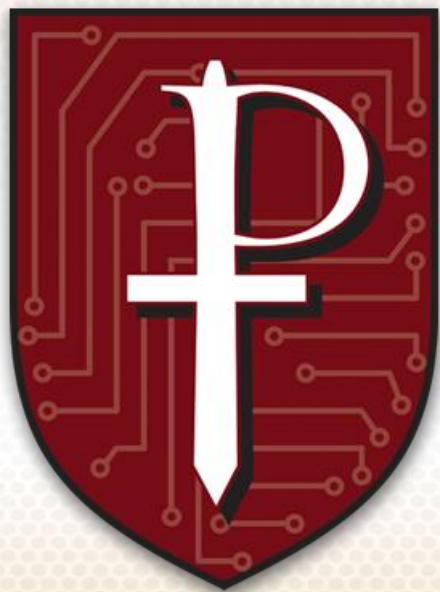


Solving the Cyber Security Puzzle

v1.2

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

As with many of the challenges facing today's society, the problems encountered in the area of cyber security are varied and complex. The threats are serious and dynamic. The assets being protected are critical to the well-being of people, organizations, and nations. The available safeguards are numerous, sophisticated, and sometimes overlapping. The challenge of finding a solution can seem overwhelming.

The challenge is similar to a complex puzzle. My son recently received a puzzle as a gift. The puzzle seems simple at first glance but it actually has over 300,000 wrong solutions. So it is with cyber security. There are many ways to almost solve the cyber-security puzzle and yet miss the real solution.

The title of this whitepaper may seem overly optimistic. Is it even possible to solve a complex puzzle where some of the inter-related pieces are constantly changing? If it is possible, what methods are used to find a solution? The answer is yes and the method is the time-tested technique of solving the puzzle one piece at a time. By classifying and examining the basic areas of cyber security, this whitepaper will identify which pieces of the puzzle are well understood and which need more work. By understanding the pieces, we can understand how they can fit together to provide a practical solution that can be implemented and maintained.

Terminology

A consistent set of terminology is needed for us to have any chance of solving the cyber-security puzzle. Words have meaning; for two people to use the same words while each is thinking of a different meaning causes confusion and throws unnecessary obstacles in the path to a solution.

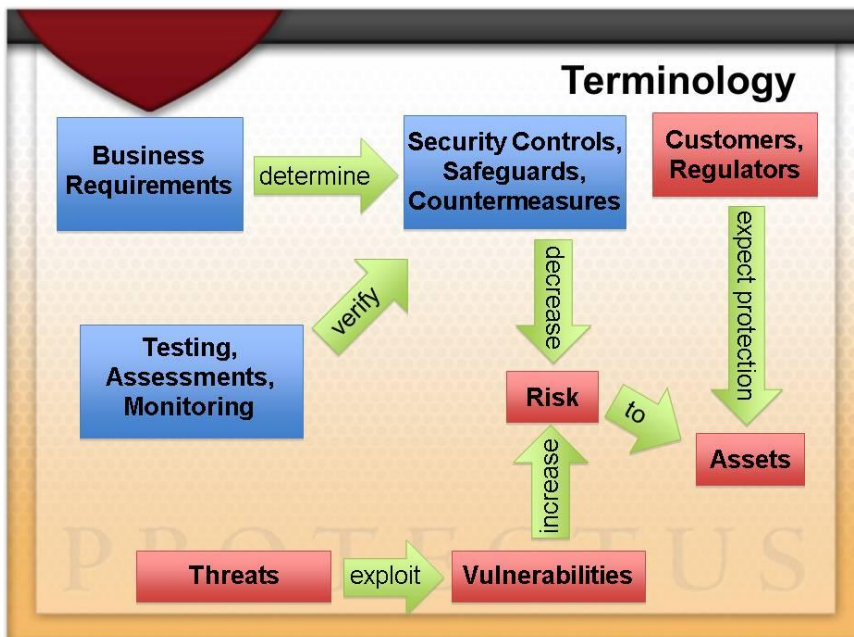


Figure 1 - Terminology

Inaccurate terminology makes the puzzle that much harder to solve. While a dictionary style list of terminology is useful, a picture is a more intuitive way of conveying meaning. Figure 1 is a

concise graphic conveying the proper use of significant terms and relationships between major areas within the field of cyber security. These are the pieces of the puzzle. We strive to make Figure 1 as simple as possible. Each term represents a basic area of focus in the field of cyber security. Now, we will add a few more descriptive words to each term and lay the groundwork for identifying which areas need the most work.

