Cyber Security System With SIEM And Honeypot In Higher Education

Jarot S. Suroso1, Caesario Putra Prastya2
Bina Nusantara University, Jakarta, Indonesia
jsembodo@binus.edu1, caesarioputraprastya@gmail.com2

Abstract—Communication science and information technology (ICT) has been progressing and contain complex implication for individual, groups and inter-country relationship. Along with ICT evolution, threats (including theft of information) increase and electronic systems are adopted. As a government agency in higher education with the country’s strategic data, XYZ cannot escape hackers trying to access the assets. Strategic assets include system and company’s data as well as systems and data which might be taken for granted by irresponsible parties. Therefore, it is necessary to secure information and data systems in XYZ. Moreover to test whether the implemented cyber security system can optimally standardize the company's information and data systems. The application of Security Information Event Management (SIEM) to cyber security systems to detect incoming threat alerts and block access to suspicious threats. While the honeypot is used to deceive the hacker into a fake system intentionally attacked and learning the tricks that intruders use when performing the action. The results of the test of the application of SIEM and Honeypot at XYZ can monitor the monitoring of information system and data-related threats in real-time, and deter and transmit cyber-attacks to adequately protect information security so that the use of cyber security systems with SIEM & Honeypot can secure the information and data systems owned by XYZ optimal.

Keywords— Information Technology, Threats, Cyber Security, SIEM, Honeypot, Realtime.

1. Introduction
The use of science and communication information technology (ICT) has progressed and has a complex impact on the lives of individuals, groups and inter-country relationships. With the advancement of ICT, it brings with it a new concept that connects all of them electronically to a zone called cyberspace, where cyberspace facilitates communication without the limitations of distance and time. Cyberspace is a zone created by electronic media that work with computer networks to communicate in one direction or both directions. Activities in cyberspace do not require direct physical relationships in traditional forms, but these activities are performed virtually. Cyberspace has formed a separate part of the world known as Maya World. The virtual world is today a necessity of human life, which is used for social media, commerce, health services, governance and the defense sector of a country.

The virtual world becomes part of the interface between the real world and the virtual world, with the side of the overlapping part having both positive and negative effects. In the virtual world, anyone can quickly change places while performing activities in different places at the same time, as well as being able to communicate and exchange information quickly in cyberspace, and many other activities that
are possible in the world virtually. Like the two opposing sides of a currency, cyberspace also has a negative side, namely the number of threat activities targeting individuals, particular groups, authorities, and threats to a country. These threats include attempts to steal information, adopt electronic systems, and take various other types of action that violate the law, commonly referred to as cybercrime.

Cybercrime is considered an exceptional crime in the international community because many countries are involved. Cybercrime has many forms of performing cyberattacks (cyber attacks) such as phishing, malware propagation, hacking passwords, hacking systems / applications, malformations, backdoor, distributed denial-of-service (DDoS). Cyber attack techniques continue to evolve as information technology evolves. Therefore, a cyber threat information security system is needed to monitor cyberattacks in real time. Figure 1.1 shows that cyber threats increase each year.

Similarly, it happened with XYZ, where many hackers are trying to access strategic assets. Strategic assets include systems and data that are related to the enterprise and where the system and data are very dangerous when accessed by irresponsible parties. The following data shows the large number of attacks leading to multiple strategic assets of XYZ, the attack can reach the target if it can not be prevented by the firewall, so that hackers can access the system or data of XYZ following the above statement, the cyber world needs special attention to avoid potential threats, especially those that affect information security. Even the most dangerous threats are linked to cybersecurity today. Cybersecurity is a non-military defence action for a country to develop a sense of defence in cybersecurity in the cybersecurity sector. Cybersecurity targets all groups, individuals, groups, organizations and governmental interests. Priority is the protection of strategic assets of defence and security that are directly related to the public. If it comes to a disruption of the system that disturbs the stability of the nation, this is the reference for building cybersecurity to protect against cyber threats.

Based on background observations, this research study was conducted to find solutions to the problem:

1. How to design the information security system using SIEM and Honeypot in XYZ?
2. Can the use of information security systems with SIEM and Honeypot effectively secure information and data systems?

