

NetDefense-21™: Replacing Antiquated CND Models & Practices

Robert J. Bagnall, InfoSec Engineer

Veridian-Trident Data Systems

10455 White Granite Dr.

Oakton, VA

703-383-1883

Robert.Bagnall@TDS.com

Abstract

NetDefense-21™ [ND-21™] is a conceptual development model examining current and future trends of computer network exploitation [CNE] and the failures of existing computer network defense [CND] practices to meet those challenges. ND-21 discusses the top 5 problems with current CND models and will offer insight into solutions suitable for conducting network defense in a dynamic, 21st Century environment. Far from a full solution, NetDefense-21 is an evolutionary development of the computer emergency response team [CERT] model with its own considerations and limitations. But the need for a fundamental, forward-thinking evolution of the CERT model is desperately overdue, and ND-21 offers one such solution by exploring the need to increase awareness and training, centralize multiple CERT teams and response processes, and automate the protection process to a far greater extent. These efforts will move the reactive, static defense posture of the current CERT model into a proactive, dynamic defense system to meet the demands of Internet connectivity and the 21st Century.

1.0 Introduction

The CERT model is dead. The dynamic, speed-drunk technology of the Internet killed it. Never before in human history have people been so connected yet so out of touch. In the modern world it takes only a millisecond to communicate, to mass-email a virus, to bring down a mammoth e-commerce site with a Distributed Denial of Service [DDoS] attack, or to kill your career by accidentally sending your boss that angry instant message you probably should have thought through first.

Well into its second decade, the CERT model now finds itself in a world it was never designed for, a world of massive interconnectivity and interoperability. CERTs were meant to carry the defensive load for a single enterprise or small group of networks, one that only dealt with your users and the occasional remote traveler.

Then came the Internet, and with it a world of communication, commerce, and connectivity that no static, in-house, reactive process could ever hope to keep up with for long. As we enter fully into the 21st Century, the CERT model must evolve, and the thought processes of management and security personnel with it. There are a few more flexible evolutionary concepts underway now, and ND-21 is one of them.

2.0 The Major Problems of Current Computer Network Defense Processes

To properly understand the changes and evolutionary steps that a concept such as NetDefense-21 offers, it is first essential to understand how current CND practices and thought processes fail to provide adequate network protection.

2.1 The Failure of Management

In identifying the ways in which management has not met the need for adequate security across the enterprise, it is important to note that the term “failure” is not used to define management in a derogatory manner. Managers face many daily challenges of which InfoSec personnel are often completely unaware. Moreover, the ineffectiveness of security administrators to correctly define the problem and adequately express the severity of consequences directly related to a lack of action contributes to the failure of management to take proper action. In today’s society, particularly in America, the desire to implement a single quick fix on a shoestring budget is often seen as a viable solution to immediate security needs. But information security requires more than an “instant gratification” solution to be truly effective over the long term, and managers can no longer afford to live by the that-can’t-happen-to-me mindset.

Indeed, the misconceptions of management are well-documented within such esteemed security circles as the SANS organization. A survey of security professionals during their 1999 Federal Security Computer Conference found that the number one error by management was that they *“assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.”* [See atch-01]

2.1.1 The Failure of Management to Adequately Address the Problem

Human beings tend to be short-sighted. With budgetary restraints what they have been, placing the proper emphasis on security needs has been all the more difficult while costs are contained and funding squeezed. Moreover, there has been a long-standing belief within management that the risk is minimal – therefore the priority assigned to information security has traditionally been low. During the days before the Internet this mentality held a lot more value, though it was a dangerous misconception even then. Today, such a belief is flawed and comes with potentially disastrous consequences.

2.1.2 The Failure of Management to Grasp the Problem Once it is Addressed

In the past, constructing a CERT or installing a firewall or Intrusion Detection System gave managers a false sense of security. Indeed, even today this mentality can still be found in many circles. But once the rage of the World Wide Web began to connect networks the potential for intrusions and the security concerns related to them increased exponentially. Currently, when issues of information protection arise, the depth of the answer that is required is largely misunderstood or not understood at all by decision-makers. The cause of this is two fold:

2.1.2.1 The Failure of InfoSec personnel to Adequately Explain the Problem – and its Solution

First, InfoSec personnel have largely been unable to impress upon management [both corporate and government] the critical need for information security. Moreover, they have been remiss in not correctly stating the depth of investment that is required to provide real, viable protection measures, nor have they correctly stated the consequences of the failure to do so.