Assets

What are the assets being protected? Within the cyber-security context, assets are generally thought to be in the form of information or data. However, we must remember that the information being protected is often a means of access to, control of, or location of real people or some type of tangible asset. Although assets vary from organization to organization, there are some common categories:

- Data
 - Strategic and tactical information
 - Account & credit card numbers
 - Personal information
 - Customer lists
 - Source code
 - Design documents
 - Intellectual property
- Brand / Reputation
- Applications



***Never spend \$10,000
protecting a \$1000 asset.***

Knowing the assets you want to protect is important so security resources can be allocated properly. When a dollar value can be assigned to an asset, it makes no sense to spend more protecting it than the asset is actually worth. Never spend \$10,000 protecting an asset worth \$1000. Of course, when peoples' lives and safety are at stake, then it is not about the dollars but about keeping people safe.

Risk

Risk is the chance of loss occurring. Note that risk is expressed in terms of a probability or a percentage. Sometimes, a more generic descriptor is used to describe risk – such as “high risk” or “low risk”.

Safeguards

Safeguards are tools and techniques used to minimize risk to assets. Other names such as countermeasures or security controls are sometime used to describe safeguards. Safeguards include tools such as firewalls, anti-virus software, anti-spyware software, Virtual Private Networks (VPNs), encryption tools, passwords, tokens, biometrics, and Intrusion Detection

Systems (IDS). Safeguards also include techniques such as changing passwords, applying patches, and implementing data backup mechanisms.

Testing

Testing is the verification of existing safeguards. Vulnerability scanning and penetration testing are examples.

Threats

Threats are the source of potential or actual harm. Also, circumstances with the potential to cause harm can be considered a threat.

Vulnerabilities

Vulnerabilities are flaws, misconfigurations or weaknesses that leave the opening for an attack or increase susceptibility to an attack.

Incident

An incident is an instance of a threat exploiting a vulnerability. Although different organizations will have varying definitions, an incident is normally associated with an organization being harmed in some way or being targeted by an attacker with the intent to do harm.

Room for Improvement

Much work has been done over the years to quantify risks, implement and test safeguards, assess threats, minimize vulnerabilities, and define incident respond methodologies. Accomplishments in all of these cyber-security areas have been useful and necessary. However, certain areas are naturally more developed and better understood than others. Many cyber-security areas are well enough understood that they only need sufficient resources to be dedicated, thereby allowing experienced personnel to apply well known principles. For areas that are well understood, having a poor outcome is caused when the basic concepts are not applied or the available tools are not used.

Risk assessments are an example of an area that has well-understood concepts, well-defined methodologies, and there is not much room for major improvements. A risk assessment may be poorly written and contain inaccurate results, but that is because the known methodologies were not properly applied - not because the methodologies were unavailable. This makes sense because many of the cyber-security risk management techniques and concepts have come from and are based on centuries of practice protecting assets from threats. The moat around a castle, for example, is a form of perimeter defense similar in concept to a firewall on a network. Extending this analogy, the Virtual Private Network (VPN) is similar to the castle drawbridge.

The OSI Model

The Open System Interconnection (OSI) model describes a layered architecture through which data flows from one computer through a network to another computer. The OSI model has seven layers that interact with adjacent layers:

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

The model divides the overall data communications problem into seven smaller pieces and makes it easier for vendors to create interoperable network devices and applications.

The popular Transmission Control Protocol / Internet Protocol (TCP/IP) model can be loosely mapped to the OSI model although there are different interpretations about exactly how the mapping is made.

Note that in both the OSI model and the TCP/IP model, the lower layers, involving bits on a wire, are very well defined while the upper layers, involving presenting data and interfaces to users, are less well defined.

One cyber-security area with room for improvement is safeguards. While many effective safeguards are available, some relatively new safeguards are still maturing. In some cases, considerable research and development effort is still needed to make certain safeguards practical, allow them to become truly effective, and bring them to the common use in the marketplace. One safeguard that is still in its infancy and has room for improvement is network security monitoring.

It is our position that network security monitoring is one of the weakest, possibly the weakest, of all safeguards available on the market today. Network security monitoring solutions sometimes go by the name of Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). The concept is simple – look for and identify or block malicious traffic. It turns out that performing network traffic monitoring in a way that actually delivers value is very difficult.

Since network traffic is invisible, providing any information at all about it can be valuable. But the most value comes from extracting as much information as possible from network traffic, automatically identifying malicious traffic, and presenting results in an intuitive format. Very few organizations even know what traffic is on their network let alone know if any of that traffic is a security threat. Traffic analysis allows the invisible to become visible.

The limitations of existing network security monitoring tools is not because the tools are broken or because the topic has been neglected but rather because network security monitoring is a relatively new area and is a difficult problem to solve. This is especially true when compared to the centuries that risk-analysis techniques have been used. There is still much work to be done in the area of network security monitoring.

