Security Monitoring on the Microsoft Enterprise Network

Published: January 2010

The Microsoft Enterprise Network is one of the world’s largest and most prominent networks. Learn how Microsoft monitors the security of its network and responds to malware and suspected intrusions or policy violations.

Introduction

Intended Audience

Technical Decision Makers

Products & Technologies

* Network Access Protection
* Internet Protocol Security
* DirectAccess technology in   
  Windows 7 and Windows   
  Server 2008 R2

The Network Security team at Microsoft is responsible for conducting security monitoring on the Microsoft enterprise network. The team also provides digital forensics for the entire company and conducts outreach with members of the broader information ecosystem in the interest of helping to secure it. This article focuses primarily on how the Network Security team does security monitoring to safeguard Microsoft’s intellectual property and corporate assets.

Structural Organization

The Network Security team is composed of the following three teams:

* **Security Monitoring**. The Security Monitoring team watches over the Microsoft enterprise network. The enterprise network does not include MSN or the other online services. Those networks have their own monitoring team. The Security Monitoring team looks broadly across the enterprise network and identifies anomalies. Where these anomalies involve a machine misbehaving (for example, because of a virus), the Security Monitoring team or the Microsoft IT Compliance team investigates and remedies the problem.
* **Investigations**. If it is determined that a person is misbehaving (for example, someone is trying to get access to the network without authorization or is downloading inappropriate content), the Investigations team steps in. This team is highly skilled in the areas of due process, chain of custody, and preservation of evidence. The team’s knowledge of due process becomes important when the team is involved in an employee discipline matter or when an issue must be referred to law enforcement.
* **Engineering Support**. The Engineering Support team builds tools and keeps the infrastructure running for the Network Security team.

The Network Security team is a part of the Trustworthy Computing Organization at Microsoft. The team has a partner relationship with Microsoft IT but is not part of Microsoft IT. Microsoft IT owns the *preventive controls*—the policies, architecture of the network, how the infrastructure is configured, firewalls, patching, and the Access Control Lists on the routers. The Network Security team owns the *detective controls*. Preventive and detective controls complement each other, but it’s important to have a separation of duties, so the organizations are separated. The first place where the Trustworthy Computing organizational chain and the IT organizational chain meet is at the CEO level.

Corporate Governance Roles

The core activities of the Network Security team involve corporate governance. As the team sees it, corporate governance consists of ensuring that the company:

* Does what it must
* Does what it has promised
* Does what it should

Doing What the Company Must

This category of compliance involves laws and regulations. Sarbanes-Oxley is an example of a federal law that applies to Microsoft and others. The Payment Card Industry Data Security Standard (PCI DSS), which requires certain data-protection standards for credit-card processing, is a regulation that applies to Microsoft in transactions involving the use of credit cards.

“Conducting very intrusive monitoring and investigations might improve security and enable the team to exceed their goals. But if employees feel that they are working in a surveillance state, these measures would be counterproductive.”

Laws and regulations don’t offer much flexibility. If a law or regulation says that a company must do something, it must do it.

Doing What the Company Has Promised

This category of compliance has to do with Microsoft’s own internal policies and standards of business conduct. These policies and standards are essentially a promise to Microsoft shareholders and others about how the company will operate. The company promises that it will restrict the use of the network to acceptable business purposes as it has defined them.

The standard of care required to support internal policies and standards is more self-defined than that of laws and regulations, but there nevertheless is a written policy corpus that the team uses as a basis for their work.

Doing What the Company Should

Ensuring that the company does what it should is a vague requirement. Companies can be held accountable for failing to follow accepted industry practices for protecting corporate assets and customer data, as well as for failing to meet reasonable expectations. Part of the Network Security team’s mission is to ensure that Microsoft meets these expectations.

Since expectations and industry practices continually change, there is no standard reference that specifies precisely what Microsoft must do. The team uses good sense and continually reviews industry best practices.

The Balancing Act

The Network Security team has to comply with laws, regulations, and internal policies, and monitor best practices and industry standards. At the same time, the team has to balance business-agility needs and the needs of Microsoft’s employees and stakeholders. Conducting very intrusive monitoring and investigations might improve security and enable the team to exceed their goals. But if employees feel that they are working in a surveillance state, these measures would be counterproductive. Business agility is also very important. The team does security monitoring to help the business. They don’t want to be a business impediment. Privacy laws also impact the team’s capabilities. The team’s network-monitoring capabilities in the US may differ from its capabilities in other countries due to variances in law.

