reports with greater accuracy. Of course, reports must be reviewed prior to distribution, to ensure accuracy and anticipate any questions that might ensue, especially from management and executives. A small incremental investment in developing, deploying, and enhancing automated reporting will provide significant return in terms of building increased credibility and lowering the overall cost of your VM and Compliance program.

Break Down Organizational Barriers

Not everyone in your organization will be ardent supporters of an enterprise VM or Compliance program. Operations teams may view the remediation instructions output from the VM or Compliance tool as an inconvenient increase in their already heavy workload. Staff reluctance to support program efforts can manifest itself in various ways, including refusal to allow scanning on networks they "own", limiting scan coverage or blocking scan traffic at network perimeters and endpoints, or complaining about service disruption from scanning—these are all common reactions from groups who may be unconvinced about the value that a VM or Compliance program can bring to their portion of the organization. Adopting appropriate strategies may help minimize some of their concerns:

1. Engage the network operations and engineering teams in designing the VM or Compliance solution, in particular to address concerns about the impact of scanning on the network. Today's local-area networks provide more than sufficient bandwidth to support continuous scanning using most automated VM and Compliance tools. For low-bandwidth or high latency wide-area networks, the solution needs to be configurable to avoid interference with other network traffic by limiting the speed and/or frequency of scans.
2. Immediately after initial deployment, establish an on-call team (with representation from the Security and IT Operations teams) to provide first-level response to any suspected disruption to operations from scanning. This team should be available around the clock, even when scanning is not active. Problems may not be immediately detected after a scan, and then may require some time to troubleshoot, especially to provide the necessary evidence and assurance that the root cause of the problem isn't due to scanning.

3. As you expand your deployment, define the standard set of VM and compliance reports you'll provide to each constituent group participating in the program, as well as consistent and measurable processes for scanning, detection, reporting, remediation, verification, and handling of exceptions and waivers. Enlist sponsorship from your organization's top-level executives as you introduce and roll out the program to each constituent group, and be prepared in advance to deal with their potential objections. The role and profile of the security team within the organization and your corporate culture will determine whether a "carrot" or "stick" approach will work best.
4. As each successive group is deployed, give the respective operations teams direct access to the output. Allow them to view results of scans against their own assets directly (partitioning the data as appropriate). Provide a formal mechanism for feedback and questions relating to scans, and provide a method to determine the status of the automated scans at any time. This will allow the teams to eliminate scans as the source of any operational issues. Provide enough specifics to permit them to evaluate the VM and Compliance solution as the cause of an anomaly, unlikely as that might be.
5. Give the operations teams reports showing the effect of their remediation efforts. Ideally, these reports will be available to them on-demand through a self-service portal. Allow them to compare their results to others, and to measure progress over time.
6. Ensure that recognition for vulnerability reduction and improvement in compliance is shared with the operations teams who are remediating the vulnerabilities or compliance issues.
7. Provide a method for operations teams to voice concerns and report suspected issues with vulnerability and compliance scanning (e.g., false positives).

Equip and Support Your Security Team

Your security team might itself present an impediment to achieving full maturity of your VM and Compliance program. Does your team have the right skills and are there enough people to do the job? Security teams report generation needs to be automated. This saves often underestimate the effort needed to maintain the VM or Compliance solution so it stays aligned with changes in the network configuration, regulatory policy, or internal IT change management procedures, which can slow progress towards full implementation. Following are some recommended practices for you and your team to adopt to improve the effectiveness of your VM or Compliance program:

1. Ensure adequate resources are assigned to deploy and maintain the solution. Hardware occasionally needs replacement, software needs updating, and changes in the network design require adjustments to the configuration of the tool. In addition, new vulnerability or compliance checks require updates.
2. Ensure staff members who perform scans and prepare reports are fully trained in the tool's use. For example, introducing new vulnerability or compliance checks often causes a spike in the reported number of vulnerable or non-compliant systems. These spikes may skew trending reports, and without proper context stakeholders could misconstrue that the organization has taken a step backwards in terms of its risk reduction efforts.
3. Position your team as "security analysts" who can advise program stakeholders on severity of vulnerabilities or compliance issues, assist in prioritizing remediation efforts, and research additional information when asked. This will increase the team's overall job satisfaction and contribute to raising the profile of your program within the organization.
4. Form a productive working relationship with your solution vendor, to raise requests for new features, and report and resolve false positive conditions, which can and do occur.
5. Develop analysis and training programs so that personnel responsible for gathering and analyzing data from the VM and Compliance tools do so in a consistent, repeatable, and correct manner.