The Model

A model is often used to provide a simplified representation of something complex. A model for network security monitoring will help demonstrate where existing tools fit into the overall

picture and also where new tools and techniques might provide improvement. Models help us to understand a complex problem and break it down into a set of smaller problems to be solved.

An example of a successful networking model is the Open Systems Interconnection (OSI) model. The OSI model defines seven layers and has been instrumental in allowing vendors to build compatible network equipment. See the sidebar on the previous page for additional information about the OSI model.

We propose a general model that can help to identify areas for improvement to network security monitoring. We give the model a more general name of Cyber Defense Traffic Analysis Model, which includes network security monitoring but can also include other relevant areas such as general network traffic or performance analysis. The model is shown in Figure 2.

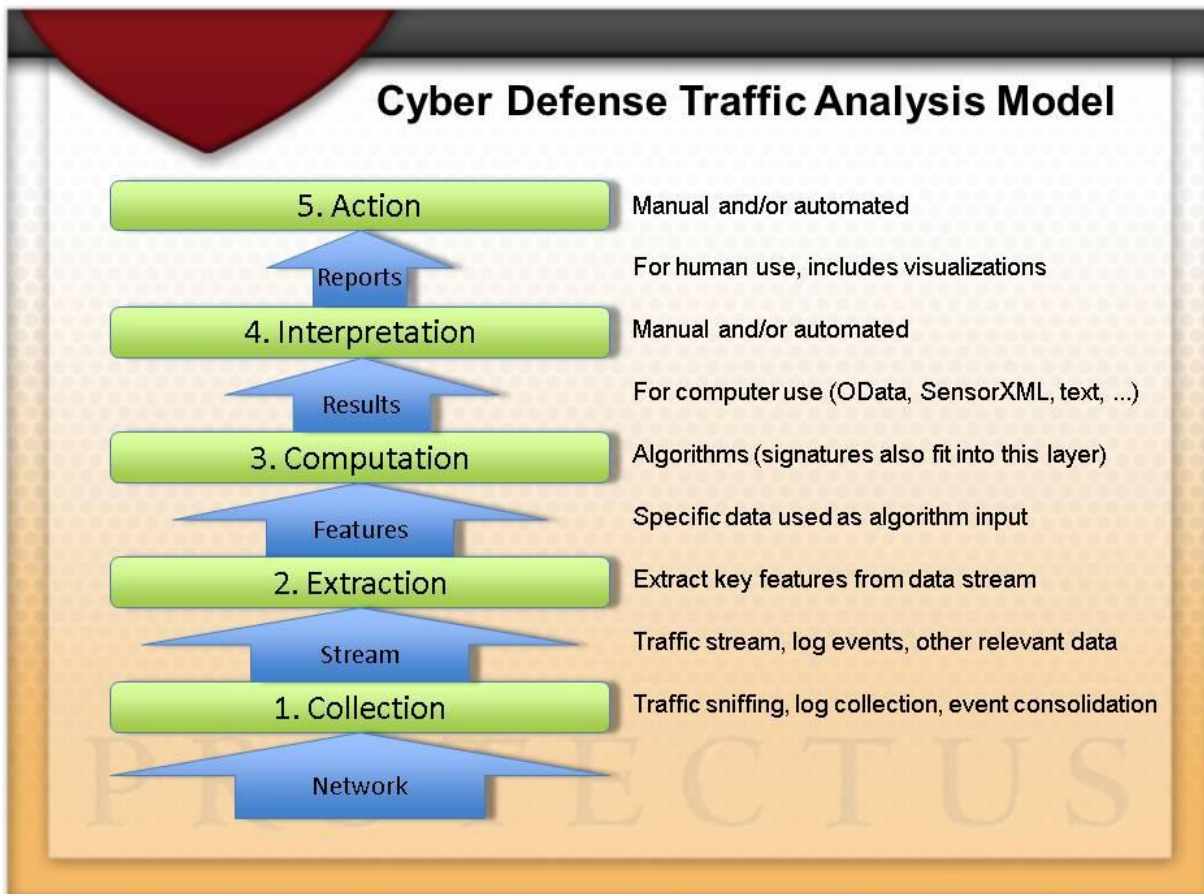


Figure 2 - The Cyber Defense Traffic Analysis Model

In Figure 2, green represents functional layers (similar to the OSI model) and blue represents data flow. Of particular interest is the opportunity for development of new algorithms in layer 3 (Computation). While new algorithms will provide improved methods to identify malicious traffic with fewer false positives, no algorithm will be 100% accurate all of the time. Therefore, presentation of and interpretation of results in layer 4 (Interpretation) is a vital step to any practical solution providing real value on real networks. As improved algorithms are deployed in layer 3 and results are efficiently and accurately interpreted in layer 4, there is room for increased automation in layer 5 (Action), to allow for active network defenses.

