Chapter 10

TOWARDS AN INTELLIGENT SECURITY EVENT INFORMATION MANAGEMENT SYSTEM

Guillermo Suarez-Tangil, Esther Palomar, Arturo Ribagorda*
Department of Computer Science
Carlos III University of Madrid, Spain

Yan Zhang†
Simula Research Laboratory, Norway

Keywords: Artificial Immune System, Event Correlation, Security Event Information Management System, Intelligent Rule Generation, Adaptive System.

Abstract

The strategy of combining artificial intelligence (AI) and self–adaptation to optimize different types of computing services is emerging as an automated and efficient approach in computer security. Such a strategy can effectively be used to assist security experts in the protection of organizations. In particular, event correlation poses a promising challenge in providing intuition and cognition to Security Information and Event Management (SIEMs) systems. In this chapter, we enhance the traditional SIEM process as a whole, especially focusing on event correlation, by applying a bio–inspired and adaptive learning system based on Artificial Immune System (AIS). Among the advantages reached, our proposal facilitates an automatic correlation of novel, multi–step attacks.

*E-mail address: guillermo.suarez.tangil@uc3m.es, {epalomar, arturo}@inf.uc3m.es
†yanzhang@simula.no

1. Introduction

Security information management is an intriguing dynamic activity that involves different disciplines aimed at proactively protecting, preventing, and swiftly responding to security attacks. The continuous evolution of attacks, specially recent distributed multi–step attacks, complicate, even more if possible, this complex task and pose additional challenges to experts and to the entire detection process [Liu et al., 2008]. On one hand, different sources (known as sensors, namely intrusion detection systems (IDSs), firewalls, server logs, to name a few) produce an incessant barrage of security data, generally heterogeneous and difficult to understand. Hence, cooperation among sensors becomes essential. On the other hand, sensors usually work independently of each other and, in general, they are inspected separately, making it difficult the extraction of relevant information of such multi-step attacks.

Security Information and Event Management (SIEM) systems then appear as a holistic solution to gather, organize and correlate security information with the clear objective of reducing the amount of time spent by security administrators and therefore improving the incident response [Aguirre and Alonso, 2012]. However, since current SIEM systems are highly dependent on the configuration of multiple heterogeneous log resources deployed over the network, a common data model to unambiguously and consistently describe the relevant security information is required. For instance, several attempts, from both academia and industry, were made so far to compile and relate the concepts of alerts, events, attacks, sensors, vulnerabilities, software, devices, etc. Hence, there is a pressing need to formalize either a standard method or a formal ground to unequivocally represent knowledge on attacks [Cheung et al., 2003]. Recent work from `The MITRE Corporation` [Mitre, 2011b] has addressed the necessity of an ontology architecture describing the automatic and semantic interoperability within the SIEM lifecycle [Parmelee, 2010]. In particular, a novel specification has been proposed namely Common Event Expression (CEE) to semi-automate the SIEM process.

On the contrary, several proposals presented so far aim at optimizing the correlation module by the incorporation of some form of advanced logic [Almgren et al., 2008]. Basically, the correlation engine infers extra information from alerts finding out connections between them [Wang et al., 2010]. Principal objectives range from reducing the large number of alerts reported to identify multi–step attack scenarios, and also to identify new attack signatures. Current SIEM systems lack of an efficient mechanism to generate correlation rules and cannot adaptively predict novel attacks either [Anuar et al., 2010]. An efficient correlation should fulfil real–time attack detection through the identification of threat pattern sequences, most in the way of a series of alerts. However, most event correlation solutions currently available still require administrators to a non–negligible configuration effort. The optimization of event correlation becomes therefore essential to realize self-managing SIEM systems.

The main **contributions** of this chapter are:

- A review of the SIEM approaches which have focused on incorporating any form of AI or self-adaptation is outlined.
- New specifications to the Mitre's ontology architecture —Common Event

Expressing— are included for systematically correlate events.

- An enhancement of the traditional correlation process is introduced by using a bio-inspired machine learning technique, namely Artificial Immune System (AIS).

1.1. Overview of our Proposal

Relative to the existing literature on improving SIEM systems by applying AI, our contribution elaborates on the application of AISs to alert correlation. Though it is not the first time this technique is considered in intrusion detection, our approach is novel regarding the way event correlation is formulated. An AIS extracts and applies several interesting properties and concepts of the human immune system to provide solutions to different types of computer processes such as networks' defenses against malicious actions. In fact, phenomena produced within the biological adaptive immune system as a result of protecting the body against the encountered pathogens, can be metaphorically exploited to optimize the attack pattern recognition process.

IDSs along with Intrusion Prevention Systems (IPS) represent traditional strategies which are currently insufficient to protect networks and computers. We introduce a new crosswise component into the SIEM architecture called *Intrusion Learning System* (ILS) as depicted in Figure 1. The main goal of the ILS layer is to bring together intelligent strategies to automatically and dynamically generate correlation rules. ILS is based on widely used AIS–concepts such as the innate immunological memory. The three systems together, namely IDS, IPS and ILS, will define the event correlation framework located at the Intranet which is isolated from the Internet by a perimetric defense, as the skin does in the human body.

Sensors are deployed within the Intranet. Hence, incoming traffic, like a pathogen, has to first trespass that physical barrier which prevents undesired agents to penetrate into the perimeter. Once inside the perimeter, both the IDS and IPS compile traditional strategies to protect network computer systems. Undesired traffic is then redirected to the ILS.

Thus, we position the following statements:

- Generally, the existing SIEM tools present limitations and contextual constraints. In addition, current SIEM frameworks deploy their own architectures. We propose a global framework which integrates the most promising research advances and formalizes an unified architecture design towards an intelligent correlation system.

- Intruder's actions swiftly evolve to become more effective, as well as more sophisticated generations of malware, i.e. polymorphic multi-step malware. In this regard, malware–analysis tools along with a bio-inspired machine learning will integrate our architecture to automatically generate specific correlation fingerprints. We believe that, by providing adaptive intelligence to the correlation engine, time spent in detecting zero-day attacks can be significantly reduced.

- Additionally, we will use advanced sandboxing techniques [Rossow et al., 2011] to automatically extract immunological knowledge by means of dynamic experiments.

