Burton IT1 Research
G00226331

Solution Path: Threats and Vulnerabilities

Published: 24 January 2012

Analyst(s): Dan Blum

This solution path helps Gartner clients develop a strategy and program for managing threats and vulnerabilities in their IT environments.

Table of Contents

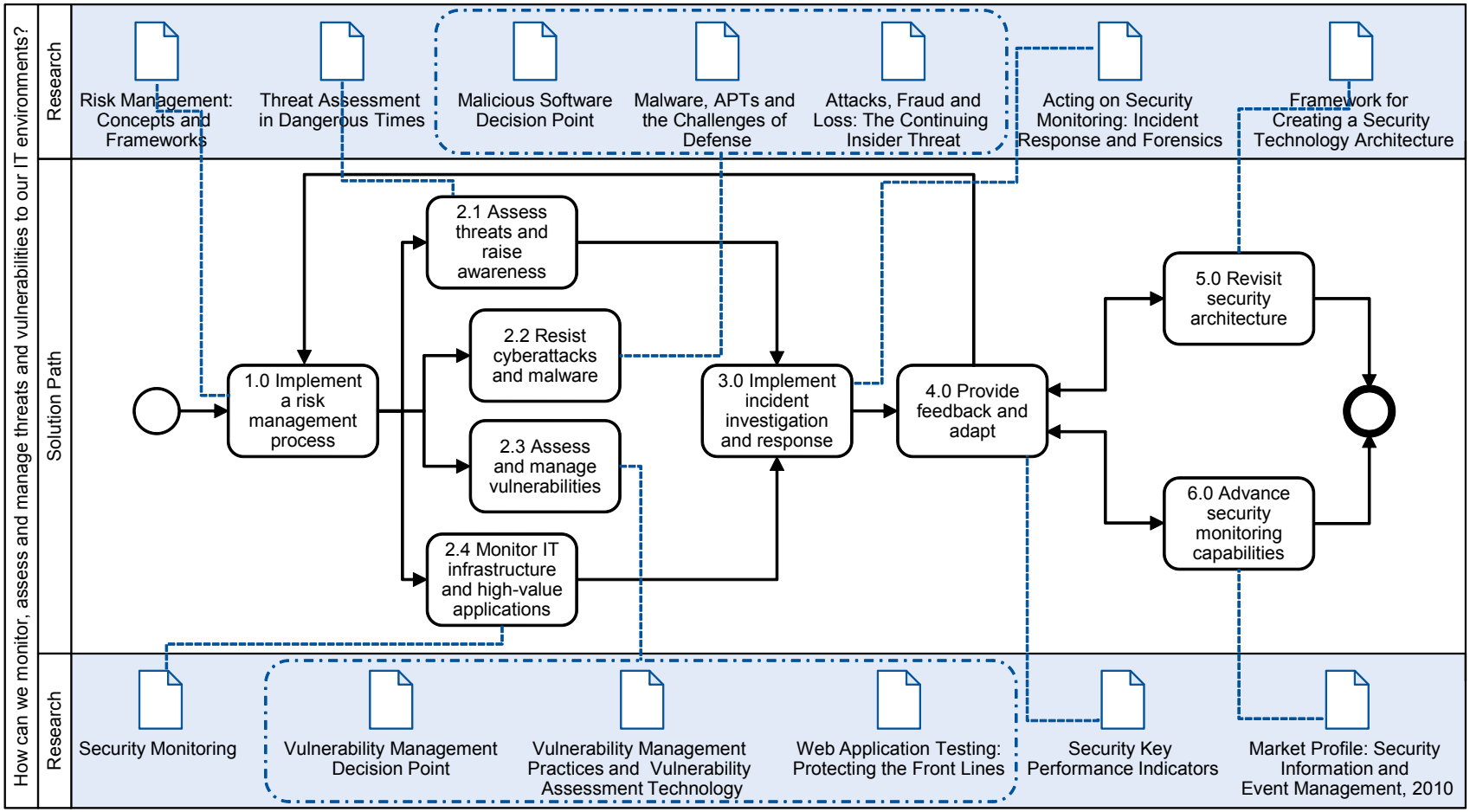
List of Figures

Problem Statement

How can we monitor, assess and manage technical threats and vulnerabilities in our IT environments?