This template, modified in MS Word 2007 and saved as a “Word 97-2003 Document” for the PC, provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

2. Literature Review

2.1 Information Security
The definition of information security has different opinions from several sources / experts. According to Sarno and Iffano, information security is an attempt to protect information assets from potential

![Figure 1. Indonesia threat 2015 & 2016](image-url)
threats. In the case of information security, the business can indirectly guarantee business continuity because information security can reduce the risks that occur in day-to-day business processes. In addition to information security, it can help optimize return on investment [1]. More and more corporate information is being stored, managed, and shared, the greater the risk of damaging, losing or disclosing data to unwanted external parties. [2] According to ISO / IEC 17799: 2005, an information security information security management system is an effort to protect against a variety of threats to ensure the sustainability of the business, minimize business risk, and increase investment in identifying opportunities. There are three key information security principles in maintaining information security from multiple sources of threat: confidentiality, availability, and integrity [2].

2.2 IDPS (Intrusion Detection Prevention System)

IDS Intrusion Detection System is a system that monitors network traffic and suspicious activity in a network system [5]. If suspicious activity related to network traffic is detected, IDS warns network administrators through the IDS console system. In some cases, IDS can also respond to anomalous traffic anomalies by blocking actions against users or Internet Protocol (IP) addresses attempting to access the network. IPS (Intrusion Prevention System) is a system that combines firewall functions with IDS features. This IPS technology can be used to prevent cyber threats leading to the local network by checking in and out each packet (input and output), and the packet is detected by the sensor if an identified attack threatens the local network denies access (blocking) and logs (logs) all data packets identified as threats. In this way, IPS acts like a firewall that allows and blocks network access and, like IDS, combines with full packet detection. IPS uses signatures as packet filtering rules to detect traffic activity on the network or terminal. The detection of incoming and outbound (inbound-outbound) threats can be prevented as early as possible before they gain access to and damage or receive access to local area networks through the use of IPS. Thus, early detection and prevention can be promoted by using IPS [3]. IDS and IPS are commonly known as IDPS (Intrusion Detection and Prevention Systems). IDPS focuses on identifying possible events. For example, IDPS can detect when an attacker successfully exploited the system by exploiting security holes in the system. The IDPS then reports the incident to the security administrator, who can immediately perform an incident response to minimize the damage caused by the incident. IDPS can also record information that can be used by event handlers [4]. There are two types of IDS and IPS, NIDS (Network-based IDS) and HIDS (Host-based IDS). IPS also has two types, NIPS (Network based IPS) and HIPS (Host based IPS). There is a fundamental difference between IDS and IPS. The difference is that IDS does not work in-line on the network when placed on the network, or it can be said that IDS only monitors the network by "connecting" or "tapping" the network to be protected. Unlike IDS, IPS is in-line in the network. To make things suspicious, IPS can close the access immediately.

Figure 2. Different placement of IDS and IPS

Link: [https://keamanan-informasi.stei.itb.ac.id/2013/10/30/menangani-serangan-intrusi-menggunakan-ids-dan-ips/](https://keamanan-informasi.stei.itb.ac.id/2013/10/30/menangani-serangan-intrusi-menggunakan-ids-dan-ips/)

1) **Network-based Intrusion Detection System (NIDS)**

NIDS is an intrusion detection system that collects data packets that travel on a network medium (wired, wireless) and matches the data packet with the signatures in the database. If the data
packet matches the intruder's signature, a warning is issued and the data packet is stored in a file or database.

2) **Host Intrusion Detection System (HIDS)**

Host-based Intrusion Detection systems or HIDS are placed as agents of a host. Intrusion detection systems such as these can examine system and application log files to detect intrusion activity. Some of these systems are reactive, which means that HIDS only notifies users when an attack has occurred. But there are also some who are proactive who can track network traffic from specific hosts installed with HIDS and perform peringantan in real time.

2.3 **SIEM (Security Information Event Management)**

Security Information and Event Management (SIEM) is a system that can analyze security events in real-time while providing long-term log storage, historical reporting, and trend analysis. They serve as event alerts and correlate vulnerability data and threat intelligence to provide insights into risk predictions (and to prioritize those risks) and audit and audit reports for compliance purposes, such as: the PCI provisions (Payment Card Industry) to perform. SIEM is able to provide information security capabilities as a holistic view of security risks through historical data collections from multiple sources such as firewalls, switches, load balancers, weblog servers, and proxy servers. This logarithmic correlation is intended to extract the meaning and intelligence of this mass data; remember when certain event conditions are met; and a dashboard that visualizes events that previously required management of multiple dashboards and reporting tools. The use of SIEM technology is determined by the need for information security. Investigating incoming attacks requires intensive resources, data access, and monitoring. SIEM is a combination of Information Management Security (SIM) and Security Event Management (SEM) [6]. While SEM or Security Event Management consolidates and stores multiple log sources and security events, SIM or Security Information Management provides an analysis and analysis of long-term trends from this log.