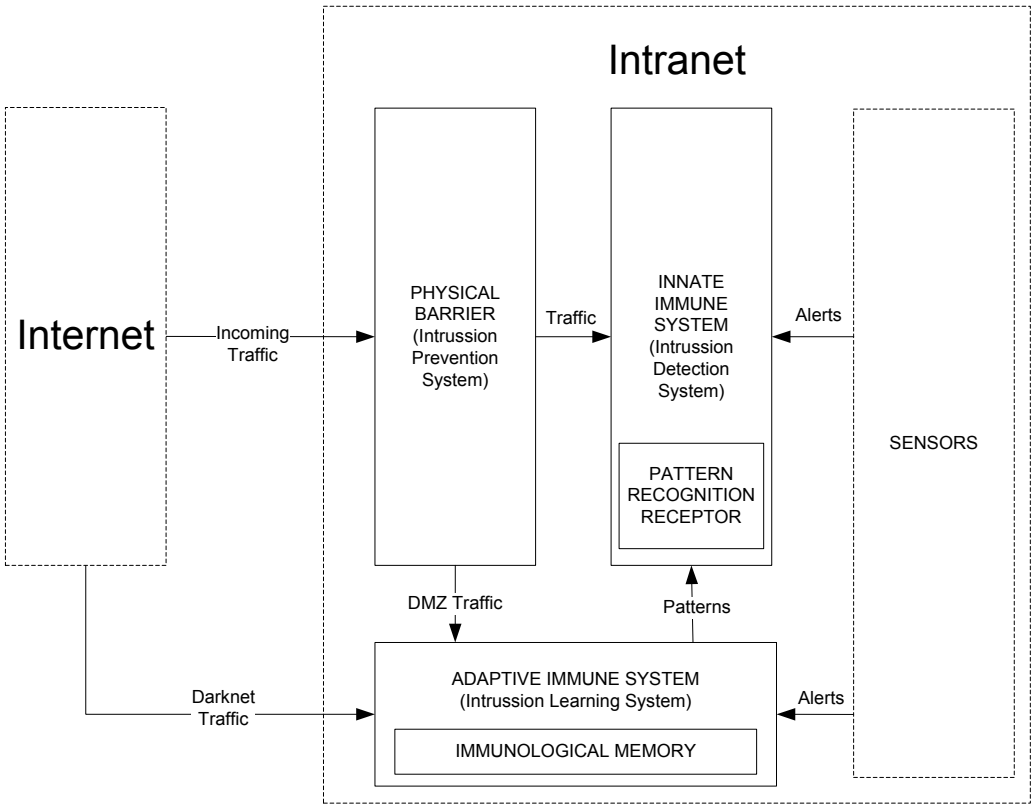

Figure 1. An event correlation framework based on AIS.

1.2. Chapter's Organization

The rest of the chapter is organized as follows. Some preliminaries and foundations of our work are described in Section 2 Next, we present our AIS-based correlation framework in Section 3 In addition, we discuss about the implementation guidelines in Section 4 Finally, we establish the main conclusions as well as the immediate future work in Section 5

2. Background and Preliminaries

This section gives some background and fundamentals to understand the application of AISs in SIEM systems.

2.1. AI-based Approaches to Optimize SIEM Frameworks

Several SIEM software products have been recently developed to provide essential intelligence to layered security frameworks, e.g. ArcSight [ESM, 2011], RSA enVision [RSA, 2011], Sensage [SenSage, 2011], Novell IBM [Sentinel, 2011], netForensics [netForensics, 2011], Bitacora [Bitacora, 2011], and OSSIM [AlienVault, 2011], to name a few. Each of the above software products establishes its own architecture and deployment

options. We refer the interested reader to [Nicolett and Kavanagh, 2011] for a comprehensive evaluation of current SIEM products.

SIEM frameworks in most cases gather a number of widely–use security and analytical tools to provide automated compliance and real–time threat management. In the literature, such tools have been classified into the following processes, according to their functionality: (i) normalization, (ii) aggregation, and (iii) correlation. Recently frameworks are also incorporating three techniques more, namely (iv) false alarm reduction, (v) attack strategy analysis, and (vi) priorization [Sadoddin and Ghorbani, 2006].

Now, the provision of intelligence and automation to the aforementioned tasks is attracting recent research interest. On the one hand, several works focused on normalization and aggregation have been widely discussed aimed at reaching standards for a common event expression [Mitre, 2011b]. On the other hand, solutions to find out unknown connections between alerts, or to identify the false alerts from those reported, or even to infer potential strategies of attacks do still persist as open issues [Sheyner et al., 2002].

Neural Networks (NN), widely used for optimizing classification problems [Ripley, 1994, Golovko and Kochurko, 2005], have been also applied to partially optimize IDSs, in particular to improve misuse filtering and malicious pattern recognition [Lippmann and Cunningham, 2000, Lei and Ghorbani, 2004, Zhang et al., 2005]. In [Ahmad et al., 2009], readers may find detailed survey on NN–based IDS. Moreover, Evolutionary Computation (EC) is especially suitable for those problems in which a cost–effort trade–off exists such as event correlation [Suarez-Tangil et al., 2009].

By inspiration also in nature, the application of AISs [Farmer et al., 1986] is emerging as a very promising and advantageous solution to optimize and further reason out especially within the domain of computer security. In particular, AISs have been applied to different other domains such as software fault prediction [Catal and Diri, 2009], and musical genre classification [Doraisamy and Golzari, 2010]. An interesting approach for mapping the human immunity entities and process on to the development of computational models is presented in [Dasgupta, 2006]. Furthermore, several works focus on analyzing how immunological concepts may be applied to intrusion detection [Kim et al., 2007], pattern recognition and classification [Carter, 2000], anomaly detection, and distributed detection [Hofmeyr, 1999]. Authors in [Twycross and Aickelin, 2010] introduce a summary of some biological information fusion by means of AIS implementation. More specifically, the work focuses on multi–sensor data fusion for parallel and distributed systems. The objective of this proposal focuses on producing efficient connections between the observed data and thus inferring an optimized decision. In fact, Twycross et al. demonstrate the convenience of applying AIS–based techniques for these purposes. Similarly, the use of Denditric Cell Algorithm (DCA) for information fusion in the context of anomaly detection [Greensmith et al., 2010] becomes a promising solution to the detection of complex attacks as described in the subsection below.

Hence, a supervised learning is possible by using AISs [Watkins et al., 2004], research directions could be headed towards the application of unsupervised learning indeed [De Castro and Timmis, 2002, Timmis and Neal, 2001].

