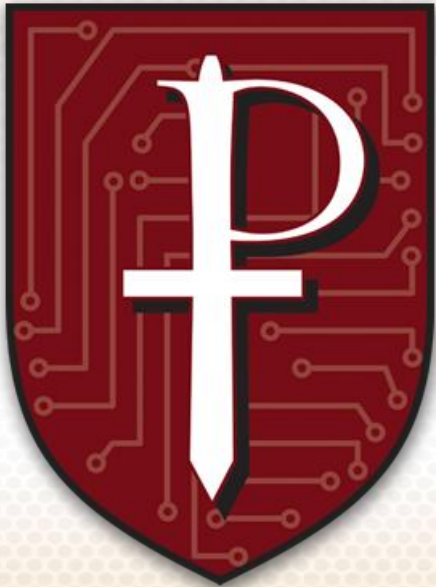


Network Security Monitoring

v 1.3

A PROTECTUS Whitepaper

PROTECTUS[®]
ENGINEERED NETWORK SECURITY



By Pete Garvin, Managing Engineer

PROTECTUS[®]
600 Weber Drive
Wadsworth, Ohio 44281

P (330)336-3577
F (330)335-7275

Introduction

Computer and data networks are a vital part of today's society. There is hardly a single aspect of our daily lives that is not in some way influenced by or completely dependent on data flowing over a network. It is interesting that while there is such a dependence on networks by most organizations, very few organizations have the tools or knowledge to actually see what is happening on their networks. Some reasons for this apparent discrepancy might be the fact that networks are generally reliable, network traffic is invisible, and human nature tends towards an out-of-sight, out-of-mind attitude.

An exception to the out-of-sight, out-of-mind attitude occurs when some type of problem or incident occurs. Hardware failures, misconfigurations, unexpected traffic volume, network attacks, and many other problems can cause a network outage, a performance problem, or a security breach that grabs our attention. Since network traffic is invisible, organizations often are not able to gather the information needed to identify and diagnose the problem.

This whitepaper is about monitoring networks especially in the area of network security. Existing practices will be reviewed and suggestions for improvement will be made.

Growing Awareness

There is a growing awareness of network security threats. News from any media outlet will frequently contain stories about data being stolen, networks being breached, or computers being compromised. I myself have received a three notification letters from security breaches involving my personal information. One letter was from a financial services company, a second was from a former employer, and the third from a hospital.

Signs of a growing awareness are not just in the minds of the most people, but the United States government is also showing signs of change. Major government organizations are creating high-level cyber-security positions on their staff. Also, the US Department of Defense has recognized cyberspace as a new domain in warfare and created a U.S. Cyber Command to unify cyber operations across the military.

While the growing awareness is good, we still have a long way to go. We are still in the very early stages of having sufficient computer security in our homes, communities, and workplaces. Even with all the progress that has been made, the practice of good computing habits is very much like the use of seat belts.

I can remember, many years ago, riding with my brothers and sisters in the back seat of a station wagon that my father was driving on the Ohio Turnpike. Although the car was moving along smoothly with all the other traffic, we were travelling much faster than today's legal

speed limit, and no one in the car was wearing a seatbelt. Driving your family down the highway at a high rate of speed while no one is wearing seatbelts may sound negligent today, but at that time it was normal. I think it is safe to say that few if any drivers or passengers wore seat belts back then. It is difficult to imagine the number of accidents, the human suffering, and all the public awareness campaigns that occurred before people generally made a habit of wearing seat belts. With all the tangible loss from automobile accidents, it still took decades for the public to develop the habit of wearing a seatbelt. So it is with network security, although the difference is that information loss can be less tangible and when there is a loss, it is much more difficult to trace back to a root-cause event. Just as it took many decades for wearing seatbelts to become the norm, it will take even longer for good network security practices to become the norm.

With all the tangible loss from automobile accidents, it still took decades for the public to develop the habit of wearing a seatbelt.

Good network monitoring can help increase awareness. Showing business owners and network managers first-hand the attacks against their system can really get their attention. They may have no idea that people were actually probing their networks. They often believe that a security breach won't happen to them and think that security by obscurity is sufficient. Since bits flowing over a wire are invisible and since the symptoms of a successful attack can easily go unnoticed, it is understandable how someone unfamiliar with the threats might have a false sense of security. Network security monitoring is one way to show the otherwise invisible activity on a network and help bring the actual threats to light.