2.1.2.2 The Failure of the Vendor to Put the Needs of the Customer Ahead of Sales

Secondly, vendors tend not to put the needs of the customer ahead of sales. All too often the success of the vendor sales force is based heavily upon sales rather than repeat business and customer service. This leads to great numbers in terms of sales, but not necessarily the best solutions for the enterprise. Vendors, taking advantage simultaneously of the InfoSec person's love of newer, faster technology gadgets and management's lack of understanding of the proper application of technology, often sell solutions that are either inadequate or overkill. This leaves security personnel feeling euphoric for having the latest technologies and management feeling as if they have "saved the kingdom" simply by buying the latest firewall or CERT solutions.

2.1.3 The Failure of Management to Properly Address the "Costs of Doing Business"

Rarely when one thinks about the cost of security, even today, are the words "training" and "awareness" included. Yet estimates of network attacks and intrusions still involve insiders around 80 percent of the time. Most systems are still compromised because of poor access accountability [password enforcement, for example] and failures in systems administration, and most system penetrations still involve some level of social engineering against unwitting personnel within the target's network.

Sufficient training and awareness in information security comes on many levels and must be considered a critical cost of doing business in the internetworked world. Without it the real cost of doing business only gets more expensive as competitors, hackers, and foreign intelligence services steal, degrade, and destroy the ability to operate, be that as a business or a government entity.

2.1.4 The Failure of Management to Understand InfoSec Personnel Motivators

Annually in America, management pays the security consultant, on average, over \$73,000. Yet do they know what your InfoSec professional needs or wants to stay within their organization? Or what brought them to their current position? Chances are the answer is "no". Shortfalls in the market availability of qualified information security personnel has made it necessary for corporations and government organizations to follow one of three courses of action to maintain a reasonably-sufficient staff.

The first of these is to adopt the practice of hiring "white hat" [or ex-] hackers, the very people they are trying to stop. Indeed many individuals within the InfoSec community are, or were at

one time in their distant past, hackers. The second option is to outsource security to a qualified InfoSec provider who, often times, will also follow the first option when manning shortfalls make other solutions impossible. The final option is to “groom” or “grow” qualified InfoSec personnel. Mostly, these individuals come from systems administration or systems analysis positions and are persons with at least some limited experience and interest in information security. Although this option is time consuming and costly, it is also the best long-term solution both for the InfoSec provider and the market as the more qualified employable information security persons there are in the marketplace the lower the salary demands paid out and the larger the pool of talent from which to choose.

Although generalities never fit all persons within a group, when management employs InfoSec individuals certain assumptions can be made. These motivators are, however, most often overlooked by the employer. The first of these is what motivates an InfoSec professional to come to a new company from their former employer. Recruiters seldom seek out the things that motivated the individual to move and even less frequently do they track and convey this information to management. Thus, when turnover occurs because motivators and expectations are not met, recruiters go back to work trolling the talent pools for fresh prospects and management scratches its head. During a 1999 SANS survey of InfoSec professionals [See atch-02], over 75% of respondents answered “training” and over 50% answered “tuition” when asked to list a few of their favorite benefits. Management needs to listen to their people and start paying attention if they want to keep them.

2.1.4.1 The Failure of the CERT Model to Encourage Training

Equally important is the fact that both the customer and the InfoSec provider are discouraged to support quality-training efforts while they are tied to the existing CERT model. The CERT model does not support training because it places InfoSec personnel at a remote location away from the provider’s home offices. The process must then be duplicated by the provider at each site they support. The logistics of such an undertaking quickly overwhelm the profits being made, so adjustments must be made.

Thus, the first budget item cut is training and individual development opportunities because it is near impossible to constantly rotate qualified personnel from the provider to the customer site and back again each time a personal development opportunity comes along. Once the training opportunities leave, so do the qualified InfoSec personnel [See Atch 01-02].