The Security Monitoring World

Performing security monitoring on any large corporate network is challenging, but Microsoft’s network has unique characteristics that make it even more so. The network is:

* **Large**. There are nearly one million machines on the enterprise network, spanning over 90 countries on every continent except Antarctica. The network contains a great deal of valuable information, ranging from customer data to Microsoft intellectual property.
* **Complex**. Much of the network is centrally managed. For example, all of the datacenter and all of the day-to-day line of business (LOB) applications are IT managed and are fully patched. But a significant portion of the enterprise network is comprised of self-managed environments. This is because product teams need the ability to test on machines with a variety of operating systems, service packs, and patches. Microsoft also has a very large extranet that the company uses to communicate with partners. The Microsoft enterprise network interfaces with a number of partner networks.
* **Dynamic**. The network is continually changing. The most dramatic example involves the fact that groups self-host developmental versions of their own products. The Network Security team sometimes sees completely new protocols appear in network traffic from one day to the next.

Problem Domains

The Security Monitoring team’s work encompasses three domains:

* **IT** **Domain**. The IT domain is focused on machine uptime. Often, what appears to be a security issue is actually a benign malfunction of some kind. In these cases, the team contacts the appropriate people (sometimes this is the owner of the machine; other times, it may be a datacenter operations team) and provides information to help them put the machine back into service.

“The team has developed three different categories of complementary sensors to address the needs of each of the domains. They don’t view any one sensor as being superior to the others. Their goal is to use a mix of sensors from these categories in order to achieve balanced coverage for all three domains.”

* **Compliance Domain**. Compliance-domain issues often involve shortcuts that people take to get some kind of business result. They may or may not realize that the thing that they are doing compromises security and is against policy. There are also cases in which people knowingly violate policy maliciously, but these are much less frequent.
* **Security Domain**. In the Security domain, the team faces determined human adversaries who try to conceal their actions. The team assumes in some cases, without trying to anticipate how, that a person with malicious intent has managed to penetrate all of the preventive security measures. How would the team detect when that happens and how would they figure out who the person was who managed to penetrate all of that security?

Three Categories of Sensors

As the team designs their security-monitoring systems, they differentiate between the three problem domains and make sure that their security-monitoring controls are appropriate for all of them. The team has developed three different categories of complementary sensors to address the needs of each of the domains. They don’t view any one sensor as being superior to the others. Their goal is to use a mix of sensors from these categories in order to achieve balanced coverage for all three domains.

Signature-Based Tools

The base platform is the classic signature-based tools like network-intrusion detection systems (NIDS). These sensors perform pattern-matching on network traffic. When they recognize a bit pattern that’s characteristic of a particular type of attack, they put up an alert and one of the team members responds. These are very good, manageable tools and many of them are enterprise scale. They are also an important foundational layer, because they catch a lot of the problems in the IT and Compliance domains.

Signature-based sensors have two chief drawbacks, however. First, being signature-based, their great strength is in finding things they know how to find. But especially in the Security domain, the team is concerned with novel attacks. Second, these sensors are commercially available, so an adversary could buy a copy, train on it, and learn how to evade it. For this reason, the team views signature-based tools as being most effective for detecting issues in the IT and Compliance domains.

Metadata Monitors

Metadata monitoring involves observing the behavior of infrastructure, for example, monitoring the flow data from a router. If, for example, a router suddenly comes under exceptionally heavy load, it’s probably worth looking into even if none of the signature-based tools generate an alert.

Metadata monitors tend to be less easily spoofable than signature-based systems because an attacker has no choice but to use the infrastructure. However, there are fewer solutions available, and they are not as enterprise-ready as the best signature-based tools.

Unconventional Sensors

For lack of a better term, the team refers to a third category of sensors as “unconventional sensors.” These sensors typically leverage a knowledge advantage that the team has over an attacker. Dark IP is an example of a quintessential sensor of this type. With Dark IP, a certain number of IP addresses are never allocated for use on the network. If a networking packet is seen with one of those IP addresses in either the source or destination field, it can be assumed to be malicious. A sensor of this type is very difficult to spoof, because the attacker has no way to know which addresses weren’t allocated.

