Designing a Collaborative Defense System

[1,2]*Wen-Yi Hsin**, [1,3]*Shian-Shyong Tseng*, [1]*Shun-Chieh Lin*
[1]Department of Computer and Information Science, National Chiao Tung University
[2]Hsin Chu County HuKou High School
[3]Department of Information Science and Applications, Asia University
[*]E-mail: shin@hkhs.hcc.edu.tw

摘要

本篇論文提出一個以警報資料為基礎的聯合防禦解決方案。大量日誌記錄與警報資料很難分析，造成系統管理員無法掌控狀況且無法針對事件的處理做出立即的決策。我們延伸分散式入侵偵測的模式，提出一個聯合防禦的架構，包含警報收集、萃取、分析、回報、資料倉儲和分析。此外我們發展一個混合式的安全資訊分享的方法，就像升起狼煙警告其他夥伴一般，參與電腦安全事件回報團隊的成員能獲得安全防禦相關的解決資訊。這個架構提供學術界和企業界一個建立有效合作的安全聯防團隊方案。經由評估實驗，並追查出 SQL Slammer 蠕蟲的傳播情形。結果發現，透過聯合防禦的機制，廣泛部署系統，能更加準確地追查出攻擊的行為，並且可以協助成員評估威脅的衝擊和採取適當的行動來降低風險。

關鍵字：聯合防禦、合作式安全系統、分散式入侵偵測系統、事件回應、電腦病蟲

ABSTRACT

This paper proposes a lightweight alert-based collaborative defense solution. Because it is hard to analyze a large number of logs and alerts, the administrator can not control the situation and make decision immediately. We propose a framework for collaborative defense by extending the original distributed intrusion detection model. It contains alert's collector, extractor, analyzer, report's generator, alert warehouse and alert's analysis. Besides, we develop a hybrid approach to share security information like raising the wolf smoke to warn partners. By the security information sharing, the members of CSIRT can obtain the solutions of defense, such as blacklists, detection rules, and security knowledge about alerts. The framework provides a solution to build effective cooperative security teams for academia and industry. We evaluate the feasibility of our framework and track the spreading behaviors of the SQL Slammer Worm. As a result, we can deploy security system more widely and detect the aggressor's behavior more accurately. The alert-based collaborative defense mechanism can help members to evaluate the impact of the threats and take proper actions to mitigate the risk.

Keywords: Collaborative Defense, Collaborative security, Cooperative Intrusion Detection, Distributed Intrusion detection, Incident Response, Worm

1. Introduction

Modern Security Systems encounter many predicaments. First, multiple security system such as a network based IDSs may flag millions of alerts per day, which may overwhelm the analysts. Second, among a large volume of alerts, a high proportion of them are false positives, some of them are low-severity alerts and some others correspond to severe attacks. It is challenging to differentiate these alerts and take appropriate actions. Third, different security systems usually run independently and may flag different alerts for a single attack.

As we know, the size and complexity of the Internet makes it likely that there will continue to be vulnerabilities in the future. The privacy issues also complicate the sharing of information on intrusion activity between networks, e.g., the reports of specific port scanning methods and attacks might be very little broad understanding of intrusion activity on a global basis. Because of these challenges, current best practices for Internet security rely heavily on word-of-mouth reports of new intrusions and security holes through entities such as CERT [CERT04] and DShield [DShield05]. Since malicious attack is difficult to prevent in the enterprise interior, Logs and Alerts is huge and hard to analyze. So the administrator can not control the situation and make decision immediately. With Worm, Virus, Trojan spreading rapidly, the scale of the problem is large and growing rapidly. The individual attacks take over one million machines, more and more successful attacks. Therefore, to share security information between million machines to collaborative defende malicious attacks with partners are important.

We have proposed a framework for collaborative defense by extending the original distributed intrusion detection model [HT+05]. The framework provides a solution to build effective cooperative security teams for academia and industry. The alert-based collaborative defense mechanism can help members to evaluate the impact of the threats and take proper actions to mitigate the risk. In this paper, deploy this framework in experimental network environment to detect the aggressor's behavior more accurately and evaluate the feasibility of our framework.