Binary Monitoring

Monitoring can mean many things. One type of monitoring that is relatively easy to implement is what we call binary monitoring. In this type of monitoring, the tools are checking for some condition that is easily detected and has virtually a 0% false positive rate. Examples of parameters often included under binary monitoring are disk space, CPU usage, free memory, and network connectivity. Standard protocols and tools can be used to detect and notify when these parameters are outside of a specified range. For example, a notification email can be sent when free disk space is less than 20%, when CPU usage exceeds 90% for more than 10 minutes, when free memory falls below 10%, or when a server stops replying to a ping request.

As long as an acceptable threshold can be selected, this type of monitoring can be practical and useful. It is helpful for a system administrator to know when a server has some parameter that is out of range and is in need of attention. But even with this simplest type of monitoring, unexpected results can arise. Assume a network administrator runs a binary monitoring tool in

The Binary System

Computers work in binary. They use two states, on and off, represented by 1's and 0's (also called bits) to do their work – but why is that? The reason is that having only two states give the lowest error rates and highest immunity to noise.

Ternary (also called trinary) computers have been made with three states, -1, 0, and +1. These are trits instead of bits.

Unless you're working with quantum computing, electronics ultimately work because electrons flow through metal or a semiconductor material such as silicon. These electrons, along with the characteristics of the circuit they flow through, determine the voltage – a continuous range of voltages is possible.

If a binary device has a 6-volt power supply, then 0 to 3 volts is assigned a binary 0 value and above 3 volts is assigned a binary 1 value. In a ternary device, 0 to 2 volts is a trinary -1 value, 4 to 6 volts is a trinary +1 value, and in between is a trinary 0 value. A 6-volt device deciding between two binary values (with at least 50% chance of a correct answer) will be correct more often than a 6-volt device deciding between three trinary values (with at least 33% chance of a correct answer) when both are operated over a range of temperature and environmental conditions. The binary device will have a lower error rate and get the right answer more often than the trinary device.

their office to monitor a web server located in a remote data center. If the monitoring system reports the web server as being down, it may be that the internet connectivity between the office and the data center is temporarily unavailable. In this scenario, the monitoring system would create an alert notifying the administrator of a server outage while the web server actually never missed a beat. This is a simple example of unexpected results can occur and why monitoring results need to be interpreted.

Thresholds

Thresholds are a part of monitoring. Establishing a threshold and alerting when the threshold is crossed is the basic definition of monitoring. Monitoring is practical when a threshold can be easily defined and accurately measured. Binary monitoring of a hard disk that crosses the threshold of less than 20% free space is one example. But what happens when the threshold is not so easily defined or when accurate measurements cannot be easily taken? In those cases, the monitoring becomes less useful due to false positives (alerts generated when there actually is not a problem) and false negatives (no alerts generated when there actually is a problem).

Some of the problems that plague network security monitoring and make it more difficult than simple binary monitoring to detect cyber attacks include:

- Cyber attacks that have various and changing types of observable symptoms.
- Difficult to define measurements for what constitutes a cyber attack.

- Symptoms that appear to be an attack on one network may be perfectly normal on another network.
- Stealthy attacks can sometimes have very few observable symptoms.

Assuming these problems can be overcome and some type of network security monitoring is deployed, a threshold must be selected. If the threshold is defined in terms of observable symptoms that can actually be measured and if the cyber attack actually creates enough of these observable symptoms, then the threshold is exceeded and the attack can be detected and stopped. If the cyber attack does not create enough observable symptoms or if it creates observable symptoms that are not being measured, then the attack is not detected. Figure 1 shows these scenarios graphically.