2.2 The Failure of CND Models to Automate Active Defense Processes

The CERT model was created to protect networks: static, closed networks with limited scope. It has been defined since its inception over a decade ago as a response system to computer intrusion. It was never designed to support active defense measures because a CERT, by its very definition, is reactive. When CERTs came into being, most hacking was still carried out by highly skilled, command line intruders who used 2400 bps modems and DOS wardialers. That era required that the potential intruder had a skill set sufficient to penetrate a powerful, high-level network. That was a time when the Bulletin Board [BBS] ruled the networked world. A time before the scripted

attack existed. A time before automated intrusion tools were commonplace. A time before the Internet was the standard.

The Internet and automation have changed everything. People, systems, and networks are connected as never before, and in a more backend, automated fashion. In modern windows environments the vast majority of system processes run behind the scenes and without the knowledge of the user. Although this system makes it convenient for the user to operate the system with little or no knowledge, it makes security far more difficult because active processes and functions taking place are out of more difficult to track.

The CERT model as it exists today is bulky, slow to take action, and expensive to maintain. This is particularly true for outsourced, in-house operations where an information security company is handling the CERT duties at the customer's site. Although the outsourcing of CND operations in this case would be thought to be more cost-effective for the customer it is in fact more expensive in terms of intangible costs and the overall security readiness posture. Hidden pitfalls such as training maintenance and employee turnover at the InfoSec company cause the customer to lose security effectiveness and forces them to accept inferior personnel when manning shortfalls of qualified individuals exist such as they do in the current American job market.

Furthermore, when InfoSec providers handle multiple on-site CERTs at various customer locations, the overall cost of building and maintaining the CERTs increases dramatically. Suddenly the InfoSec provider has to be concerned with maintaining a full staff compliment at each location, has to handle the administrative overhead associated with reaching each staff at each locale to keep them abreast of changing information at the home office, and has to rotate staff in and out of each location if they want to maintain proficiencies through training. These costs swiftly build, creating excessive overhead at the InfoSec provider that is, in turn, passed on to the customer.

Often, to cut corners on overhead and to appease customers' fiscal concerns, InfoSec providers will slow training opportunities for on-site staff to a trickle or eliminate them altogether. This approach only exacerbates the problems of turnover and overhead as new staff members must be hired and trained in the duties and nuances of their positions to replace the recent exodus of the disgruntled staff who have left. The CND models of tomorrow must allow for a more dynamic, adaptable plan for InfoSec professionals on staff, one that is more in tune with their needs.

2.3 The Failure of Signature File Anti-Virus Defense as a Popular Model

Signature-based anti-virus defense has become the de facto standard both within the government and corporate America. This is because, up until very recently, there was no viable alternative. But the advent of four primary factors has proven that reliance solely on signature-based AV defense, even in multiple layers by differing vendor products, is no longer the best protection solution.

First, the popularity of easy-to-use compilers and programming languages such as Visual Basic®, Visual C++®, Java®, and Active-X® has greatly simplified the virus writing process. This has

been exacerbated by the embedding of these languages and their capabilities into popular productivity programs such as Microsoft Office® and browsers such as Netscape Communicator® and Microsoft Internet Explorer®. Now the malicious code is easier than ever to write, and is often imported for use by default in the programs people use everyday to get their work done.

Second, the rise of Melissa and other easy-to-code, easy-to-alter macro virus families as an attack tool has made regular signature file updating a logistical nightmare, particularly for large enterprises. Prior to Melissa, AV vendors normally suggested a monthly update to a system's signature files. Since Melissa came on the scene in April 1999, these same vendors now recommend bi-monthly or even weekly updates to system signature files.

The Melissa macro consisted of a mere 105 lines of Visual Basic® script. Using the VB Script program, it becomes simple for minor alterations to be made to the code that will not only change its performance and effectiveness but its signature as well. This was proved with the flood of Melissa family spin offs that have plagued the information landscape since April of 1999. This problem will only get worse as connectivity increases, networks grow larger, and signature files become bigger and more difficult to implement.