NSC94-2752-E-009-006-PAE

2. Related Work

DShield [DShield05] is a distributed intrusion detection system, which collect crackers' activities from all over the Internet by collecting the log of firewalls shared from Internet users. It can be used to discover trends in activity and prepare better firewall rules through monitoring the statistics Top N port number and IP address, and the trend analysis which includes increasing (positive) or decreasing (negative) in activity of the last two days during 33 days. The definition of Computer Security Incident Response Teams (CSIRT) is that an entity with a security role or responsibility in a given organization has a communication and collaborative component with other internal or external related entities [WS+98] [Masurkar03-1]. The European CSIRT Network (eCSIRT.net) is a Distributed IDS Sensor Network [European04], which is a globally project to provide the resources for a distributed IDS sensor network monitoring specific honeypot systems for exchanging experiences and knowledge, establishes pilot services, and promotes common standards and procedures for responding to security incidents. Symantec DeepSight™ threat management system [DeepSight05] is an example of a centralized scheme, where sites can opt-in and share their IDS alerts.

It is important for collaborative defense to share information in order to discover attacks involving multiple organizations. Sharing information among IDS is important, especially for the purpose of detecting coordinated intrusions and intrusions distributed across a set of hosts and network elements. At present the Information Sharing solution mainly has two kinds; the first kind is Web-based information like FIRST [Masurkar03-2] and DShield, and the second kind is XML messages like CSIRT and eCSIRT (IDMEF [CD01] and IODEF [HS03]). We use SQL's DML to publish/subcribe data.

3. Framework

As mentioned above, the collaborative defense system that is operating at present can't meet the demand of medium and small-scale organizations. Therefore we propose a system framework for the network administrators. We have referred to related studies about distributed intrusion detection and CSIRT to outline our approach to the problem. In the intrusion detection field, an alert is a message from an analyzer signaling that one or more events of interest have been detected. We say that an alert is a kind of event, since it reflects the state of IDS [MM+03]. We design a component called "CSIRC", referring to "Computer Security Incident Response Center", in every collaborative organization.

The system requirements focus on the interaction of the entire collaborative defense system with the viewpoint of management. Such management environments are often capable of handling hundreds of alerts per second. Basically, the intrusion detection system must integrate with the management platform, and ensure an easy configuration and a certain level of performance. But the requirements of collaborative defense system are more and complicated. It must contain collaborative, modularity, scalability, heterogeneity, availability, and decentralization.

3.1 Architecture Design

We present an approach to organizing autonomous but cooperative component systems to detect distributed attacks and exchange information. Our approach is based on the dependency among the distributed alerts in a signature. Unlike the hierarchical architecture, we organizes the cooperative IDSs according to the intrinsic relationships between the distributed alerts involved in attacks, and, as a result, a Local CSIRC needs to send a piece of information to Global CSIRC only when the information is essential for detecting the outer attackers. The target of our design aims mainly at the academic use as well as at industrial purpose. It can cooperate with the hierarchical structure of enterprises and take the limitation of network's bandwidth into consideration.

Collaborative Defense Model

Firstly, we propose a basic and hierarchical model for constructing Collaborative Defense System. We can represent the model in a simple diagram as Figure 1 [HT+05].

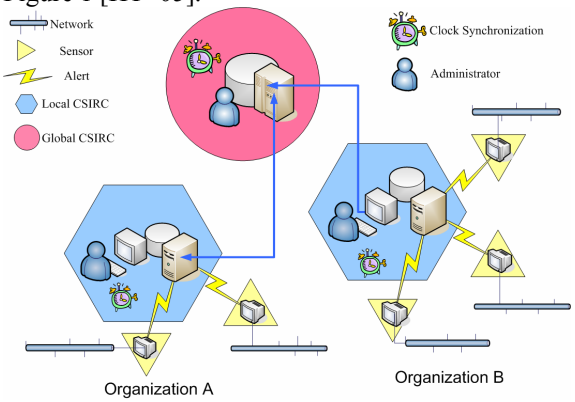

Figure 1: Collaborative Defense Model

Inside the Collaborative Defense Model, Several companies or schools organize Computer Security Incident Team (CSIRT). The CSIRT cooperates by using a hierarchical communication framework. This cooperation is driven by interests expressed by the CSIRTs.