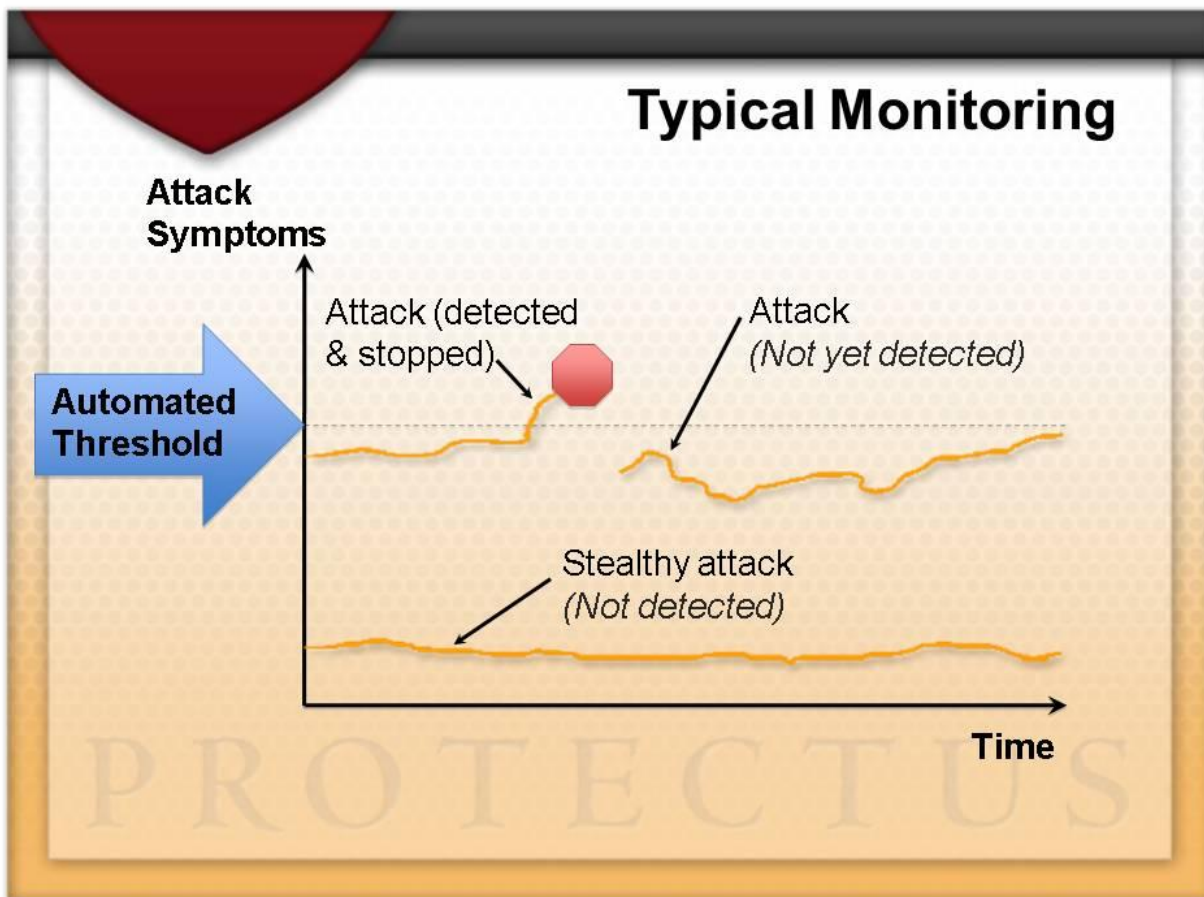


Figure 1 - Typical Monitoring

Note that stealthy cyber attacks by definition create very few observable symptoms. So the question must be asked – why not simply lower the threshold? The answer is that lowering the threshold creates more false-positive alerts. When an administrator is peppered all day long with hundreds of alerts from a monitoring system, it does not take long before those alerts are ignored and become meaningless.

One technique we use in our KnightHawk™ service to resolve this problem is to periodically perform deep-dive analysis. Deep-dive analysis is a manual process in which the threshold is pushed very low by a human analyst. Figure 2 shows how the deep-dive allows an analyst to detect stealthy attacks that would otherwise go unnoticed. During the deep-dive, an analyst takes data collected by the network security monitoring system, places it in the context of the network being monitored, and correlates information from the various data sources. This allows for a much deeper understanding of the available data. By reviewing the security monitoring data in this way, the analyst is able to identify symptoms lurking below the automated threshold, apply additional scrutiny as needed, and weed-out apparent symptoms that can be safely ignored. As a result, the chances of detecting a stealthy attack are greatly increased.