2.2. On the Utility of Information Fusion Techniques over the Extraction of Relevancy of Events

Works on information fusion have been mainly focused on the enhancement of the analysis task and even on the employment of automatic procedures for real time analysis [Corona et al., 2009]. In particular, the information fusion techniques proposed so far in computer security have been mainly motivated by the fact that the information needed to perform such an analysis is mostly distributed within a multisensor environment. Moreover, these sensing units are typically located at different places, and the information they process is not homogeneous and is represented at different abstraction levels. In fact, information fusion has proven to provide with a very useful support for combining observations coming from different sources, as described in the following.

Current applications of information fusion to computer security range from providing automated classification of events and detection systems to effectively correlating different events which jointly constitute a multi-step attack happening within the monitored environment. For instance, the approach presented in [Giacinto et al., 2003] applies artificial NNs to test specific fusion rules. Each ANN is devoted to classify a different feature set related to the packet under test.

An information fusion framework for intrusion detection is proposed in [Bass, 2000] which prefigures the following levels: Data refinement, Object refinement, Situation refinement, Threat assessment, Resource management, and Knowledge. This conceptual framework serves as a guideline to other models.

Other fusion methods for intrusion classification rely on probability theory such as the DempsterShafer theory and Bayesian probability theory [Siaterlis and Maglaris, 2004].

Currently, information fusion research in computer security points out open issues regarding security data representation, i.e., the context of events, specially when taking a decision about the presence of an intrusion. A context-based representation of events is specially useful for further processing, and the definition of similarity metrics. The overview proposed in [Corona et al., 2009] states that data should be organized considering its context and proposes an uniform way to describe the context of data in terms of: (i) Where data is acquired (ii) When data is acquired, (iii) Which services are available and which data are they related to, (iv) Number of persons who will be able to access each service, (v) Which is the criticality of services, and (vi) Which is the sender and the receiver of each communication. Therefore, data representation should be driven by the knowledge of the relevant features. This sets the basis of other approaches based on predefined attack scenarios which usually apply a common language for formally defining such event patterns like a standardized format such as IDMEF. For example, a fusion model to correlate alerts is proposed in [Feng et al., 2007], which comprises the following stages: source preprocessing, alert data normalization, spacial alert fusion, and temporal alert fusion.

In summary, information fusion is emerging as a practical tool for obtaining more relevant, efficient and qualitatively better information out of the extremely large amount of data produced within a multisensor networking environment.

Table 1. (a) Application domain concepts, and (b) extension of CEE [Mitre, 2011b] event taxonomy domain for systematically correlate events.

	Domain	Concept
(a)	Sensor	Defined as a monitoring device which is focused on detecting events produced under a specific context.
	Event	Event is defined as a phenomenon produced when a particular security pre–condition becomes true. Generally such conditions denote established patterns extracted from previous interactions between two or more networking nodes.
	Event Record	The event's record consists of a set of attributes, which identifies a certain event's properties. CEE terminology refers to this domain as a collection of event fields namely event record. The specification of these attributes depends on the SIEM system.
	Event Category	Group of similar events that represents a possible way of grouping related events (*CEE Tag*). Each categorization is called *Tag Type* and is defined by a categorization methodology.
(b)	Event Aggregation	Event aggregation gathers together a collection of events which fulfill particular premises.
	Event Correlation	Event correlation must probabilistically define the relationship between a set of aggregated events.
	Correlation Record	The correlation's record consists of a set of attributes, which identifies a certain correlation's properties.
	Correlation Category	Represents a correlation produced as a response of the successful relationship between a set of attributes (namely *Correlation Tag*).

2.3. Common Correlation Expression. Our Approach

CEE [Mitre, 2011b] standardizes a common language and syntax for security information and events —it defines an event taxonomy for systematically categorizing events. Basically, *event categories* are established to form groups of events based on the categorizations of the events. Common event categories are listed as *CEE Tags* whereas the related events are grouped by *Tag Types*. CEE Dictionary and Event Taxonomy (CDET) helps to identify similar events through an event categorization methodology. CDET defines a collection of *CEE Tags*, which represents common event categories. Each *Tag Type* represents one possible way of grouping related events as part of the event categorization methodology. However, such methodology is conceived to identify only similar events and lacks on components regarding event correlation concepts. In this section, we propose an extension of the CEE taxonomy to include correlation specifications for categorization. Table 1–(a) depicts the most important concepts within our application domain.

A complete taxonomy should incorporate additional specifications to describe events related to complex multi–step attacks. Thus, we propose new terms to incorporate event correlation specification into the CDET categorization's methodology as defined in Table 1–(b).

Events are aggregated into the same correlation record when they hold the same values for a subset of attributes. A possible correlation record could comprise events with the same values for IP_{src}, IP_{dst}, Port_{dst}, Sensor_{id}, and Sensor_{sid}. Thus, a correlation record can be characterized by its categorization attributes or fields.

We then define the characteristics of a multi–step attack as the relationship between different correlation records. We have identified the following metrics to identify such

dependencies:

- *Number of events* for each pair of Sensor$_{id}$, and Sensor$_{sid}$.
- Number of different *correlation categories* per tuple of Sensor$_{id}$, and Sensor$_{sid}$.
- Number of *occurrences* a categorization.
- Total number of different *sources and destinations IP* addresses.
- Total number of *events* and *categories*.
- Maximum and minimum slot of *time* in between events.

Additionally, we have identified several *Correlation Tags* that can be used to systematically categorize correlations between events according to the way events are aggregated. Aggregation of events can be categorized into the following tags: (i) based on the topology described by the interaction between a number C of computers, (ii) based on the nature of the attack, and (iii) on the order of the aggregation, as follows:

I Topological classification: A tuple T of events can describe the aggregation of t events in a $N : M$ topology where N is the number of different sources and M different receivers. According to the topology we can identify the following three kinds of attacks: (i) Unidirectional, (ii) Bidirectional, and (iii) Multi–directional. First, unidirectional attacks are those in which there are only one source and one destination (1:1). Additionally, there are two other interactions that can be categorized in this group, i.e., one source and multiple destinations (1:M), or multiple sources and one destination (N:1) on each tuple. Next, bidirectional attacks are those in which there are two sources (2:2). And multi–directional attacks are those in which there are multiple sources and destinations (N:M).

II Natural classification: According to its nature, an attack is defined to be: (i) insider, or (ii) outsider attack. Insider attacks are launched by any malicious machine which belongs to the network domain being monitored. Hence, passive countermeasures such as blocking connections can be adopted.On the contrary, countermeasures against outsider attacks require an active intervention.