This model can divide two levels: *Local View* and *Global View.*

Level 1 Local View: Here we present a framework for doing distributed intrusion detection with centralized analysis components. We design a local CSIRC to collect alerts data from sensors which are deployed in different sub network of organization. Then the local CSIRC extract, store and analyze these alerts, and send the alert selected to global CSIRC.

As Figure 1 shows, the red circle represents global CSIRC, the blue hexagons are local CSIRC, and the yellow triangles indicate IDS sensors. Establish a Global CSIRC to coordinate the sub-organizations. Install the CSIRC component in every organization. Set up the IDS's sensors in different sub networks.

Level 2: Global View: CSIRTs cooperate by using a hierarchical communication framework. The local CSIRCs report information to the global CSIRC. It is a very important task for the global CSIRC to coordinate the members of CSIRT. The purpose of the global CSIRC would be to offer a means to coordinate intelligence related to possible cyber attacks and provide a conduit to warn collaborative organizations that such attacks may take place. The Global CSIRC plays a security consulting role serving as a clearinghouse for security information.

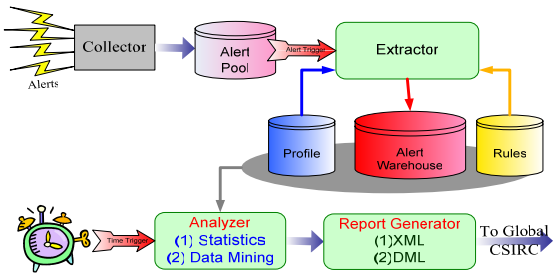

Figure 2: CSIRC

Computer Security Incident Response Center

Let us introduce the components of CSIRC as following. And please refer to the Figure 2.

(1) Collector: The component of Collector is responsible for collecting the alerts from sensors. Then the collector puts alerts to a temporary storage called "Alert Pool," due to the consideration of decreasing processing time and increasing storage capacity before the system collect huge alerts.

(2) Extractor: When Alert Pool receives alerts, it will trigger the extractor. The main task of Extractor is to extract alerts according to the definition of local profile. By the way, we can reduce, filter and classify alerts in order to prepare for long-term analysis.

(3) Analyzer: The second stage focuses on the data analysis of long-term alerts. The Analyzer component makes periodic analysis of alert, such as per hour or per day. The analysis method may be divided into two categories: statistics method and data mining. The purpose of the analysis is to summarize the alerts and look for the abnormal threat.

(4) Reporter: The Reporter reports to Global CSIRC the abnormal alerts as well as the result of analysis. At the same time, it shares information with other Local CSIRC on suspicious alerts and determines when to be more vigilant or more relaxed.

3.2 Alert Extraction

As mentioned in related works, on any given network, on any given day, any IDS's sensor can fire thousands of alerts. How can we deal with so many alerts? How can we find the real threats and vulnerabilities? We have designed a component of *Extractor* to do extraction of alerts. The Alert Extraction functions act as the module of classifying, filtering, labeling, and aggregating. It will solve the following problems: (1) Work division between the cooperative organizations. (2)How to make proper response policies? (3)How to avoid alert flooding? At the same time, alert extraction might be useful for estimating speed of propagation of alert.

From the administrator's viewpoint, it is very important to deny attacks from outside and try to find victims inside. Based on the principle of responsibility division, we classify alert in a simple way and make different policies reacting to different categories of alerts. We divide alerts into four categories according to the sources and the targets.

(1) *A1*: Both of the sources and the targets are the computers inside the organization. They are classified as inner attack events. For this kind of alerts, our response policy is to notify the users to carry on safety inspection and patch mending.