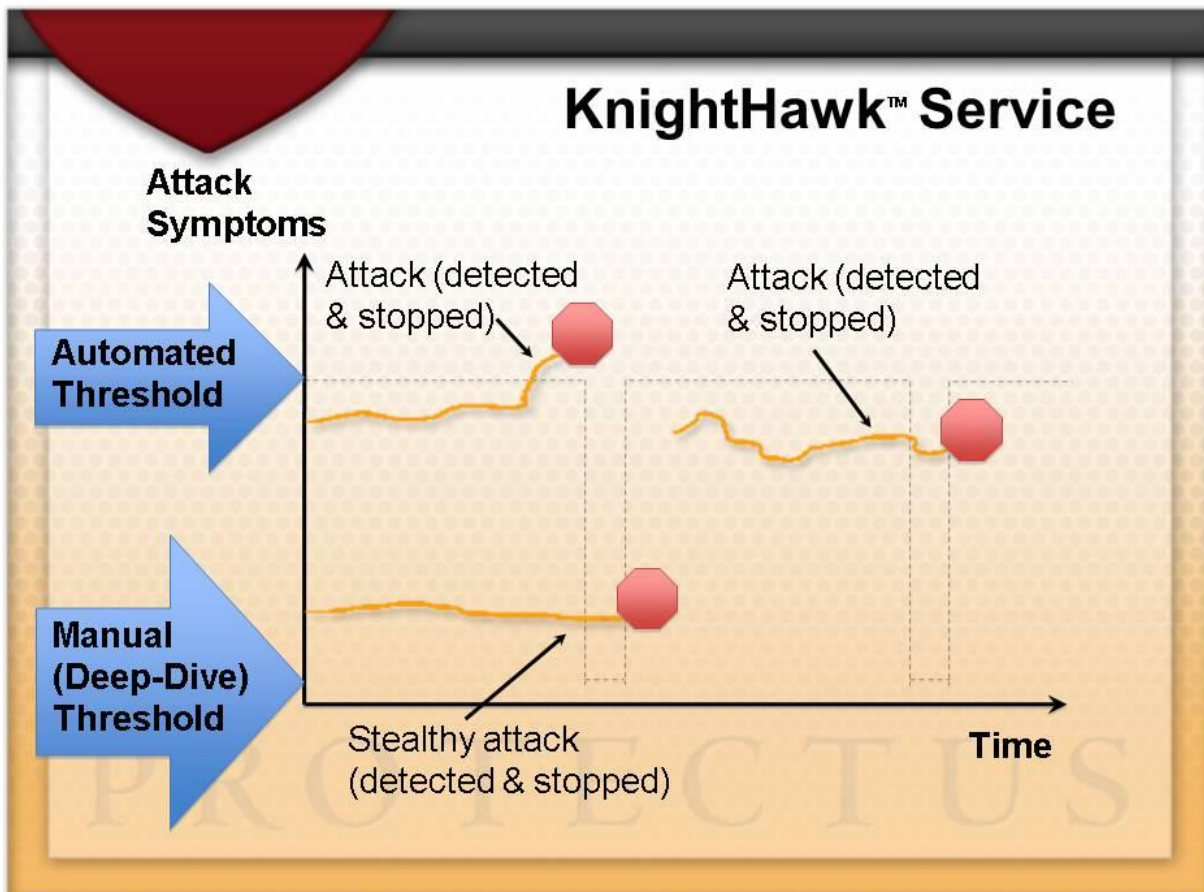


Figure 2 – Deep-Dive Analysis Used in the KnightHawk™ Service

Improved algorithms

The deep-dive is a useful technique but is limited in that it requires valuable time from a human analyst. What is ideally needed is a technique to lower the automated threshold. While today's technology is not good enough to completely eliminate the analyst from the loop, there is room for improved technology that can better identify potential threats in a way that allows

the analyst to be as productive and efficient as possible. This is where improved algorithms come into play.

Improved algorithms can be used to lower the automated threshold. To do this, they analyze traffic data and either identify traffic of interest by learning from an analyst or organizing traffic into logical groups based on its characteristics. Figure 3 demonstrates the effect of improved algorithms lowering the automated threshold.