Third, the lack of a central AV authority [within either government or industry] and the inconvenience of accessing signature file updates have further exacerbated the protection process. During the five days immediately following the arrival of Melissa in April 1999, it was virtually impossible to gain access to the update download sites of either Symantec® [makers of Norton Anti-Virus®] or McAfee® [makers of Virus Shield®]. They experienced a Denial of Service [DoS] simply by virtue of the fact that millions of users and administrators needed to get to the same data, and two or three mirrors off the primary site were not going to suffice.

Finally, the advent of stronger, more effective vaccination-based, perimeter anti-virus defense products like Achilles Shield® by InDefense® make multi-layered AV protection far more viable than exclusive use of dual signature file based systems. Vaccination-based products require updates normally only for product version revisions because they base virus response not on the signature of a specific virus but rather on the behavior patterns of the family type each virus falls into. There are currently only three virus families in existence: boot sector, macro, and executable viruses. Vaccination-based AV systems provide supplemental perimeter protection in between regular signature file AV updates on servers.

2.4 The Failure of Basic Security Policy and Access Enforcement

The weakest link in the security chain is still the human one. The single greatest example of this is the failure of organizations to implement and enforce the most basic building blocks of information security: policy and access. An enterprise can be state of the art, it can house the best equipment, utilize the most up-to-date software, and be managed by the best personnel. But if the users of that network are not being made to adhere to basic policies and access controls, the network may as well have a welcome mat in front of it.

Too few corporations and government organizations develop solid, secure information protection policies and practices, and even fewer make a proper effort to enforce good policies once they are adopted. Without these there can be no network security because there is no enforced responsibility for an irresponsible act by users and managers. All too often security policies are subverted in the name of ease of use or, worse still, are simply ignored by users and managers altogether.

Lax security practices lead to poor habits and non-observant behavior patterns by users and ties the hands of security personnel when they lack a complete commitment from management. Then, when true security concerns such as social engineering surface, the posture of the entire organization is not prepared to adequately recognize, respond to, or prevent the intrusion. The entire enterprise is at risk because a lack of awareness and vigilance have come to be the results of poor security policy and access enforcement.

3.0 The Solution: NetDefense-21

ND-21 is a dynamic solution set that involves a remote, multi-customer, “defense in depth” approach, coupled with active processes and a heavily automated network protection workload. Because ND-21 includes a full commitment to training and awareness, it is a proactive information security model; one that lowers security risk by preparing customer users to make protection constant in their minds and building robust security policies and practices to support that thinking.

ND-21 encompasses a single entity divided into four divisions: 1> Knowledge, 2> R&D, 3> Analysis, and 4> Active Defense. These four entities, while not unique in scope, interoperate under a one-of-a-kind charter and approach. They are staffed by a single team, at a single location, serving many customer networks. Each division provides specific solutions, and both the division and its solution set is designed to be inter-reliant with the others just as each of the pieces are interconnected. As the success or failure of the whole security approach only holds the worth of its weakest link, so should follow the applications, policies, practices, and processes that support the security approach.

ND-21 personnel rotate through two of the four divisions every six months. Personnel from the Active Defense Division rotate through the R&D Division and, conversely, Knowledge Division personnel rotate through the Analysis Division. The rotation date is based upon their date of hire with exceptions being made for vacation time, training, and other scheduling conflicts.

Additionally, personnel from every division are required to spend two weeks annually outside of their normal comfort zone in one of the two remaining divisions they normally do not rotate through. This is to provide each member with a broad perspective of how each piece of the security plan interoperates with every other one, and how every decision they make in their normal position affects the others. Overall, these measures ensure that the entire staff remains on the cutting edge of their craft at all times, and that each member has operational experience and a balanced perspective.

The following sections will discuss the functions of the various divisions, staffing and training concerns, and how the total ND-21 team approaches solutions to each of the aforementioned security concerns.

3.1 The Active Defense Division

The Active Defense [AD] Division is the core of the ND-21 concept. AD is the “war room” where a staff of up to 30 personnel work 24 hours a day, seven days a week, and 365 days a year to defend, evaluate, and evolve up to 10 customer networks. AD is the one division where the moment-to-moment dynamic defense measures are consistently being tested, measured, and evolved.