(2) *A2*: The inside computer attacks the computer outside. The reason for the attack is the computer may be infected by Worms or Trojans; perhaps it is the misuse of the users. The response policy of A2 alert: Notify users to carry on safety inspection and patch mending. A1 and A2 are the inner events which the administrator must eliminate the vulnerabilities immediately. They are the responsibility for the local administrator.

(3) *A3*: A3 alerts are the outer event which should be blocked from WAN and reported to the global CSIRC. The response policies of A3 alert: First, undergo the safety and vulnerabilities inspection for the victims. Secondly, we will act as a defense against the threats; for example, establish the rule of firewall to keep out the attackers. Thirdly, notify this kind of incidents to other cooperative organizations.

(4) *Others (Exceptions)*: Besides the three kinds mentioned above, there are some exceptions. For instance, the sources of the attack may not be in the range defined by the profile. The response policy of exceptions: Notify the administrator to check the detail of alerts. They are the responsibility for the local administrator.

To extract alerts according to the definition of the profile might be useful for estimating the speed of propagation of attack information.

Rule 1: Each alert mentioned above is assigned exactly to one alert type.

Rule 2: If Local.Priority or Alert.Priority=high then send alert to Administrator and Warehouse and Labeling "urgent".

Rule 3: If SourceIP included in LocalIP then send to Exception and Labeling "Inner event".

Rule 4: If Target IP included in LocalIP then send alert to Warehouse and Labeling "defend"
Else send to Exception.

Rule 5: If TargetPort included in Port.WhiteList send

to Warehouse and Labeling “service attack”
Else send to Exception and Labeling “try attack”

3.3 Alert Analysis

The alert analysis is a very extensive research issue. As mentioned earlier, there are a lot of ways in the analysis of alert. Alert analysis is an investigation into a network incident. In order to assess the risk to your organization as well as to evaluate the impact of the incident and take actions to mitigate the threats, we make use of two simple methods to analyze alert data, trend analysis and association rule analysis.

Our trend analysis focuses on the amount and categories of alerts, the variation of the amount, and the first offense of alerts. Association analysis can help us find the frequent co-occurrences of attribute values belonging to different attributes that represent various alerts. For example, through association analysis, we may find many MS-SQL Worm attacks are from the source IP address 61.159.15.X to the target IP address 140.126.167.Y at the destination port 1434. After association rule analysis, we can get the results of frequency, support and confidence for alert type and the sources. A sample result of association analysis is as follows.

Source =[192.168.2.30] ➔ Alert=[4] AND Dest=[192.168.1.2] Support=85.639% Confidence=99.942%
Source =[192.168.2.30] ➔ Alert=[4] AND Alert[13] AND Alert[20] Support=70.328% Confidence=90.153%

4. The Experiment of Deploying System

4.1 Experimental Environment Description

Our experiment environment is set up in the academic network including an experimental CSIRT and several members, e.g., KDE Lab in NCTU, Hukou High School, HsinChu County Network Center, two elementary schools and two junior high schools in HsinChu County of Taiwan, for the evaluation of the Alert-Based Collaborative Defense (ABCD).

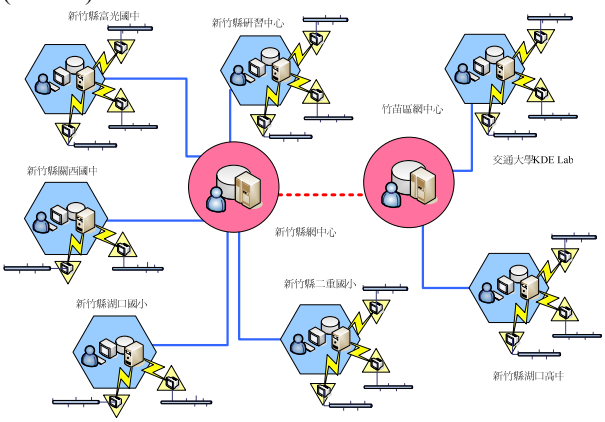

Figure 3: Our Experimental CSIRT

Some of the basic profile of the experimental environment in this ABCD system is shown as Table 1.