Although the model is primarily intended for use with newer algorithms, it is generic enough to be applied to signature-based traffic analysis techniques. Figure 3 shows how the popular Snort IDS system maps to the model.

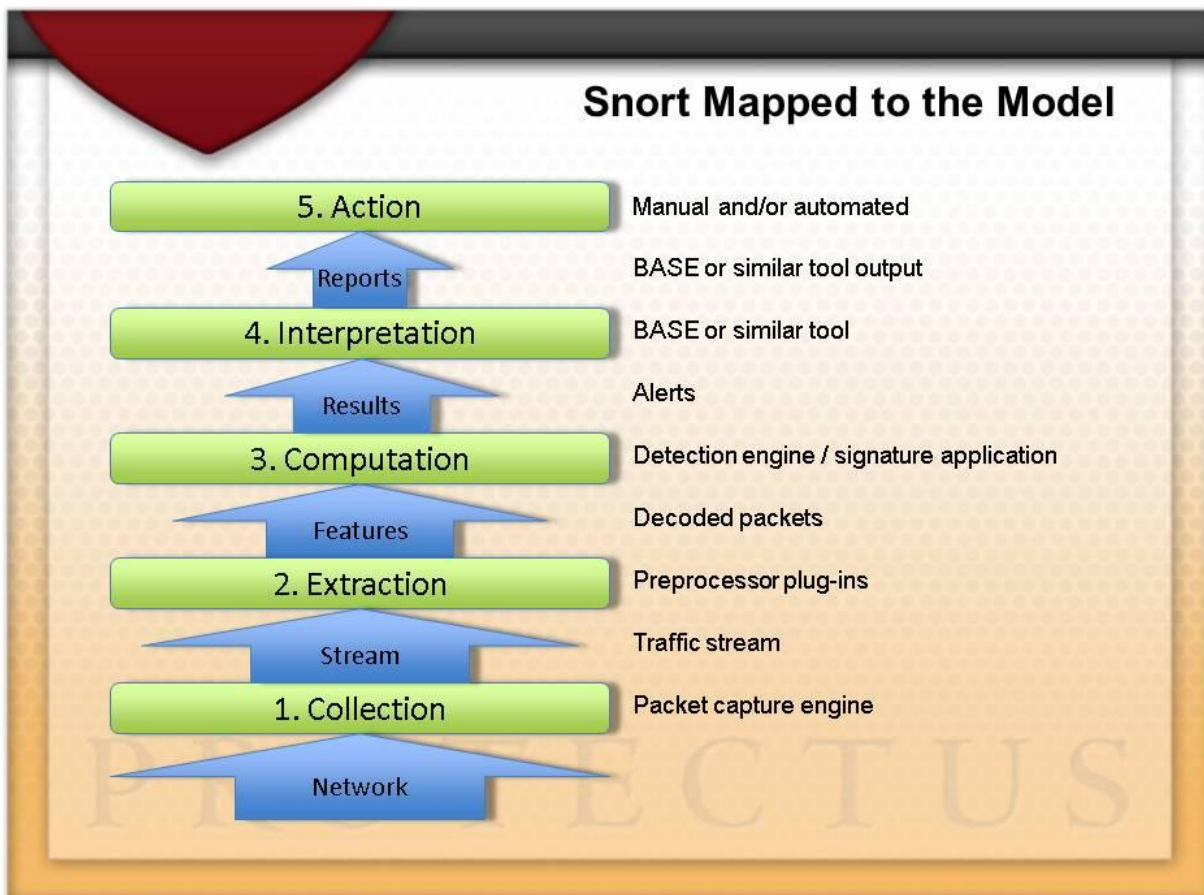


Figure 3 -Snort Mapped to the Model

Figure 3 shows one example of mapping Snort to the model. Other examples could be shown depending on how Snort is implemented and the supporting tools used for alert processing.

Similarity with the OSI model can be seen in that the lower layers, dealing with bits on a wire, are the most stable, well defined, and best understood. While there is room for speed and performance improvements in the lower layers, the middle and upper layers have the most potential for future improvements. Independently developed point solutions are most common in the middle and upper layers. With the currently available upper-layer point solutions, it is common for cyber attacks to remain undetected. We believe that the most room for improvement lies in identifying improved algorithms and developing tools to more intuitively interpret results.

Conclusion

Solving the cyber-security puzzle is possible by recognizing which pieces need the most work and making improvement in those areas. Of the available cyber-security safeguards on the market, network security monitoring is one that has the most room for improvement. The Cyber Defense Traffic Analysis Model helps to show that the lower layers of the model are relatively well developed while the middle and upper layers have the most room for improvement. By identifying new algorithms and providing analysts with improved tools for interpretation of results, organizations can enable automated actions and implement active network defenses.

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.