The number of Active Defense Divisions that are built and operated by an InfoSec provider at any one time is only limited by the number of contracts and quality personnel the provider has at that time. One additional consideration for multiple AD Divisions includes expanding the number of personnel within the three remaining divisions. Because the roles of these divisions serve to support the efforts of the AD division, they must be similarly enlarged to adequately accommodate the growth of AD.

AD personnel will perform a wide variety of functions. They will be responsible for direct security-related liaison with customers, will provide random penetration testing and risk assessments, and will monitor network defenses. AD personnel will also implement the scripts and proprietary tool kits that they develop, specific to each customer, in concert with both the ND-21™ R&D Division and the customer’s own management information systems [MIS] staff. They will recommend evolutionary security measures required to adequately grow the entire enterprise specific to customer needs and requirements. These functions will be performed under the umbrella of computer internetworked defense [CID]™ as described below.

3.1.1 Computer Internetworked Defense -- A New Approach to Protection

CID is enterprise defense for the world of the Internet. Networks are no longer closed, stationary, or inaccessible. The connectivity and frenzy of the web has thus relegated standard CND models to the realm of ancient history. Today, the solution must be quick, responsive where necessary, proactive if possible, and interoperable with the overall security focus.

CID is a new way of thinking about enterprise security because it focuses first on the assumption that the customer network is interconnected with others, as well as remote and traveling systems, and that the policies and access controls on those connected systems are not under the customer’s direct control. This concern plays a large role in how the customer network is protected. Then it takes steps to eliminate or mitigate those risks. The second focus of CID is to make training and awareness a prime factor in the overall approach to security. Proper focus on this factor virtually eliminates risk in some of the most common and easily exploitable areas of the overall security posture within the enterprise.

3.1.2 Training within the AD Division

Proper and regular training of InfoSec personnel is a critical component in any information protection plan. Yet it is still largely ignored or only given a half-hearted effort by organizations that employ security personnel on their regular staff. Worse still, too many InfoSec providers are guilty of the same lax behavior. As previously stated, the CERT model as it exists today does not make training a priority. ND-21 is designed to support individual development opportunities for InfoSec personnel through the steps described below.

The ND-21 concept replaces the current multi-location CERT teams with a single active defense cell, housed at the provider's location, and running continually on three shifts. The entire team would consist of 7 to 10 personnel per shift.

Because the entire team works in one cell, it is possible to coordinate the defense and maintenance of multiple customer sites simultaneously. Shift and personnel overlap enables a single, big picture perspective, allowing each team to be intimately familiar with status and situational concerns across all customer networks at a glance. Working with on-site systems administrators, ND-21 teams can guide preventative maintenance measures and, when necessary, direct responses from a single locale.

Training in this environment comes in many forms. First, situational training scenarios are instantly available based upon the proximity of the three shift teams, shift overlap, and multi-customer support. In any dynamic environment, changing conditions will provide unique experiences for on-the-job learning. ND-21 enhances these opportunities because the lessons that are learned in a live environment on each customer network are either witnessed first hand or passed on when the next shift arrives. Under the CERT model, passing important situational lessons learned across several customer sites would be a giant undertaking.

Second, with ND-21 training offered within the InfoSec provider's organization now becomes accessible to the InfoSec team members because they are housed at the provider's headquarters. This allows larger, more focused providers with complete training programs the ability to provide their personnel with training maintenance and enhancement opportunities it would otherwise be far more difficult to offer with many personnel scattered across multiple sites.

Third, personal development opportunities outside of the provider would also be more accessible to provider personnel simply due to the fact that more competent replacements would be immediately available. With three shifts on staff at a single site, coverage overlap by personnel who had been groomed with similar and complementary skill sets would be a simple task to achieve and maintain. This would allow for training growth opportunities outside the provider organization that could be felt by all customers the provider supports. Similarly, such training opportunities could also be more readily shared throughout the staff due to their proximity and overlap.