CSIRC	IP Range	Sensors	Service	Priority	Bandwidth	Hosts	Firewall
HKHS	140.126.167/24 163.19.12/24	7	Open	2	1.54M 3M/640K	<300	Yes
HCC	163.19.0/24 ~ 163.19.103/24	3	Half	1	>100M	>1000	Yes
HCC1	163.19.30/24	1	Open	3	3M/640K	<100	NO
HCC2	163.19.41/24	1	Open	3	3M/640K	<100	NO
HCC3	163.19.64/24	1	Open	3	3M/640K	<100	NO
HCC4	163.19.82/24	1	Open	3	3M/640K	<100	NO
NCTU	140.113/16	2	Open	3	>100M	>1000	NO

4.2 Data Schema

In data treating processes, the jobs of data transformation and storage play a very important role. The Alert Pool provides a temporary storage for IDS’s Alerts. The design purpose is to avoid too many alerts simultaneously resulting in processing time not enough. Therefore, we have designed one more collection tier. The alert data are saved in the original IDS’s alert format.

In the profile, we can find specification about sub-network, including basic information of network administrator, sensors, hosts, and network. The profile describes the environment of the network, just like to build a model. Properly modeling the network allows the importance of each alert to be correctly assessed. Furthermore, the profile offers data for extraction and analysis, for instance, to classify the alerts or determine whether they are false alarms. Therefore, the data in the profile are like a “White list” which tells us what’s normal.

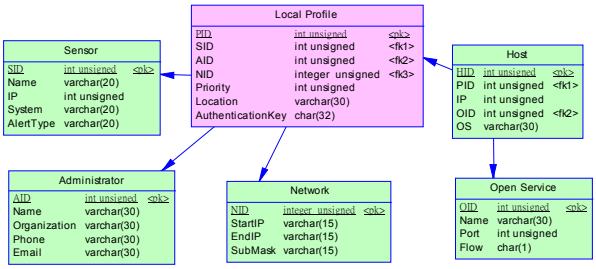

Figure 4: The Schema of Profile

We build an alert warehouse. The objectives of the long-term data warehouse resemble those of the original data management. The alert warehouse can provide evidence for *computer forensics* and serve as data source for future *data mining*.

In Global CSIRC, we used MS-SQL Server 2000 software to construct the distributed database environment and manage the huge dataset over 6,000,000 records. We used the SQL DML statements to publish and subscribe alerts between the Local CSIRC and Global CSIRC. Combining the Data Transformation Services of MS-SQL, we can automate processes to extract, transform and load alert data from other CSIRCs. The examples of DML statements are:

Statement 1: Subscribe A2 Alert

```
SELECT    *
```

```
FROM   All_Alerts
WHERE (ip_src BETWEEN Profile.StartIP AND
Profile.EndIP)  AND  (ip_dst  BETWEEN
Profile.StartIP AND Profile.EndIP)
ORDER BY   [timestamp]
```

Statement 2: Subscribe A3 Alert of T-day

```
SELECT   *
FROM   All_Alerts
WHERE ((ip_src NOT BETWEEN Profile.StartIP
AND Profile.EndIP) AND (ip_dst BETWEEN
Profile.StartIP  AND  Profile.EndIP)) AND
([timestamp] BETWEEN ' T-day 00:00:00' AND '
T-day 23:59:59')
ORDER BY   [timestamp]
```

Statement 3: Top N List of Attackers

```
SELECT   ip_src AS Attacker, COUNT(ip_src) AS
Counts
FROM   A3_Alerts
GROUP BY   ip_src
ORDER BY   Counts DESC
```

4.3 Experimental Result

In Global CSIRC, we used MS-SQL Server 2000 software to construct the distributed database environment. We collected over 6,000,000 alerts in the three main CSIRCs including HKHS, HCC and NCTU from March 25 to May 25, 2005. We used the SQL DML statements to publish and subscribe alerts between the Local CSIRC and Global CSIRC. Also, we used Data Transformation Services of MS-SQL to automatically extract, transform and load alert data from other CSIRCs periodically. The followings show the Local View and Global View Let of the ABCD system.

