CYBERSHIELD™ NETWORKS
Intelligent Security for a Changing World

The Intelligent, Proactive Information Assurance and Security Technology

IPDM

Next Generation Network Intrusion Prevention and Deception Management Revealed

Webb Wang

CSO/CTO, and Conceptual Architect

CyberShield Networks, Inc.

August 2004

A White Paper

CyberShield Networks Winning Security Formula:
Effectiveness = Intelligence + Time

CORPORATE HEADQUARTERS

1584 Ohio Avenue • Palm Harbor FL, 34683 • Main 727-787-9148 • Fax 727-787-9368

CYBERSHIELD™ NETWORKS
Intelligent Security for a Changing World

1. Introduction

Today's network security marketplace is crowded with all kinds of products addressing all sorts of security domains, IDS, IPS, HIDS, HIPS, Firewalls, Anomaly Analysis, Misuse Analysis, just to name a few.

However, with all of these offerings combined, according to the most recent CSI/FBI reports, they still only provide about 40 to 50 percent total overall effectiveness towards protecting our network assets.

What's the problem? Well, by deeply examining the entire security domain these products are targeting, and the technologies these products are employing, it is really not that difficult to understand that each of them are only focusing on one aspect of the entire network security domain. This effectively leaves limited or, in most cases, zero time for the security professional to intervene before the attack takes place, not to mention inordinately large numbers of false alarms that simply overburden the individual(s) responsible for the security of enterprise assets. Hence, they inherit much lower or, sometimes, even zero effectiveness towards protecting that enterprise. These common low rates of effectiveness render both technology and personnel almost ineffective in dealing with the constant battle against myriad network attacks that change daily in both nature and scope.

What exactly is a highly effective approach to network security and the protection of critical assets?

Cybershield Networks strongly believes that the highest effectiveness in a network security product must empower security professionals to easily distinguish bad network traffic from good traffic with super low or even better, no false alarms. This higher effectiveness must also empower security professionals with ample time to intervene with potential attacks in order to craft an appropriate security counter measure, applying real-time preventative measures, or real-time defensive security policies or other initiatives before an attack can compromise the enterprise.

CyberShield Networks IPDM Technology suite is built with this strong philosophy in mind. We firmly believe that to be able to achieve the highest levels of effectiveness in combating and mitigating attacks, you must constantly possess complete and accurate intelligence about everything involved in the event, including the attacker and your entire enterprise (network assets, your entire IP space, all applications, and proprietary information contained therein), plus the ability to buy yourself ample time with early warning to be able to proactively and preemptively defeat your attacker.

With the constantly evolving internet, the network domain has evolved into a cyber battlefield, where security professionals are constantly facing battles with attackers from both determined ones such as professional attackers, and under-determined ones, such as script-kiddies, and myriad worms and viruses), and the only way to

win this cyber war is to arm yourself with the deepest, broadest, and most accurate intelligence you can possibly get, along with enough time to strategically place yourself into a winning posture.

That winning security formula is:

Effectiveness = Intelligence + Time.

2. About Intelligence

Intelligence is about knowing everything involved and everything that is about to be involved.

Are you fully capable of laying out a winning security strategy if you do not know fully what assets are under your protection? In other words, do you truly know the battlefield?

Will you be able to defeat your enemy if you do not know his/her motivation and capacity?

The completeness and accuracy of collected intelligence is one significant, though major contributing factor towards enabling you to make concise and effective decisions in fighting any type of attack. Completeness encompasses the following:

-entire compilation of all network assets you must protect
-what those assets are
-what information is contained on them
-their operating requirements (highest availability vs. highest data integrity, for example),
-the entire IP space owned by the organization
-where each network asset is located within the enterprise
-both assigned and un-assigned IP spaces
-and, detailed and accurate reconnaissance information about your attackers or soon-to-be attackers.

Intelligence is about the ability to distinguish good traffic from the bad with absolute accuracy from both known attacks and unknown attacks (i.e. day zero attacks).

Virtually all of today's existing security products on the market have failed to live up to expectations in one way or another due to serious lack of accuracy.

Absolute accuracy in the alert of an attack, or potential attack, is another significant and contributing factor towards creating a winning security posture in fighting attackers. Absolute accuracy gives security professionals the highest confidence in initiating security counter-measures.

After all, any intelligence is rendered useless if you are unable to tell what's bad vs. good, and what to use vs. what not to use.

CyberShield Networks IPDM Technology suite is specifically designed with the innate ability of collecting the most complete intelligence with the highest level of accuracy deeply embedded within. In fact, we are proud to be able to say that IPDM is truly able to issue attack warnings with the industry's highest accuracy.

To further extend our wining security formula, we strongly believe that **Superior Intelligence = Completeness + Accuracy**.

3. About Time

The second half of our winning security formula is about time. Time is everything, especially in the world of network security, where sometimes, even a couple of seconds before an actual attack can take place makes a substantial difference. The ability to able to receive early warnings of attacks in order to gain ample time to analyze, determine, and deploy an appropriate and effective security mitigation measurement is of paramount importance.

The ability to issue early attack warnings not only empowers security professionals with enough time to take action, but also empowers them to take proactive or pre-emptive actions against attackers. Imagine that a potential attack has been detected, and you being notified that it's about to move on to compromising your true network assets, and you have the ability to proactively divert this attack into a virtual cage where the attacker gets completed quarantined, or, you have the ability to slow down or even halt the attack, and at the same time having enough time to notify your perimeter defense devices (such as a firewall) to take initiatives to block and prevent such attack from happening, or ever happening in the future. Let's think about the benefits of that capability for a moment.

In addition to the ability of initiating proactive steps towards protecting your network assets from being harmed, **the other huge benefit of having enough time is that you have now clearly identified a attack along with its attacker, you have the opportunity and ability to mount defensive initiatives to further deepen your understanding or intelligence about your attacker, and to share that highly accurate intelligence with your peers (both professional and business) to further enhance your entire security posture. Those are major and unique benefits, which translate to quantifiable ROI.**

CyberShield Networks IPDM Technology suites are precisely designed to deliver these benefits including early attack warning, along with the pre-built tools to help security professionals utilize this precious time to take proactive and defensive action.

To complete our winning security formula, we also strongly believe that **Time = Proactiveness + Defensiveness.**

4. Our Product Offering

CyberShield Networks' belief in achieving highest effectiveness you must possess both solid intelligence and ample time, and this is the foundation of IPDM Technologies and its highly unique methodologies.

All components contained within these product suites have been strategically positioned to help deliver to security professionals a much more effective, much more powerful solution in the fight against ever evolving network attacks.

Our flagship component, RouterShield, is developed to enable our product suite to be able to detect the attacks and issue warnings with the highest accuracy along with the ability to discover with the highest levels of confidence unknown (or day zero) attacks. RouterShield also empowers security professionals the ability to proactively intervene with on-going attacks to further strengthen their security posture.

RouterShield combined with CyberIntercept provides security professionals a complete, unfettered holistic view of everything belonging to and happening on the enterprise network resources under their care. All of this intelligence data is collected, analyzed, and correlated by our CyberAnalytics component to further organize the massive amounts of intelligence into ready-to-use, easy-to-understand security information, which further strengthens your security professionals in creating and maintaining the edge in a winning security policy or measurement.

Our unique, eye-catching and graphically intense, interactive CyberRADAR Command Center brings security professionals an all-in-one operating console to further simplify, streamline, proactively and effectively manage all security actions, which, in turn, transforms security initiatives into much more effective and much more positive rates of return in your effort to protect your precious network assets.