3.2 The R&D Division

The R&D Division does just what its name implies and much more. R&D is responsible for many primary and secondary functions that support the overall effectiveness and goals of the ND-21 concept. In this mode, the R&D Division will be responsible for a number of tasks.

3.2.1 Hostile Tool, Script, and Virus Evaluation and Reporting

First, the R&D Division will be responsible for evaluating new and emerging hostile code, to include scripts, tools, and viruses. They will coordinate outside reporting and apply the lessons they learn from their own evaluation to the specific network defense requirements of customers. Additionally, they will work with the Analysis and Knowledge Divisions to coordinate web-based dissemination of evaluations.

3.2.2 Exploit Evaluation and Reporting

Second, the R&D Division will be responsible for evaluating and reporting on new and emerging exploits to systems and networks. Once again, these evaluations will focus on both the impact on specific customer networks as well as coordination and dissemination of information through the Analysis and Knowledge Divisions. The R&D Division will evaluate hostile code and exploits inside a closed test network. This test network will be a sub net of the greater closed training network within the ND-21 enterprise. In addition, where new exploits are uncovered within live customer environments, ND-21 will eradicate the danger and replicate the event on the test network to better determine corrective actions and future protections without impacting the customer networks.

3.2.3 Script, Tool, and Bot Development for CID Efforts

Third, the R&D Division will be charged with the responsibility of not simply evaluating hostile tools and scripts, but creating other scripts, tools, and bots to support CID efforts as well. The R&D Division will create custom scripts to act as trip wires and alarms across critical customer systems. They will also develop bots to scan log files for intrusion signatures and anomalies and for custom search profile creation to scour more regularly and efficiently not only the ND-21 and customer networks, but the open source community too.

3.2.4 Security Advisories

The R&D Division will be responsible for coordinating with the Analysis and Knowledge Divisions to post security advisories within the ND-21 enterprise and out to its customers as well as informational releases through major reporting agencies such as CERT/CC and the National Infrastructure Protection Center.

R&D Security Advisories will cover a wide variety of topics, to include hostile code, to exploits, potential and real vulnerabilities, new protective measures, scripts, and code, and new vendor product evaluations.

3.2.5 Training within the R&D Division

Training will be a large part of R&D efforts, both in-house for R&D personnel and outside efforts for the customer and greater community-at-large. First and foremost, the R&D training focus will center on a program of cross-pollination of skill sets. That is, each member's background and training will be passed throughout the team as will be the case in all ND-21 divisions.

Training within the R&D Division, like the entire ND-21™ team, will involve position shifts between divisions, internal classes and hands-on exercises, as well as external development opportunities such as DEFCON, Black Hat, and SANS.

3.3 The Knowledge Division

The Knowledge Division is the heart of training, awareness, education, and InfoSec policy in the ND-21 model. This division is responsible not only for internal training across the entire ND-21 enterprise, but for the following critical functions.

3.3.1 Policy and Procedure Development and Implementation

First, the Knowledge Division will develop a pair of base templates [one enterprise standard and one for military and U.S. intelligence requirements] of standard policies and procedures related to Information Security. This base set will then be adapted to fit each new customer's unique network requirements. Basic security standards do not change, nor do they go out of style. Thus, a template of strong, standard, yet flexible InfoSec policies and procedures can be built and still easily adapted to the dynamic environs of a live customer network.

3.3.2 Training and Awareness Efforts [Outside the Division]

Customer user security awareness is another major factor lacking in organizational information security. It costs customers in terms of money and security posture because a lack of security awareness makes it easy for potential intruders to use social engineering, hacking, and other ruses to gain access to networks and information they would otherwise be forbidden from accessing.

Basic security awareness is a large part of the ND-21 approach to ensuring that the entire customer enterprise is protected because, like training, this portion of ND-21 shores up the weakest link – the human one. Awareness programs within ND-21 could include an annual Security Awareness Week for all personnel within the organization, a Security Corner web presence within the customer Intranet for advisories and reminders, a security awareness presence within customer publications, events, and meetings, and a CEO/Commander-focused security training session demonstrating the simplicity of intrusion and its financial impact.