Local CSIRC

There are at most 180,000 alerts every day in the CSIRC of HKHS. Figure 5 shows the amounts of alerts in the campus have periodicity; the days illustrated as circle are Saturday and Sunday and April 5, 2005 is a holiday.

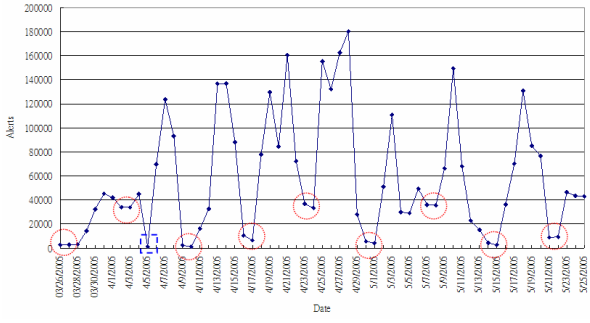

Figure 5: Periodic change of alerts

In the A1, there are many SNMP alerts and ICMP redirect alerts because of the faults of network management. In the Exception, we forgot considering these IP addresses: 255.255.255.255 (broadcast address) and 224.0.0.0~ 239.255.255.255 (the IP address of Class D for Multicast). These addresses are inner IP added into Local Profile. Also, the killer of bandwidth could be immediately discovered using top N of A2 alerts.

Global CSIRC

The Global CSIRC provides the statistics of alerts and attackers, which can help administrators understand the trend of threats and making proper decision.

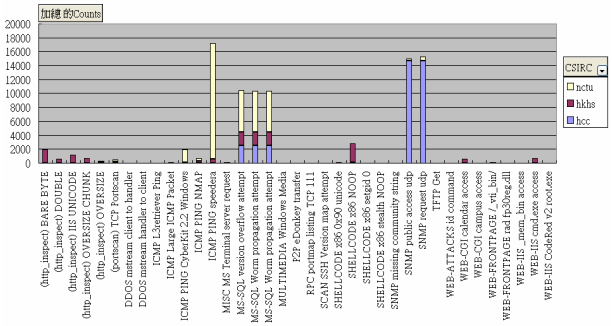

Figure 6: The bar chart of global Alerts

4.4 Case Study

The A3 alerts in the Global CSIRC can be used to track the behaviors of the Worm propagation. The SQL Slammer Worm, which is attack victim through 1434 port with UDP flow, is discovered by ABCD system during our experiment.

In Figure 7, an alert corresponding to an attempt of propagation of the MS-SQL worm is shown. Through our ABCD system, we can easily understand the situations of the attacks of MS-SQL Worms. In the duration of A, there are two immediate sharp increase and decrease. At the time of B, the CSIRC of HCC had added a rule to firewall to block the connections by port 1434. Therefore sensors did not detect the worm again after April 9. In the duration of C, the CSIRC of NCTU joined in the team. The amount of MS-SQL Worm alerts is a steep rise. In the duration of D, The amount of alerts falls right down to the lowest point in NCTU because its CSIRC had crashed down. Finally, it shows the MS-SQL worms spreading again.

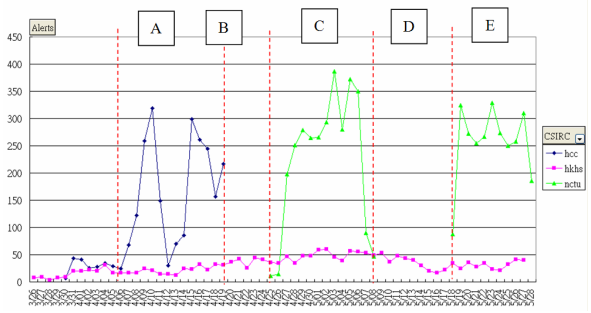

Figure 7: The spreading MS-SQL worm

From the Global CSIRC, we can gain the information of defense, such as Top N of attacker. It can be used to discover trends in activity and prepare better firewall rules. The range of the unfriendly IP from the statistics of connections in the Global CSIRC could be also obtained. Based upon the MS

Analysis services, several attacks could be easily visualized. We also can find the range of the unfriendly IP from the statistics of connections in the Global CSIRC as shown in Figure 8.