Solution Path Diagram

Figure 1. Managing Threats and Vulnerabilities



Source: Gartner (January 2012)

What You Need to Know

Simply from reading the news, it's clear that global compliance requirements are increasing and that external threats are becoming more numerous and capable. At the same time, many enterprise environments are becoming more complex, with increased globalization and outsourcing, and this potentially leads to more vulnerabilities and insider threats.

Any organization in any industry needs to make an effort to protect itself against threats and vulnerabilities. However, organizations in the national defense, government, financial services, critical infrastructure, telecommunications or media industries — as well as many other types of organizations that manufacture or develop valuable, proprietary trade secrets and technologies — must recognize that they're at risk of attacks from advanced persistent threats (APTs), such as national intelligence agencies and organized cybercrime groups. Organizations should conduct their security program starting with the assumption that they may — even now — already be compromised by an APT and should make a concerted effort to limit current and future damages.

Gartner provides this solution path as a starting point for implementing a risk-appropriate threat assessment and vulnerability management program in the enterprise.

Solution Path

This solution path provides a step-by-step road map to understanding the problems, solutions and choices required to answer the question: "How can an organization monitor, assess and manage technical threats and vulnerabilities to its IT environment?" Each step recommends general strategies and refers readers to research with more detailed recommendations. Some steps also point to specific Reference Architecture Decision Points, walking readers through a road map of architectural choices.

Implement a Risk Management Process

Because risks are a function of threats, vulnerabilities and consequences, an enterprise threat and vulnerability management program is closely related to the risk management process. However, threat and vulnerability management should operate continuously — providing feedback to the risk management process, as well as providing or supporting operational services (such as protection against malware, remediation of vulnerabilities and investigations of adverse events).

Risk management itself must be front and center to enterprise information security programs. Most organizations should, at least on an annual basis, conduct an enterprisewide risk assessment. Moreover, more limited or localized risk assessments should be triggered by business and IT changes or other events, such as opening a new site, deploying a new e-commerce system or taking on a new strategic outsourcing partner.

Assess Threats and Raise Awareness

Organizations must assess the threats posed by internal or external people. While APTs have garnered considerable notoriety lately, insider risk is also an ever-present danger (see "Attacks,

Fraud, and Loss: The Continuing Insider Threat" for more information). Because a variety of attacks from insider threats (e.g., rogue financial traders) and external threats (e.g., APTs or hacktivists) can credibly cause medium or high consequences, it's important to raise awareness of the risks — not only in the security department, but also across the organization. This is especially true in light of attackers' use of social engineering techniques, such as spear-phishing emails, for initial penetration of the target organization.

"Threat Assessment in Dangerous Times" recommends, at minimum, that organizations understand the threat landscape for their industries or lines of business and gather threat data by participating in information sharing forums. Organizations should disseminate threat data to the groups that need it and should provide actionable instructions. Depending on the risk level and the nature of the business, organizations may also need to organize a dedicated threat assessment team and/or make use of third-party threat intelligence, brand protection services and/or other services. Organizations should also factor the results of threat assessment into protection programs to better understand the likelihood and nature of different types of attacks.

Gartner's threat assessment guidance also advises organizations to participate in information sharing forums, such as the International Information Integrity Institute (I-4), International Security Forum (ISF), or the various Information Sharing and Analysis Centers (ISACs), to learn of the threats that peer organizations have or haven't discovered. If appropriate, this information can be used to help justify security budget and staffing to progress the IT security architecture from one that just deals with basic threats and vulnerabilities to one that also leverages increased resources and/or advanced technologies for its defense.