III Ordinal classification: Relative to the importance of the order, an aggregated event can be classified into (i) non-relevant, or (ii) relevant.

For the sake of illustration, consider a correlation extracted from a sandbox in which a `Solaris` server was infected with the `Conficker` worm. Assume that the sandbox has reported several events comprising the following correlation categorization: *insider*, *multi–directional* in $1 : M$ and *non-relevant*. First, we know that the infected machine is located inside the Intranet, and therefore it is compromising other computers within the network. Second, since events generated by `Confiker` are stochastic, the order in which they were reported is not relevant for the correlation. On the other hand, an instantiation of the `Bredavi` Trojan within the same sandbox gives us a *bidirectional* topology, i.e. the

attacker tends to contact the compromised system through a *backdoor* (one–direction) and, subsequently, the compromised system sends a reply back (bi–direction). In this case, the order of the events is tagged as *relevant* and the attack is originated by an outsider.

Important Remarks. Classifying multi–step correlations can help security operators to determine the nature of an attack and its impact. Regarding current and also future impact, the malware is actually evolving and so does the wide-spread adoption of automated malware generators. These malware generators facilitate the creation of new pieces of malware by reusing modules of other specimens. Additionally, other utilities and toolkits are used to generate different variants of the same piece of malware with slightly-different packing options or even exhibiting different behavior —both static and dynamic analysis strategies are then obfuscated and therefore concealed. Thus, it is part of our proposal to automate the identification of new encountered malware behavior according to the expected evolution of its ancestors.

2.4. A Methodology for applying AIS to SIEM

Our goal is to build a complex adaptive system into a SIEM system, which already involves diverse and multiple interconnected elements. In particular, our proposed AIS-based correlation mechanism tends to provide the SIEM system for the capability to change and learn from experience. In this section we further elaborate on the essential concepts which lead to an AIS–based implementation in this domain, as introduced in a previous work [Suarez-Tangil et al., 2011], namely:

1. **Application domain**. We must first define the main assumptions and definitions within this particular application domain and the correlation problem to be solved.

   To this regard, event correlation can be perceived from two different viewpoints, according to its application domain: (i) that automatically learns without human supervision, and (ii) that requires an expert supervision. In our context, the correlation rules which were automatically extracted are then treated as *temporary* rules, until a consolidation process is carried out. On the other hand, expert supervision will guide the process to extract attack-related knowledge and form *permanent* correlation rules.

2. **Immunity–based approach**. As we will describe below, there are different techniques presented so far. To identify the most suitable AIS technique is not trivial in all instances.

   As we mentioned before, several works in the literature address optimization problems by using immunity–based approaches such as *dendric cell algorithm*, *gene libraries*, and *idiotypic networks* [Kim et al., 2007]. Most of the proposals are based on *immune network models* [Jerne, 1974][1], *clonal selection with mutation* [Kim and Bentley, 2001b], and *negative selection* [Kim and Bentley, 2001a]. Basically, immune network models are based on idiotypic networks, and tend to define models in which immune entities, also known as *B cells*

[1]The immune network theory was first introduced by Jerne [Jerne, 1974] as a way to explain the memory and learning capabilities exhibited by the immune system. This theory has inspired a subfield of optimization algorithms as many other fields unrelated to biological immunology.

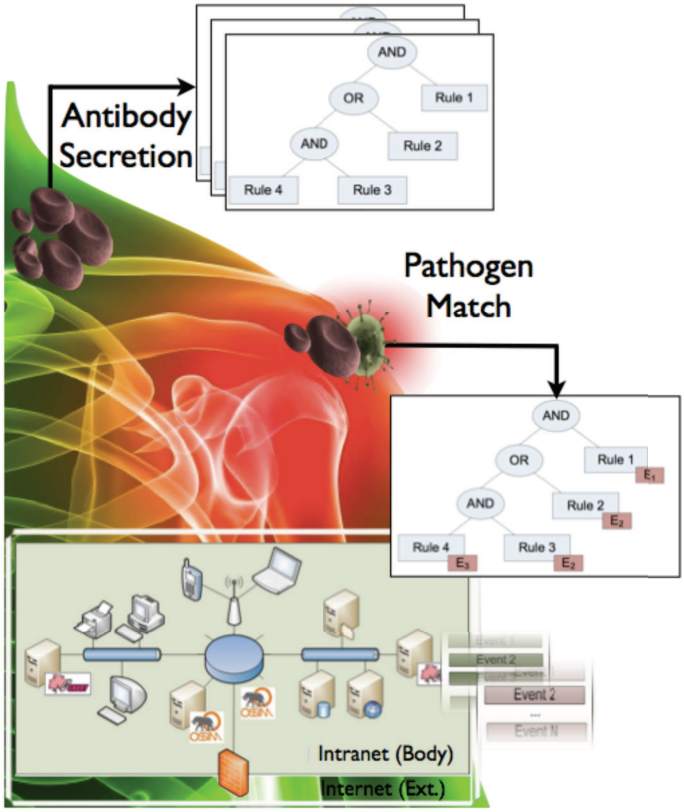

Figure 2. A mapping between the entities of the human immune system and those in our event correlation model.

[De Castro and Timmis, 2002], are interconnected in accordance with an affinity threshold. On one hand, clonal selection defines the strategy to mitigate an infection, i.e. by cloning the most successful antibodies. In particular, the maturation process introduces random variations over the antibodies cloned and thus increasing the probability to detect unknown behaviors. On the other hand, negative selection is used after the maturation phase, aiming at identifying non–self cells from self–cells, and also at deleting self–reacting cells. This algorithm is used for pattern recognition problems to obtain new patterns from available knowledge.

3. **Representation**. We must establish an interpreted codification for the immune entities and the elements involved in the correlation context.

   A representation for an event correlation model in terms of its similarities with the human immune system was previously discussed in [Suarez-Tangil et al., 2011]. In that work, a mapping between the entities of the human immune and those in the correlation model was proposed (see Figure 2 for details). In particular, artificial immune theory defines the concept of secreting proteins (correlation categorizations) as the mechanism used to detect non–self pathogens —malicious activity in the form

of events— which in turn are destroyed by antibodies (represented as rule patterns). Proteins constitute the parameters to monitor (as described in Section 2.3) and then allow us to distinguish between self and non–self behaviors.

4. **Adaptive immune algorithm**. Finally, we define the immune algorithm to automatically generate correlation categorizations. We propose an immune algorithm based on the most popular immunological approaches, as described in Section 3 This algorithm elaborates on a novel adaptive component for the proposed ILS module.