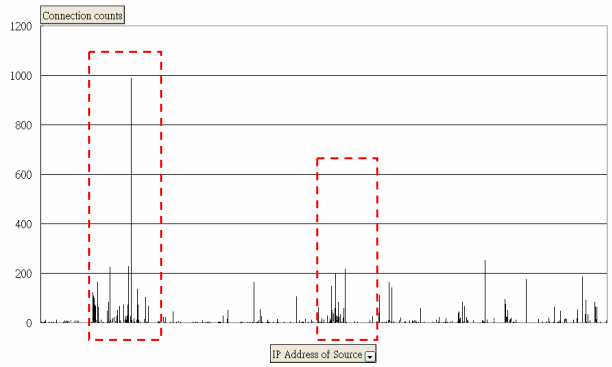

Figure 8: The distribution map of attackers' IP

5. Conclusion and Future Work

In this paper, we deployed an alert-based collaborative defense framework on a Hsinchu county, Taiwan environment to exchange alerting information for detecting distributed attacks. The spreading behaviors of SQL Slammer Worm are discovered during our experimental in real world. As a result, the alert-based collaborative defense mechanism can help members to evaluate the impact of the threats and take proper actions to mitigate the risk.

Acknowledgement

This work was partially supported by National Science Council of the Republic of China under Grant No. NSC94-2752-E-009-006-PAE.

References

[CD01] David A. Curry and Herve Debar, "Intrusion detection message exchange format data model and extensible markup language (xml) document type definition", Internet Draft, draft-ietf-idwg-idmef-xml-03.txt, February 2001.

[CERT04] CERT Coordination Center, URL: http://www.cert.org/, 2004.

[DeepSight05] DeepSight™ Threat Management System, Symantec Co., URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=158&EID=0, 2005.

[DShield05] DShield.org, URL: http://www.dshield.org/, 2005.

[DW01] Herv´e Debar, and Andreas Wespi, "Aggregation and Correlation of Intrusion Detection Alerts", 2001.

[European04] The European CSIRT Networkt, URL: http://www.ecsirt.net/, 2004.

[HT+05] Wen-Yi Hsin, Shian-Shyong Tseng, Shun-Chieh Lin,"A Study of Alert-Based Collaborative Defense", International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN), 2005

[HS03] Arne Helme, Stelvio, "eCSIRT.net Deliverable1 Common Language Specication & Guideline to Application of the Common Language part (i)", December 2003.

[Masurkar03-1] Vijay Masurkar, "Responding to a Customer's Security Incidents—Part 1: Establishing Teams and a Policy", 2003.

[Masurkar03-2] Vijay Masurkar, "Responding to a Customer's Security Incidents—Part 2: Executing a Policy", 2003.

[MM+03] Benjamin Morin, Ludovic M´e, Herv´e Debar1, and Mireille Ducass´e, "M2D2: A Formal Data Model for IDS Alert Correlation", 2003.

[NJ+01] Peng Ning, Sushil Jajodia, Xiaoyang Sean Wang, "Abstraction-based Intrusion Detection in Distributed Environments", 2001.

[PN97] Phillip A. Porras and Peter G. Neumann, "EMERALD: event monitoring enabling responses to anomalous live disturbances", In 1997 National Information Systems Security Conference, Oct 1997.

[SB+91] S. Snapp, J. Brentano, and G. Dias et al., "DIDS (Distributed Intrusion Detection System) – motivation, architecture, and an early prototype", In Proceedings of the 14th National Computer Security Conference, October 1991.

[SC+96] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle, "GrIDS-a graph based intrusion detection system for large networks", In Proceedings of the 19th National Information Systems Security Conference, September 1996.

[Snort05] Snort® Intrusion Detection/Prevention System, URL: http://www.snort.org/, 2005"

[VK98] G. Vigna and R. A. Kemmereer, "NetSTAT: A Network-based Intrusion Detection Approach", 1998.

[WS+98] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, "Handbook for Computer Security Incident Response Teams (CSIRTs)", December 1998.