Adding More Value

The most effective VM and Compliance programs are characterized by continuous improvement, so that increases in capability and functionality are part of the programs' natural evolution, and not just a one-off effort. Examples of these natural progressions include integrating additional data sources with the existing VM or Compliance solution and using the data to provide reports that influence business decisions:

1. Adding asset management data permits correlation of system age and other system attributes with overall organizational risk. Older machines are more difficult (and more expensive) to maintain and keep secure.
2. Tying business function to specific systems can provide business units an easy way to monitor their overall vulnerability or compliance risk, making it easier to justify and prioritize investments in IT security.
3. Providing multiple views of vulnerability and compliance exposure through strategic placement and configuration of scanning devices will enable fine-grained examination of risk which would help in incident response planning as well as prioritization of remediation.
4. Tying DHCP leases to the VM tool via API calls can provide a "scan on connect" service that will automatically scan new devices. Passing the results of the scan to a network management system can provide an enhanced form of network access control, where systems with specific vulnerabilities can be quarantined until they are remediated.

Tie Output to Program Goals

Once your organization is comfortable with automated and continuous VM and compliance scans and understands the value of information in the reports, you will be ready to extend your program to support establishment and measurement of performance goals. Remember that one of the primary goals of a VM or Compliance program is to measure the risk of vulnerabilities and misconfigurations within a set of systems. When the program is providing accurate, actionable data that is being used by operations and security staff to guide remediation activity, you can begin to use the tools and processes in security planning. By creating time-based trend reports using the metrics established through your program, you can set risk reduction goals and track progress towards their achievement.

Take Your Program to the Next Level

The most effective VM and Compliance programs continuously adapt to remain fully aligned with risk reduction goals that evolve over time, whether due to regulatory changes, M&A activity, new threats, or other factors. Adopting a deployment methodology that incorporates continuous program improvement will enable your organization to improve security and reduce risk through more rapid and accurate identification and remediation of vulnerabilities and compliance findings in critical systems.

As your VM or Compliance program matures, you may find it difficult to establish meaningful goals that represent concrete improvements to the program. In this case, it may be useful to obtain external input and validation of proposed changes. Your VM and compliance tool vendor might suggest additional products or services, or encourage you to participate in information exchanges with other customers who might be able to provide external guidance. Particularly with VM and Compliance solutions, best-in-class programs often evolve to a point where external collaboration and information sharing can bring a fresh perspective to take them to the next stage of maturity. Don't be afraid to find out what colleagues in other organizations are doing, and to evaluate whether their practices can help your program.

About the Authors

Bill Rudiak is nCircle's Director of Professional Services, responsible for definition and delivery of the company's consulting and training programs. Seth Bromberger is principal of NCI Security LLC, (www.ncisecurity.com), a full-service consulting firm dedicated to protecting critical infrastructure across multiple sectors including energy, oil & gas and finance.

About nCircle

nCircle is the leading provider of Information Risk & Security Performance Management solutions to more than 6,500 businesses and government agencies worldwide. nCircle solutions enable enterprises of all sizes to 1) automate compliance and reduce risk, and 2) measure and compare the performance of their IT security program with their own goals and industry peers. nCircle solutions may be deployed on a customer's premise, as a cloud-based service, or in combination, for maximum flexibility and value. nCircle has won numerous awards for growth, innovation, customer satisfaction and technology leadership and has been ranked among the top 100 best places to work in the San Francisco Bay Area. nCircle is headquartered in San Francisco, CA, with regional offices throughout the United States and in London and Toronto. To learn how you can more effectively protect your company visit us at www.ncircle.com.

nCircle
www.ncircle.com

nCircle is the leading provider of Information Risk & Security Performance Management solutions to more than 6,500 businesses and government agencies worldwide. nCircle solutions enable enterprises of all sizes to 1) automate compliance and reduce risk, and 2) measure and compare the performance of their IT security program with their own goals and industry peers. nCircle solutions may be deployed on a customer's premise, as a cloud-based service, or in combination, for maximum flexibility and value. nCircle has won numerous awards for growth, innovation, customer satisfaction and technology leadership. nCircle is headquartered in San Francisco, CA, with regional offices throughout the United States and in London and Toronto. To learn how you can more effectively protect your company visit us at www.ncircle.com

Corporate Headquarters
101 Second Street, Suite 400
San Francisco, CA 94105
Tel: +1 888 464 2900
Email: info@ncircle.com

Europe Headquarters
Venture House, Arlington Square, Downshire Way
Bracknell, RG12 1WA, United Kingdom
Tel: +44 (0) 1344 668 600
Email: emea@ncircle.com