Sensors in this category are particularly effective against issues in the Security domain. They are difficult to spoof and avoid. However, because they involve very specific knowledge of one’s own network, they tend to be custom-built rather than bought off the shelf, and are often less manageable and scalable.

Achieving the Right Mix

In general, the tools in these categories form a spectrum, with signature-based tools being strongest against IT and Compliance issues, unconventional sensors being strongest in the Security domain, and metadata monitoring lying in between. The key to success is to architect an overall solution that uses an appropriate mix from all three categories in order to achieve the desired amount of coverage in the three problem domains.

Purpose-Built Sensors vs. Instrumented Network Infrastructure

The Security Monitoring team has a certain number of sensors that are purpose-built—they are designed to be sensors. NIDS are an example of purpose-built sensors. These sensors have the advantage of having correlation engines already available for them, as well as a console that analysts can use to view alerts.

“The team foresees a day when Microsoft might not have a network core at all, but would instead consist of company-operated resources directly connected to the Internet.”

The team also uses data from the network infrastructure. For example, they harvest data from various network devices, effectively turning them into sensors. They do the same thing with the logs from line-of-business application servers. The team uses a Security Event Manager (SEM) to help make sense of this data. All of the data goes through the SEM, where it is correlated according to the rules that the team writes and is displayed in a console. The team also maintains a very large historical database. This data serves two purposes. As it arrives, it is used by the Security Monitoring team to detect anomalous activity. The Investigations team also uses the data to identify a particular person’s activities over time.

Security Monitoring Process

The Security Monitoring team collects, analyzes, and responds to events detected on the network. The team also does a lot of checks, confirmations, and recalibrations. The following list describes the process:

1. Collect and analyze the data. Data is pulled from a number of different sources and then it is harmonized so that it can be compared. The data is then correlated to develop a comprehensive view of what’s happening on the network. This view is then vetted to see if it is consistent with other indicators of the network’s state.
2. Remedy the problem. When the analysis indicates a problem on the network, the problem is assigned to the appropriate team to resolve. The problem is assigned to the:

* IT Compliance team, if it involves a policy or regulatory-compliance issue
* Security Monitoring team, if it involves a potential security issue
* Investigations team, if it involves a violation of standards of business conduct

The responsible team determines the right course of action and engages other teams for help as needed.

1. Review. The team always takes steps to independently confirm that the remedy was successful, and that the problem no longer exists. This is an important step, and one that many companies overlook.

The team continually recalibrates their process. Recalibration consists of three things:

* Maintaining a baseline to understand what the team can actually see and do
* Developing a target to specify what the team would like to be able to see and do
* Adjusting the monitoring to move the baseline as close as possible to the target

Partnerships Are Key

The Microsoft enterprise network is a very large network, so it’s very important for the Security Monitoring team to have healthy and vibrant relationships with partner teams. The team partners with the following Microsoft teams and external organizations:

* **Microsoft Security Response Center (MSRC)**. The team works extensively with the MSRC to get insight into the different types of vulnerabilities. For example, what has been recently patched and how much are different vulnerabilities being exploited?
* **Microsoft IT**. The team works with Microsoft IT to understand the preventive controls that Microsoft IT is deploying and what the team should be seeing on their monitors as a result.

“A proxy server has value even in the absence of a network core, because of its ability to help protect client machines from harmful Web sites. The team therefore believes that there will be “proxies in the cloud” that can be used as monitoring platforms.”

* **Microsoft Malware Protection Center (MMPC)**. This is Microsoft’s internal anti-virus team. Other companies should work with their anti-virus vendors. These vendors can often provide more information about malware than is available on a public Web site. This can provide a company with useful information to help them build signatures, to know when signatures from the vendor will be on their way, and so on.
* **IT Security Engineering Department**. The team works extensively with the IT Security Engineering department to understand where the network is headed. How is it changing? What will it look like in one year? How is it going to impact the way that they have to do monitoring?
* **IT Operations Team**. The team gets occasional help from the Operations team to get access to certain parts of the infrastructure where there are problems.
* **MSN and Other Online Services Monitoring Team**. The team collaborates closely with this team to share information and to take collective action if they see something happening.
* **External Organizations**. The team stays in touch with a number of external organizations, including anti-virus vendors, Computer Emergency Response Teams (CERTs), and other organizations that help the team stay abreast of events in the larger information ecosystem.