Resist Cyberattacks and Malware

Threats use direct cyberattacks (hacking), social engineering (e.g., phishing) and malware to exploit vulnerable systems or unaware users and to accomplish their intents. They also sometimes employ physical attacks, such as stealing a mobile computer or backup media. One thing that's clear from "Threat Landscape" is that, even if organizations aren't already themselves the subject of targeted attacks, by tolerating vulnerabilities and allowing malware into their IT environments, they may become targets of opportunity. This is due to an increasingly collaborative cybercrime environment in which some hackers specialize in writing malware, while others specialize in exploitation. Thus, if one of your systems is compromised by spyware, your users' credentials may be sold in an underground forum (server root accounts fetch a higher price).

Resisting malware, therefore, must be part of most organizations' baseline security defense capability. Typically, anti-malware tools are implemented on most client and server endpoints and in network security gateways. However, planners must make many technical choices, such as whether to layer defenses along diverse infection and exfiltration vectors and whether to emphasize blacklisting, whitelisting, behavioral, reputation and other approaches at a particular layer for a particular use case. To plan an optimized malware defense, see "Malicious Software" and "Malware, APTs, and the Challenges of Defense."

Assess and Manage Vulnerabilities

Vulnerability management also needs to be part of every organization's security program. Organizations should implement vulnerability scanning and remediation for IT infrastructure (e.g., network routers and host operating systems) and for any applications that are in widespread use. Organizations should also include virtual and cloud environments, as well as mobile, wireless and non-PC devices (e.g., printers), in the program.

Vulnerability management tools have evolved from simple scan-and-report mechanisms to process-focused systems that manage the full implementation of technical security policy on host and network devices. But even advanced vulnerability management products may lack an out-of-the-box capability for leveraging detailed context to properly classify vulnerabilities and to prioritize remediation steps.

Thus, if organizations are unwilling to invest in a comprehensive set of vulnerability management tools and processes — or are in the early stages of deploying — technical professionals must do more of the prioritization, triage, testing and classification work manually. In practice, this means identifying high-value systems (note that some regulations, such as Payment Card Industry Data Security Standard [PCI DSS], require vulnerability management) and making sure that all applications on those systems are frequently scanned, updated and remediated using either enterprisewide or point-vendor-supplied solutions. For guidance on how to implement vulnerability management both initially and at an advanced level, see the upcoming documents "Vulnerability Management Practices and Vulnerability Assessment Technology" and "Vulnerability and Security Configuration Assessment Solutions Comparison," as well as "Vulnerability Management."

To expand coverage of vulnerability management, organizations should also deploy perimeter policy validation tools and application security testing tools (at least for critical applications). For more information, see "Tools for Network-Aware Firewall Policy Assessment and Operational Support," "Dynamic Software Security Testing: Web Application Scanning Technology Assessment," and "Web Application Testing: Protecting the Front Lines."

Monitor IT Infrastructure and High-Value Applications

Security monitoring is required to detect cyberattacks, abnormal behavior of privileged users or systems, and much more that may signify a threat or vulnerability is present. The better the monitoring, the earlier the detection and (hopefully) the lower the impact. As with vulnerability management, organizations should start by monitoring IT infrastructure and high-value systems. Enterprises may also have regulatory obligations (e.g., PCI DSS, Sarbanes-Oxley Act [SOX] or Health Insurance Portability and Accountability Act [HIPAA]) to monitor certain types of activity.

Security monitoring is related to operational monitoring and touches virtually every part of the IT security infrastructure. For example, security monitoring must keep track of the malware and vulnerability scanning mechanisms discussed above, and must also consume and record events from network devices, endpoints and applications.

Note that we'll revisit monitoring in the last step, which recommends that organizations continually advance technical security monitoring technologies. This involves processes as well as tools.

Security monitoring requirements must first be specified in policy and tie in with a broader security architecture. Even early efforts should be architecturally cohesive; see "Security Monitoring" for more information.