3. A Novel Architecture for an Artificial Immunity-based SIEM System

In this section, we introduce a novel approach to extend and enhance traditional SIEM systems based on artificial immune network theory. Our three-layer architecture comprises the following building blocks (separated with solid lines in Fig. 3):

- The physical barrier offers protection against pathogens attacking the system from outside, like some sort of prevention layer.
- The Innate Immune System (present in humans at birth) deploys immune agents which are in charge of protecting the system against invaders as well as providing pattern recognition mechanisms.
- The Adaptive Immune System (included in the ILS) defines the logic of the biological functions and components to learn, adapt and memorize antigens and also to secrete the appropriate anti–body (i.e. which are represented by the correlation rules in our domain).

3.1. The Physical Barrier and the Innate Immune System

Both together, the physical barrier and the innate immune system, already have their equivalences in current SIEM systems.

The physical barrier, placed "in-line", represents a first layer of protection and compiles a number of devices, either hardware or software such as firewalls, VPNs, and IPSs, aimed at protecting the intranet from malicious activity. For instance, unauthorized incoming traffic is not only blocked, but also logged and reported to the SIEM. In other words, these devices prevent pathogens e.g. bacteria and viruses from entering the organism, i.e. the intranet.

A second layer of protection consists then in the innate immune system. The Intranet deploys this layer by monitoring and detecting the encountered malicious activity. To this regard, IDSs are strategically located within intranet (most in the way of network IDS — NIDS, switches and routers) and also on simple hosts or servers (HIDS). These devices must "know" as many attack signatures or patterns as possible. Alerts (the innate responses) from these devices are usually triggered when any monitored packet matches a signature (or an immune pattern).

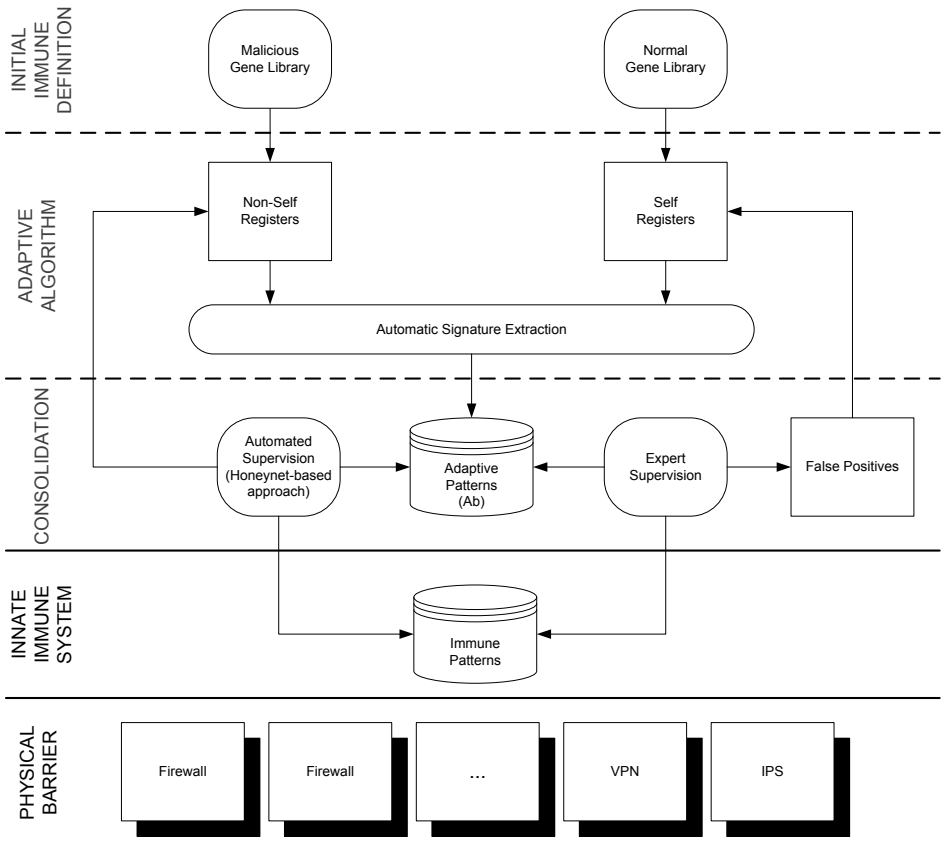

Figure 3. A three–layer architecture which combines traditional IDS concepts, data mining, honeynets and, just when strictly needed, the security expert supervision.

3.2. The Adaptive Immune System

In our domain, the adaptive immune system is equivalent to the new SIEM component called ILS. Its responsibility ranges from introducing intuition and cognition into the SIEM to allow immunological memory. In particular, ILS will provide (i) more efficient correlation rules, (ii) adaptive immunological memory, and (iii) more effective incident response.

We envision ILS as a three–phase protocol (separated with dashed lines in Fig. 3) which combines traditional IDS concepts, data mining, honeynets and the expert supervision (if strictly needed), as follows:

I **Initial innate immune definition**. In this phase, the expert must define a range of values for the collection of correlation categorizations.

II **Adaptive algorithm**. The adaptive algorithm produces a number of correlation categorizations that will be used to learn new correlation rules.

III **Adaptive immunological memory consolidation**. New correlation categorizations are consolidated in this phase.

Sections below further elaborate on these three ILS phases.

3.2.1. Initial Innate Immune Definition

As a SIEM system includes a series of tools and methods to defend an organization from intrusions, so the biological innate immune system receives at birth. In our domain, it is expected that sensors recognize and respond the unauthorized packets at least in a generic way. Thus, a series of correlation categorizations must be defined during the initial phase.

Initial values will act as generic discriminators for both self cells and non-self cells. Now, we must decide how to implement the appropriate value for each correlation categorization. To this regard, existing repositories collect known attacks and their associated correlation rules. Generally, these repositories are also known as *Gene Libraries*, and they are essential for the process below.

Therefore, we define two libraries, namely malicious and normal behavior. The former consists of misuse patterns whereas the latter contains the anomaly–detection data. On one hand, misuse patterns can be extracted from well–known attack rule definition sets, such as Vulnerability Research Team (VRT), Snort rules [Team, 2011] specially suitable for defining network anomaly rules, antivirus signatures [Le Pennec et al., 2005] when looking for host anomaly detection rules, and/or repositories of high-level languages which describe computer–specific attacks like STATL [Eckmann et al., 2002] or CAPEC [Mitre, 2011a]. A knowledge database can be easily extracted to conform with the libraries.