Challenges

The Security Monitoring team faces several key challenges:

* **Network Growth**. Like many corporate or enterprise networks, the Microsoft enterprise network is continually growing. It is an ongoing challenge to know exactly where sensors should be placed and which assets are most important. Meeting this challenge requires the team to stay in close touch with the IT Network teams, as well as asset owners around the company.
* **Data Volume**. It would be easy for the team to gather data indiscriminately and collect more than it can analyze. To avoid this, the team instituted a business-driven process with the following steps:

1. Analyze the key questions that the team must answer.
2. Determine the analytic techniques and data needed to answer those questions.
3. Identify the data sources.

In many ways, this process inverts the usual approach, by helping the analysts to identify the data they *don’t* need, rather than focusing exclusively on the data they do need.

“As the network core disappears, the team anticipates that sensor locations will be driven by asset value so they will place the sensors near the things they protect.”

* **Legal Framework**. A growing number of laws in the US and elsewhere require companies to collect certain data or forbid them from collecting other data. It is an ongoing challenge to meet obligations on a network that spans the globe.

Trends

The Security Monitoring team sees the following trends affecting their work:

* **Disappearance of the Network Core**. A general trend is that companies want to minimize how much network infrastructure that they must own and operate. Few companies today own the Wide Area Network (WAN) media that connects their international networks, and many would prefer to outsource even the media between buildings within a campus. This trend will be accelerated by DirectAccess®, a technology in Microsoft® Windows® 7 that allows machines to access corporate assets through the Internet using Network Access Protection (NAP) and Internet Protocol Security (IPsec). The team foresees a day when Microsoft might not have a network core at all, but would instead consist of company-operated resources directly connected to the Internet. In this case, much of the infrastructure that the team utilizes for sensors might not be available.
* **Floating Edges**. In contrast to many companies, Microsoft does not believe that the dissolution of the network core portends the end of the network edge. A proxy server, for example, has value even in the absence of a network core, because of its ability to help protect client machines from harmful Web sites. The team therefore believes that there will be “proxies in the cloud” that can be used as monitoring platforms.
* **Strong Authentication**. Strong authentication will be more and more the norm. This is a good thing for security monitoring.
* **New Form Factors**. Mobile devices are an example of a new form factor. The fact that an IP address is no longer tied to a physical place is going to change the way that the team does security monitoring.

Coming Doctrinal Changes

Considering the current challenges as well as the trends, the Security Monitoring team anticipates that the doctrine will change in the following ways in the next few years:

* **Asset-Bastion Model**. Today, the common industry practice is to place sensors in locations where they can see a lot of traffic (topology-based). However, as the network core disappears, companies may only be able to place sensors at or near the critical assets that they continue to host. The team believes that this change will create some advantages, such as allowing companies to better manage the amount of data that they collect, while also giving their sensors access to business-logic data that can help them improve the accuracy of their monitoring.
* **Diversity of Sensors**. The team foresees a general trend toward a more diverse mix of home-grown and commercial tools. This will be needed not only to ensure that companies maintain the right balance between detecting IT, Compliance, and Security domain issues, but also to take advantage of the business-logic data available in the asset-bastion model.
* **Shift from Reactive to Proactive Stance**. The team anticipates continuing the shift from a reactive stance to a more proactive one. A security analyst cannot rely solely on a tool to indicate what is happening on the network and to gauge the level of importance of the event. As threats continue to increase, the team will continue to need analysts who apply human ingenuity and open-ended problem-solving skills.

Conclusion

In order to safeguard Microsoft’s intellectual property and digital assets, the Network Security team at Microsoft has to comply with federal laws, industry regulations, and corporate policies, while balancing business-agility needs and the needs of Microsoft employees and stakeholders.

The Security Monitoring team, which is a part of the Network Security team, uses a variety of sensors and other tools to monitor the Microsoft enterprise network. These tools include signature-based sensors, metadata monitors, unconventional sensors, and instrumented network infrastructure.

The Security Monitoring team faces many challenges in monitoring such a large, complex, and dynamic network. With rapid network growth, an explosion in the volume of data, and new form factors such as mobile devices, it’s very important for the team to have vibrant partnerships with other teams at Microsoft and in the industry.

For More Information

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada Order Centre at (800) 933-4750. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information via the World Wide Web, go to:

<http://www.microsoft.com>

<http://www.microsoft.com/technet/itshowcase>

© 2010 Microsoft Corporation. All rights reserved.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft, DirectAccess, and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.