3.4 The Analysis Division

The Analysis Division will be responsible for managing the informational backbone and general knowledge base of the ND-21 enterprise. Working alongside the Knowledge Division, the

Analysis Division will be the web link to both customers and the greater community-at-large. Through the efforts of the entire ND-21 team, the Analysis Division will post exploit information, attack information, hostile code analysis, vendor product evaluations, and security advisories. Some of these services will be free to the public, others will be available on a for-pay basis. Additionally, the Analysis Division will provide customers with a valuable number of additional services.

3.4.1 The Information Warfare Warehouse [IW2]

More than a mere database, IW2 is an information store designed with the analyst in mind. It would be capable of storing data, mining data, providing automatic link and relational analysis [based upon in-house scripting], and would generate security reporting based upon pre-established criteria.

IW2 is designed to be more than a repository. For ND-21 customers, IW2 would also store and analyze their network traffic, assess potential vulnerabilities and penetrations, and alert the Active Defense Division when anomalies are found. Additionally, IW2 would provide redundant protection for customer networks by making customer network traffic data keyword searchable. IW2 would also utilize custom scripting and bot technologies to both mine open source and customer network data as well as scour its own information store for analyst-driven search queries.

With IW2, analysts could build, edit, and store search profiles as well as the search results they reap from their queries. These results are also available in a bot database to allow other users to adopt and utilize them as their own, seriously decreasing the time to search and preventing redundancy. Additionally, ND-21 analysts can schedule their search profiles so that the queries can be rerun at predesignated times in the future as determined by analyst needs.

3.4.2 Predictive and Proactive Link Analysis

IW2 could be scripted to provide predictive and link analysis throughout the entire ND-21 data set. But even advanced automation capabilities only take the analysis process so far. Truly effective analysis still requires human input. While the custom programming of the R&D Division is designed to support and supplement human analysis, it is never intended to fully replace it.

The Analysis Division would be responsible for the maintenance of IW2 as well as applying the advanced tool technologies in the pursuit of proactive analysis and profiling of every type of threat entity, from non-state hackers to virus writers to foreign intelligence services, the criminal underworld, and terrorists.

Who are the potential threats? What capabilities and skill sets do they possess? Who trains them, and whom are they talking to? How can the CID processes be improved to stop them? These are just a few of the questions the Analysis Division would be charged with asking, and would work side-by-side with the other ND-21 divisions to find the best solutions.

3.4.3 The Need for an Independent Mobile Code Rating System

Viruses, worms, and trojan horses are all well-documented dangers and are rated as to their threat to networks by a few anti-virus authorities to tell them which ones are most dangerous. But these authorities are commercial anti-virus entities, mostly vendors such as Network Associates® and Symantec®, who do a scant job in providing an accurate assessment at best. This is because it is in their best interest, financially, to promote the broadest possible danger standards. Moreover, there is no variable factor in any of the major hostile code rating criteria currently in use, and no independent, credible, non-AV organization is providing truly accurate assessments of the threats. ND-21 would include, as a service to customers, an independent hostile code rating system for the community-at-large. The rating system would assess the hostility and threat of each piece of hostile code based upon the overall effectiveness of the code itself and its potential to damage versus any factors related profit motive. This service could further be tailored to better assess the security concerns of individual customers based upon the SMC-RS™ model designed by Robert Bagnall and Geoffery French of Veridian-Trident Data Systems.

4.0 Conclusion

It was the author's intent to layout one possible solution: a 21st Century active security architecture to effectively defend a network in a real-time sense rather than the static, reactive, expensive defense models that exist in the industry today. While no solution is the only option, the author considers ND-21 to be the most viable given the current culture, market, and technologies that exist in the Information Security field.

Net Defense-21 is one potential future of InfoSec. It is CID, CND with a proactive, automated focus, and lies at the very heart of dynamic protection because it is built upon on an active defense concept. ND-21 shores up the gaps in certain weak defenses, leaves others as they are, and eliminates still others entirely in favor of more flexible solutions. Foremost in the author's mind, however, is always the end user – both the weakest link in the chain and the largest influence on the overall security posture. Because in the end we are all users, and it is the user who will ultimately make or break the success of InfoSec efforts no matter how large the enterprise.