On the other hand, heuristics extracted from an anomaly–based detection can be also defined here [Lee and Stolfo, 2000, Davis and Clark, 2011]. For example, consider an OSSIM[1] in which misuse patterns are instantiated. Consider that we are using the notation defined in Section 2.3 We could define as a normal activity to log in to a workstation as long as the number of attempts does not exceed a certain threshold t, being $t \in$ *Num. of occurrences–per–categorization*. A categorization here could be established as the number of connections to a telnet, ftp, smtp, or http port. Hence, the appropriate OSSIM's sensor, e.g. OSSIM's *telnet option decoder*, will report an event every time a telnet connection is established. Different values for the threshold —for network probe, scan, flood, DoS, root to local (R2L) and user to root (U2R) rates,— have been extensively analyzed in the literature [Davis and Clark, 2011].

3.2.2. Adaptive Algorithm for an Automatic Signature Extraction

The main objective of the adaptive algorithm is to learn new correlation rules from observing the random adaptations of both normal and malicious gene libraries. Foundations of this algorithm rely on the AIS principles, as follows:

1. **Antibody secretion**. Antibodies are those patterns responsible of identifying a specific sequence of events (i.e. the antigen). Thus, an antibody represents the rule capable of recognizing a certain correlation pattern. In this stage, antibodies are generated by random combinations of the attributes stored in the `Malicious Gene Library` as well as by the mutations occurred to their values.

[1] OSSIM [AlienVault, 2011] is an open source SIEM implementation which centralizes the detecting and monitoring of the security events within an organization.

2. **Negative selection**. Negative selection eliminates inappropriate and immature antibodies. Basically, self-reacting rules are deleted from the set of adaptive candidates, and therefore ensuring that new antibodies will not detect self-cells by mistake. This algorithm applies the knowledge (Normal Gene Library) which was defined during the initial innate immune definition. Additionally, *Danger Theory* can be used here as an intriguing mechanism for reducing the number of false alerts, for example, by responding more aggressively against pathogens based on the correlation of danger signals [Aickelin and Greensmith, 2007].

3. **Pathogen matching**. Pathogens are harmful agents causing disease to their hosts. Pathogen matching is the process in which pathogens are identified by antibodies and is part of the intrusion detection process. Matching event correlation rules has been discussed in [Suarez-Tangil et al., 2009].

4. **Clonal selection**. Clonal selection based on affinity mutation aims at optimizing the pattern recognition algorithm by cloning the most interesting correlation rules and mutating its attributes afterwards.

Note that the above AIS–based techniques will produce a number of randomly generated correlation rules. However, most promising rules will be distinguished during the following consolidation process.

3.2.3. Adaptive Immunological Memory Consolidation

Correlation rules, obtained automatically, are now consolidated based on two different criteria: (1) by automatic techniques and, just when strictly needed, (2) by using the expertise of security administrators. Consolidation of a rule involves the process of evaluating the convenience of the generated correlations. In case of a rule is likely to detect a certain intrusion, then it will be exported to the immune system as part of the learning process. Otherwise, the rule will continue adapting its definition until consolidation is achieved.

On one hand, we define the automatic consolidation process as follows. Rules generated in the previous phase are automatically evaluated and a likelihood of matching a potential correlation is calculated. Likelihood of matching determines the probability of matching a collection of events as a result of an unknown attack. Only those rules with likelihood above a threshold will be consolidated. To this regard, rules are first deployed in a sandbox which has been exposed to numerous events launched from a network telescope or *darknet* (a number of unused network addresses). In addition, traffic incoming the darknet is, by definition, unrequested and therefore likely to be generated by an intruder. The more similarity between the rule with any of the events produced in the darknet, the more likelihood of the rule. However, if none of the immunological rules matches, then the immunological memory (associated to each correlation) will be decreased.

Furthermore, honeynets appear as the best candidate to assist the automated consolidation process. A honeynet is a group of networking nodes used to trap malware by simulating to be unprotected and vulnerable, so that attackers' activities can be studied. The key idea is to validate the generated categorizations using the non–self activity reported on the darknet as part of a honeynet.

```
Data: Normal and Malicious Categories
Result: Correlation Rules
// Expert and Automated self/non-self discrimination
GenLibrary ← InitialInnateImmuneDefinition;
while SIEM is learning do
    thread
        MemoryCells ← AutomatedSignatureExtraction(GenLibrary);
        ConsolidatedRules ← AutomatedConsolidation(MemoryCells, Pathogens);
    end
    thread
        // Honeypot--based Sandbox Pathogens ← PathogenGeneration;
        FeatureExtraction(Pathogens);
        Clustering(Pathogens);
    end
    thread
        ExpertSupervision(ConsolidatedRules);
    end
end
```

Algorithm 1: Threefold approach for based on two paradigms: (i) automated and (ii) expert supervision.

On the other hand, the expert can manually inspect and validate the correlation rules in terms of their accuracy. In any case, correlations that were not consolidated by the expert and/or failed during the automatic consolidation will be discarded.

4. Discussion

Our implementation efforts focus on integrating the proposed AIS-based framework into an open source SIEM such as OSSIM [AlienVault, 2011]. As mentioned before, implementation can be tackled according to the principles defined on Section , or based on the two criteria above: (i) with an automatic supervision or (ii) requiring the expert supervision, as described in Algorithm 1.

According to the former, the automatic signature extraction principle is based on randomly generating event correlation rules. Source of randomness is seeded not only using elements from the Gene Library [Kim et al., 2007] but also using attributes from the strongest consolidated antibodies. Affinity maturation based on the principles of mutation and selection can be applied here to reach the strongest antibodies.

Secondly, automatic supervision of event correlation rules can be driven by honeypot-based sandboxing. For instance work introduces in [Yegneswaran et al., 2005] presents a system, called Nemean, for automatic generation of intrusion signatures for NIDS from honeynet packet traces. Based on this approach, we define *detectors* as the randomly generated rules. Algorithm 2 describes detector's life cycle as an essential process for correlation rules consolidation. Basically, generated detectors are considered naive until rules are consolidated. If a pathogen matches with a detector, then the latter is incorporated into the immunological memory.