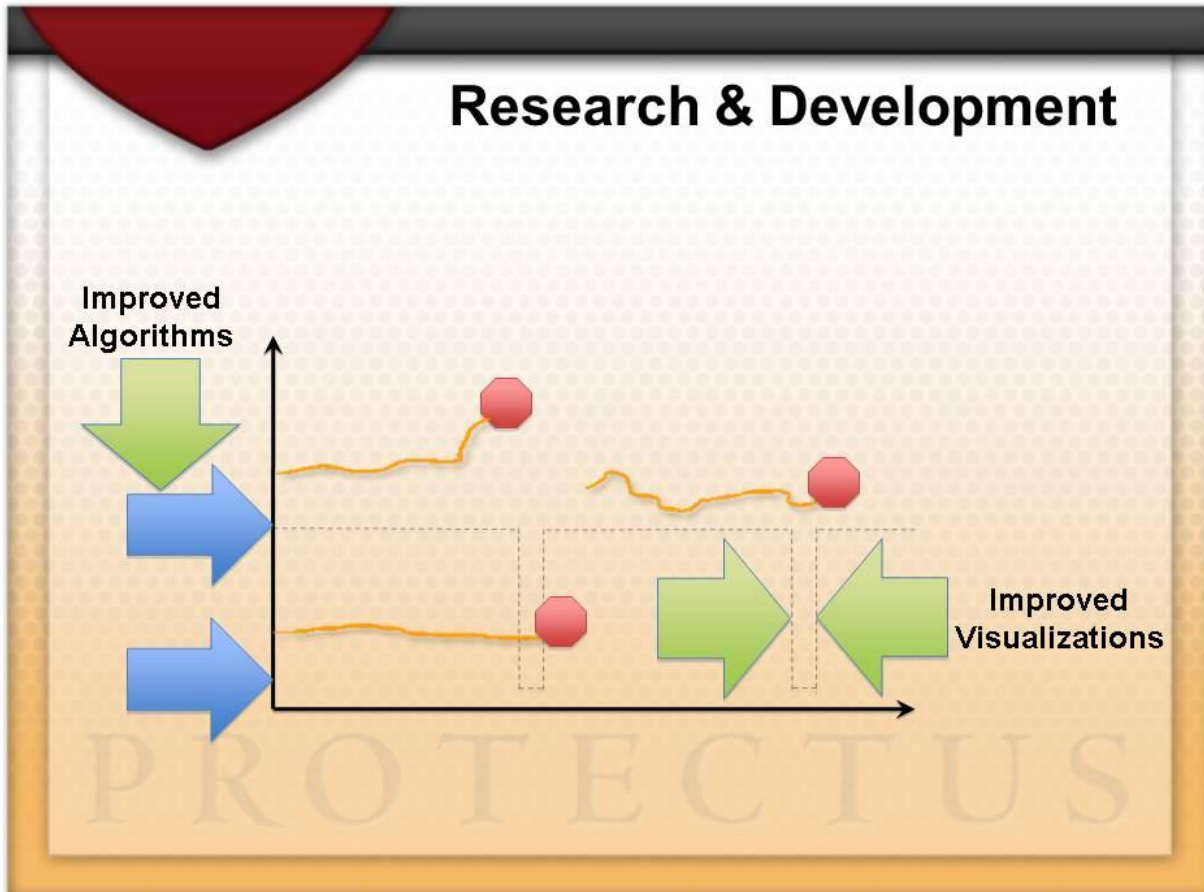


Figure 3 - Benefits of Improved Algorithms and Visualizations

Visualization techniques

In addition to lowering the automated threshold, it is desirable to decrease the deep-dive window duration by making the analyst as productive as possible. The effect of improved visualization and interpretation is also demonstrated in Figure 3. When the right tools are used to display algorithm results and present them within the larger context of overall network traffic, an analyst can more easily interpret the results and more quickly reach conclusions

about what is actually happening on a network. By increasing the analyst's efficiency in this way, the time needed for an analyst to complete a deep-dive is decreased .

About PROTECTUS

PROTECTUS, LLC supplements teams with network security and performance capabilities for customers in a range of industry segments. Our hands-on experience defending networks dovetails perfectly with our ongoing research and development efforts in the area of improved network security tools and techniques. PROTECTUS is privately held and is based in Northeast Ohio.