- **Security Information Management (SIM)** - log management and compliance reporting.
- **Security Event Management (SEM)** - Monitoring management and real-time events for security events from networks, security devices, systems, and applications.

SIEM technology is typically used for three primary use cases:

- Compliance - log management and compliance reporting.
- Threat Management - direct monitoring of user activity, data access and application activity and incident management.
- A deployment that offers a mix of compliance and threat management.

SIEM was developed to meet the governance compliance reporting requirements that have been developed, but companies are taking this as an opportunity to implement technologies that enhance their threat management and incident response capabilities.

2.4 **HONEYPOT**

The honeypot is a computer system and the directory is like a real computer. However, the purpose of this computer is to make hackers fall into it when we as users observe and follow their behavior. So we can define it as a wrong system that looks like a real system. They differ from other security systems in that they not only find a solution to a particular problem, but are also capable of implementing various security issues and finding multiple approaches to them [7]. For example, they can be used to record malicious activity in compromised systems, they can also be used to learn new threats to users and to develop ideas on how to resolve these issues. In general, the main goal in designing a honey pot is to attack and examine the system. Needless to say that behind the honey pot no valuable data should be.

Unlike other security tools, honeypots do not provide a stand-alone solution to specific problems [8]. For example, the firewall analyzes incoming and outgoing traffic and then determines whether the packet is allowed or not. They basically control the traffic in the network. Intrusion detection systems monitor networks or systems for unauthorized activity. Instead, honeypots are more flexible and apply to many security situations. You do not monitor or control the traffic. Instead, they receive the attack and collect data.
3. Research Methodology
The method used is the Network Development Life Cycle (NDLC), namely, analysis, design, simulation prototype, implementation, monitoring, and management. This method will be used to analyze and design the phases of research performed in this study, as shown in Figure 3.1 and research framework is shown in Figure 3.2.

![Figure 3. Topology Honeypot.](image1)

![Figure 4. NDLC Method.](image2)

![Figure 5. Research Framework.](image3)

Integrate and implement a security system designed with the actual system, both in monitoring cyber threats and automatically defending interference activity and redirecting inbound attacks to the shadow server to secure real data. Layered security is designed to ensure that data remains secure in accordance with CIA principles (confidentiality, integrity, and availability).

4. Result and Discussion
SIEM is here an application of software or appliance hardware devices in which there are applications that monitor suspicious activity in a network or system. SIEM checks the incoming and outgoing data on the inbound and outbound pages of a network and the system it owns. Honeypot here is a wrong system that uses the actual system to stop the shadow where here Honeypot hackers want to access the data from the server, in addition to the Honeypot here, as hackers are tempted to start their action at the Backup data against cyber threats intended for administrators. The software used to create this information security system is software that is open source, meaning that the software is used freely.
without having to pay the license. Open source software is also easy to get and can be freely downloaded from the Internet. The hardware needed to create an information security system is a server that has enough RAM and has been installed with the software needed to build an information security system.

The steps of the discovery system and the SIEM server are as follows:
1. The sensor as a collector in SIEM receives the protocol and returns it with various types of communication protocols.
2. The collector stores data in a SIEM database.
3. Subsequently, an analysis or risk assessment of the incoming and outgoing events is carried out by the network.
4. If the incident is considered a threat, IPS sends a command to the firewall to block access and provide information from the control panel.
5. The SIEM system displays all alarms and events detected by the sensor, the information coming from an information security system that is synchronized.
6. The user interface of the SIEM system allows the administrator to monitor events in real time.

4.1 SIEM and Honeypot General Architecture

The cyber security system consists of two main parts, the section having different tasks and functions. For the first part as a collector in information related to Internet security, system cyber security implemented by IDS sensors and other devices that send their logs to the SIEM. While the second part is the part that processes information, and collects information obtained from collectors. Information - The information is collected in a cyber security analysis database. Below you will find an overview of the architecture of the SIEM sensor, the database and the server.