Finally, security experts may optionally supervise the learning process in order to reinforce the consolidation process.

```
Data: Pathogens, Affinity Mutation, Normal and Malicious Gen Library
Result: Memory Cells
Detectors ← RandomGeneration(GenLibraries)
foreach NaiveDetector ← in Detectors do
    if match(NaiveDetector, Pathogen) then
        AddForConsolidation(NaiveDetector);
        AddForClonalSelection(NaiveDetector, AffinityMutation);
    else
        Dies(NaiveDetector);
    end
end
```

Algorithm 2: Automatic signature extraction for event correlation rules.

5. Conclusions

SIEM technology, focused on developing effective methods and tools to assist network administrators during the whole network security management, is still evolving rapidly. Both, lack of standards and adaptability, hinder even more the analysis of the huge amount of security information collected every day. Similarly, novel multi-step malware is one of the major threats in the Internet today. Several techniques for an automated analysis of malware have been proposed so far. Sandboxing is, in this regard, a powerful tool to accomplish dynamic analysis. However, this and other techniques fail on dynamically establishing cross correlation relationships among traces recorded on multiple affected devices.

In this chapter, we introduce a novel SIEM architecture based on a bio-inspired technique, namely AIS, to adaptively learn new correlation rules and reactively face multi–step attacks. Our SIEM system is designed to learn even from unknown malware. Our proposal comprises various strategies already used in intrusion detection, data mining, honeynets analysis and, when strictly needed, the expert supervision. Our hope is that this new framework will, directly or indirectly, inspire new directions on applying intelligence to security event correlation.

References

[Aguirre and Alonso, 2012] Aguirre, I. and Alonso, S. (2012). Improving the automation of security information management: A collaborative approach. *IEEE Security Privacy*, 10(1):55–59.

[Ahmad et al., 2009] Ahmad, I., Abdullah, A. B., and Alghamdi, A. S. (2009). Artificial neural network approaches to intrusion detection: a review. In *Proceedings of the 8th Wseas international conference on telecommunications and informatics*, pages 200–205. WSEAS.

[Aickelin and Greensmith, 2007] Aickelin, U. and Greensmith, J. (2007). Sensing danger: Innate immunology for intrusion detection. *Information Security Technical Report*, 12(4):218–227.

[AlienVault, 2011] AlienVault (Visited November 2011). Open source security information management (ossim). `http://www.ossim.net`.

[Almgren et al., 2008] Almgren, M., Lindqvist, U., and Jonsson, E. (2008). A multi-sensor model to improve automated attack detection. In *Recent Advances in Intrusion Detection*, volume 5230, pages 291–310. Springer Berlin / Heidelberg.

[Anuar et al., 2010] Anuar, N., Papadaki, M., Furnell, S., and Clarke, N. (2010). An investigation and survey of response options for Intrusion Response Systems (IRSs). In *Information Security for South Africa (ISSA), 2010*, pages 1–8. IEEE.

[Bass, 2000] Bass, T. (2000). Intrusion detection systems and multisensor data fusion. *Commun. ACM*, 43:99–105.

[Bitacora, 2011] Bitacora (Visited November 2011). System of centralization, management and exploitation of a company's events. `http://bitacora.s21sec.com/`.

[Carter, 2000] Carter, J. H. (2000). The immune system as a model for pattern recognition and classification. *Journal of the American Medical Informatics Association: JAMIA*, 7(1):28–41.

[Catal and Diri, 2009] Catal, C. and Diri, B. (2009). Investigating the effect of dataset size, metrics sets, and feature selection techniques on software fault prediction problem. *Information Sciences*, 179(8):1040–1058.

[Cheung et al., 2003] Cheung, S., Lindqvist, U., and Fong, M. (2003). Modeling multistep cyber attacks for scenario recognition. In *Procs. of the DARPA Information Survivability Conference and Exposition*, volume 1, pages 284–292.

[Corona et al., 2009] Corona, I., Giacinto, G., Mazzariello, C., Roli, F., and Sansone, C. (2009). Information fusion for computer security: State of the art and open issues. *Inf. Fusion*, 10:274–284.

[Dasgupta, 2006] Dasgupta, D. (2006). Advances in artificial immune systems. *IEEE Comp. Intelligent Magazine*, 1(4):40–49.

[Davis and Clark, 2011] Davis, J. J. and Clark, A. J. (2011). Data preprocessing for anomaly based network intrusion detection: A review. *Computers & Security*, 30(6-7):353–375.

[De Castro and Timmis, 2002] De Castro, L. and Timmis, J. (2002). *Artificial immune systems: a new computational intelligence approach*. Springer Verlag.

[Doraisamy and Golzari, 2010] Doraisamy, S. and Golzari, S. (2010). Automatic Musical Genre Classification and Artificial Immune Recognition System. *Advances in Music Information Retrieval*, page 391.

[Eckmann et al., 2002] Eckmann, S., Vigna, G., and Kemmerer, R. (2002). Statl: An attack language for state-based intrusion detection. *Journal of Computer Security*, 10(1/2):71–104.

[ESM, 2011] ESM, A. (Visited November 2011). Enterprise security manager. `http://www.arcsight.com/products/products-esm/`.

[Farmer et al., 1986] Farmer, J. D., Packard, N. H., and Perelson, A. S. (1986). The immune system, adaptation, and machine learning. *Physica D: Nonlinear Phenomena*, 22(1-3):187–204.

[Feng et al., 2007] Feng, C., Peng, J., Qiao, H., and Rozenblit, J. W. (2007). Alert fusion for a computer host based intrusion detection system. In *Procs. of the 14th Annual IEEE Int. Conf. and Workshops on the Engineering of Computer-Based Systems*, pages 433–440. IEEE Computer Society.

[Giacinto et al., 2003] Giacinto, G., Roli, F., and Didaci, L. (2003). Fusion of multiple classifiers for intrusion detection in computer networks. *Pattern Recogn. Lett.*, 24:1795–1803.

[Golovko and Kochurko, 2005] Golovko, V. and Kochurko, P. (2005). Intrusion recognition using neural networks. In *IEEE Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, pages 108–111. IDAACS.

[Greensmith et al., 2010] Greensmith, J., Aickelin, U., and Tedesco, G. (2010). Information fusion for anomaly detection with the dendritic cell algorithm. *Information Fusion*, 11(1):21–34.

[Hofmeyr, 1999] Hofmeyr, S. (1999). *An immunological model of distributed detection and its application to computer security*. PhD thesis, University of New Mexico.

[Jerne, 1974] Jerne, N. K. (1974). Towards a network theory of the immune system. *Ann. Immunol.*, 125C:373–389.