Implement Incident Investigation and Response Processes

Incidents happen, and organizations must learn from them. As organizations implement security monitoring, they're also more likely to detect the incidents. Once they've detected incidents, organizations may need to investigate and respond. As described in the Assess Threats and Raise Awareness section of this research, organizations should also participate in information sharing forums to learn from incidents that happened to peer organizations.

"Acting on Security Monitoring: Incident Response and Forensics" provides information on how organizations communicate internally, build procedures, identify and train responsible staff, respond to different kinds of incidents, and communicate externally.

Provide Feedback and Adapt

Finally, staff must take feedback from threat assessment, vulnerability management and security monitoring and use it to adapt the security architecture and feed into risk management processes. As part of architecture planning and risk management, periodically revisit the question of whether to take threat detection, vulnerability management and monitoring to a higher (but more expensive) level of sophistication. Metrics are important to the feedback process because they can provide triggers or thresholds for making decisions on when to invoke crisis management procedures or make other significant changes. For more information on metrics, see "Security Key Performance Indicators."

Revisit Security Architecture

Because enhancing an organization's ability to address technical threats and vulnerabilities touches many different points in the IT infrastructure and the organization, planners should also revisit the overall security architecture to help make choices. Even organizations laboring under serious threats don't necessarily require all the advanced technologies. See "Framework for Creating a Security Technology Architecture" as a starting point for reviewing security architecture overall.

Finally, threat and vulnerability management, as well as security monitoring, provides vital feedback to and security programs. As this feedback reaches global security organizations, they must adapt to it.

Advance Security Monitoring Capabilities

Implementing basic anti-malware, vulnerability management and security monitoring (see the Monitor IT Infrastructure and High-Value Applications section of this research) will give organizations some breathing room and significantly reduce their likelihood of becoming a target of opportunity, as well as help detect and respond to attacks that occur. However, some adversaries — such as APTs — are capable of launching repeated sophisticated and coordinated cyberattacks,

social engineering attacks, and targeted malware that may leverage zero-day exploits of as-yet-undetected vulnerabilities. These kinds of adversaries include, but are not limited to, hostile nation-state actors and organized criminal enterprises. Adversaries may already have penetrated your organization and may be operating as insiders, or they may be working as teams and will soon do so.

Organizations at higher risk of APTs include those in the national defense, government, financial services, critical infrastructure, telecommunications or media industries, as well as any other organization with high-value intellectual property or other kinds of assets. Such organizations should make an effort to discover whether they or their peers have been, or currently are, infiltrated. If the attackers make mistakes, then organizations may discover them through routine anti-malware detection and security infrastructure monitoring. But if the attackers don't make mistakes, organizations may only be able to discover them through advanced monitoring technologies, such as threat detection sandboxes, network forensic analysis, network behavior anomaly detection, honeypots, or advanced security information and event management (SIEM) deployments. Some tools (e.g., threat detection sandboxes deployed in an appliance) can be deployed on a trial basis to "test the waters"; others require time, tuning and customization (e.g., SIEM correlation).

For in-depth coverage of SIEM technology, see "Security Information and Event Management Technology Assessment." Note, however, that there isn't a single security monitoring solution; while an SIEM system may perform a critical function as a monitoring hub, a variety of other product categories may be needed. See "Data Loss Prevention," "Selecting Secure Web Gateway Solutions" and the upcoming "Enhancing Security and Compliance with Database Audit and Protection" for more information.

Acronym Key and Glossary Terms

APT	advanced persistent threat
HIPAA	Health Insurance Portability and Accountability Act
I-4	International Information Integrity Institute
ISAC	Information Sharing and Analysis Centers
ISF	International Security Forum
PCI DSS	Payment Card Industry Data Security Standard
SIEM	security information and event management
SOX	Sarbanes-Oxley Act

Regional Headquarters

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Japan Headquarters
Gartner Japan Ltd.
Atago Green Hills MORI Tower 5F
2-5-1 Atago, Minato-ku
Tokyo 105-6205
JAPAN
+ 81 3 6430 1800

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600