4.2 Topology

Topology proposed, the system SIEM and Honeypot in the implementation can be applied as shown in Figure 3, where the system SIEM and the Honeypot All these devices are connected to the Internet network, where devices are used between LAN sensor, firewall, router, Switch, SIEM Server, System Server, Honeypot Server, and Switch are connected for employee PC distribution. Sentry leader in the system Cyber security Inbound sensor installs events capture from the outside, the sensor is connected to the firewall to ward off attacks on cyber security systems. Firewall is with a router to set the routing on cyber security system and the needs of the corporate network. Once it is
connected to the sensor outgoing to capture the event from the inside, then connected to 3-switch, SIEM in connection with the system SIEM, switching system connected to the system by a company honeypot from the server, and the last one Router connected to the distribution switch was overshadowed employee PC needs.

![Suggested Topology](image)

**Figure 8.** Suggested topology.

### 4.3 Attack Test System Test Results

If the server suffers a hacker attack in the form of SQL injection in a network of companies that have implemented the cyber security system using SIEM and honeypot. The attack on the server of the company was detected by the sensor.

![Attack Block Topology](image)

**Figure 9.** Attack block topology.

### 4.4 Results of Attack Attack System Tests

Attacked by DDOS hackers on the network of companies implementing the cyber security system with SIEM and Honeypot. The attack on the server of the company was detected by the sensor. From events intercepted by the sensor, iptables are routed and redirected to the honeypot server to distract hackers. So that the scanning process does not point back to the server, but to the honeypot.

![Attack Transfer Topology](image)

**Figure 10.** Attack transfer topology.

### B. Test Results of The Target Attack Transmission System

If the server receives a hacker attack in the form of port scanning in the network of companies that have implemented the cyber security system using SIEM and Honeypot. The attack on the server of the company was detected by the sensor. From events intercepted by the sensor, iptables are routed and redirected to the honeypot server to distract hackers. So that the scanning process does not point back to the server, but to the honeypot.
Figure 11. Topology of the transmission of the target attack.

The template is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

1) For papers with more than six authors: Add author names horizontally, moving to a third row if needed for more than 8 authors.

2) For papers with less than six authors: To change the default, adjust the template as follows.
   a) Selection: Highlight all author and affiliation lines.
   b) Change number of columns: Select the Columns icon from the MS Word Standard toolbar and then select the correct number of columns from the selection palette.
   c) Deletion: Delete the author and affiliation lines for the extra authors.

5. Conclusion
Based on the analysis of the application of Cyber Security System using SIEM and Honeypot at XYZ can close as follows:

1. The Cyber Security System was developed using a dual security system between Security Information Event Management (SIEM) and the Honeypot to effectively secure critical assets of the company. successfully developed by using company equipment to protect the system and data at XYZ.

2. The cyber security system is developed using enterprise devices and networks implemented through the Network Base IDS (NIDS) method.

3. Based on the results of the tests, the cyber security system with SIEM and Honeypot has the reliability and ability to maintain cyber security. A proven cyber security system with SIEM and Honeypot can overcome attacks on SQL Injection, DDOS, and Port Scanning testing.

References
[1] Indrajit, R. E. (2011). Pengantar Konsep Keamanan Informasi di Dunia Cyber. Jakarta: APTIKOM.
[2] Sarno, Riyanto., Iffano, Irsyat. (2009). Sistem Manajemen Keamanan Informasi. ITSPress.
[3] Deris Stiawan, Intrusion Prevention System (IPS) dan Tantangan dalam pengembangannya, Jurusan Sistem Komputer, FASILKOM, Universitas Sriwijaya.
[4] Mokube, I. & Adams M., 2007. Honeypots: Concepts, Approaches, and Challenges. ACMSE 2007, March 23-24, 2007, Winston-Salem, North Carolina, USA, pp.321-325.
[5] O’Brien, James A. 2005. Introduction to Information System. Mc Graw Hill.
[6] Research, G. (2011). How to deploy SIEM technology. Technical report.
[7] Mokube, I. & Adams M., 2007. Honeypots: Concepts, Approaches, and Challenges. ACMSE 2007, March 23-24, 2007, Winston-Salem, North Carolina, USA, pp.321-325.
[8] Spitzner, Lance. (2012). Honeypots: tracking hackers. Addison-Wesley Longman Publishing Co., Inc.