[Kim and Bentley, 2001a] Kim, J. and Bentley, P. (2001a). An evaluation of negative selection in an artificial immune system for network intrusion detection. In *Proc. of GECCO*, pages 1330–1337. Citeseer.

[Kim and Bentley, 2001b] Kim, J. and Bentley, P. (2001b). Towards an artificial immune system for network intrusion detection: An investigation of clonal selection with a negative selection operator. In *Proc. of the 2001 Congress on Evolutionary Computation*, volume 2, pages 1244–1252. IEEE.

[Kim et al., 2007] Kim, J., Bentley, P., Aickelin, U., Greensmith, J., Tedesco, G., and Twycross, J. (2007). Immune system approaches to intrusion detection–a review. *Natural computing*, 6(4):413–466.

[Le Pennec et al., 2005] Le Pennec, J., Hericourt, O., et al. (2005). Method and system for retrieving an anti-virus signature from one or a plurality of virus-free certificate authorities. US Patent 6,976,271.

[Lee and Stolfo, 2000] Lee, W. and Stolfo, S. (2000). A framework for constructing features and models for intrusion detection systems. *ACM Transactions on Information and System*, 3(4):227–261.

[Lei and Ghorbani, 2004] Lei, J. Z. and Ghorbani, A. (2004). Network intrusion detection using an improved competitive learning neural network. In *Proc. of second annual conf. on communication networks and services research*, pages 190–197. IEEE Computer Society.

[Lippmann and Cunningham, 2000] Lippmann, R. P. and Cunningham, R. K. (2000). Improving intrusion detection performance using keyword selection and neural networks. *Computer Networks*, 34(4):597–603. Recent Advances in Intrusion Detection Systems.

[Liu et al., 2008] Liu, Z., Wang, C., and Chen, S. (2008). Correlating multi-step attack and constructing attack scenarios based on attack pattern modeling. In *Procs. of the ISA 2008 Int. Conf. on Information Security and Assurance*, pages 214–219.

[Mitre, 2011b] Mitre (2011b). Common event expression. Technical report, The MITRE Corporation. http://cee.mitre.org/docs/CEE_Profile_Specification-v0.6.pdf.

[Mitre, 2011a] Mitre (Visited November 2011a). Common attack pattern enumeration and classification. Technical report, The MITRE Corporation. http://capec.mitre.org/.

[netForensics, 2011] netForensics (Visited November 2011). nfx sim one. `http://www.netforensics.com/products/security\_information\_management/SIM\_One/`.

[Nicolett and Kavanagh, 2011] Nicolett, M. and Kavanagh, K. M. (2011). Magic quadrant for security information and event management. *Gartner RAS Core Research Note G*, 21245:1–31.

[Parmelee, 2010] Parmelee, M. C. (2010). Toward the semantic interoperability of the security information and event management lifecycle. In *Working Notes for the 2010 AAAI Workshop on Intelligent Security (SecArt)*, page 18. The MITRE Corporation.

[Ripley, 1994] Ripley, B. (1994). Neural networks and related methods for classification. *Journal of the Royal Statistical Society*, 56(3):409–456.

[Rossow et al., 2011] Rossow, C., Dietrich, C., Bos, H., and Cavallaro, L. (2011). Sandnet: Network traffic analysis of malicious software. In *Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security*, pages 76–86. ACM.

[RSA, 2011] RSA (Visited November 2011). envision. `http://www.rsa.com/node.aspx?id=3170`.

[Sadoddin and Ghorbani, 2006] Sadoddin, R. and Ghorbani, A. (2006). Alert correlation survey: framework and techniques. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust*, pages 1–10. ACM.

[SenSage, 2011] SenSage (Visited November 2011). Sensage siem solution. `http://www.sensage.com/`.

[Sentinel, 2011] Sentinel, N. (Visited November 2011). Sentinel. `http://www.novell.com/products/sentinel/`.

[Sheyner et al., 2002] Sheyner, O., Haines, J., Jha, S., Lippmann, R., and Wing, J. M. (2002). Automated generation and analysis of attack graphs. In *Procs. of the 2002 IEEE Symposium on Security and Privacy*, pages 273–. IEEE Computer Society.

[Siaterlis and Maglaris, 2004] Siaterlis, C. and Maglaris, B. (2004). Towards multisensor data fusion for dos detection. In *Procs. of the 2004 ACM symposium on Applied computing*, pages 439–446. ACM.

[Suarez-Tangil et al., 2009] Suarez-Tangil, G., Palomar, E., Fuentes, J. D., Blasco, J., and Ribagorda, A. (2009). Automatic rule generation based on genetic programming for event correlation. In *Computational Intelligence in Security for Information*, Advances in Soft Computing, pages 127–134, Burgos, Spain. Heidelberg, Springer Berlin.

[Suarez-Tangil et al., 2011] Suarez-Tangil, G., Palomar, E., Pastrana, S., and Ribagorda, A. (2011). Artificial immunity-based correlation system. In *Procs. of the Int. Conf. on Security and Cryptography (SECRYPT)*, page 99.

[Team, 2011] Team, V. R. (Visited November 2011). Vrt certified snort rules. `http://www.snort.org/snort-rules`.

[Timmis and Neal, 2001] Timmis, J. and Neal, M. (2001). A resource limited artificial immune system for data analysis. *Knowledge-Based Systems*, 14(3–4):121–130.

[Twycross and Aickelin, 2010] Twycross, J. and Aickelin, U. (2010). Information fusion in the immune system. *Information Fusion*, 11(1):35–44.

[Wang et al., 2010] Wang, L., Ghorbani, A., and Li, Y. (2010). Automatic multi-step attack pattern discovering. *International Journal of Network Security*, 10(2):142–152.

[Watkins et al., 2004] Watkins, A., Timmis, J., and Boggess, L. (2004). Artificial Immune Recognition System (AIRS): An Immune-Inspired Supervised Learning Algorithm. *Genetic Programming and Evolvable Machines*, 5(3):291–317.

[Yegneswaran et al., 2005] Yegneswaran, V., Giffin, J., Barford, P., and Jha, S. (2005). An architecture for generating semantics-aware signatures. In *Proceedings of the 14th conference on USENIX Security Symposium-Volume 14*, pages 7–7. USENIX Association.

[Zhang et al., 2005] Zhang, C., Jiang, J., and Kamel, M. (2005). Intrusion detection using hierarchical neural networks. *Pattern Recognition Letters*, 26(6):779–791.