Developing and Analysis of Cyber Security Models for Security Operation Center in Myanmar

Wai Phyo Aung
Department of Automation Control System
Moscow Automobile and Road Construction State Technical University,Russia
myfamily46123@gmail.com

Htar Htar Lwin
Faculty of Computer Systems and Technologies
University of Computer Studies,Yangon
htarhtarlwin@ucsy.edu.mm

Kyaw Kyaw Lin
Department of Computer Technology
Defence Services Academy
Pyin Oo Lwin
kklin1500@gmail.com

Abstract

In counteraction to the increasing threat of cyber terrorism, the modeling to be predicted in guessing the predictive models for estimating the incidence of cyber-attacks for enterprise network in Myanmar are seriously needed. Although we need these models, there is no record of attacks, defenseless, outcome and threat to utilize the developing predictive models and authentication. The main purpose of this research is to determine whether SOC (Security Operation Center) manager uses cyber security model by using SOC results figures to prepare further cyber defense and incident response plan. The goal of this study was achieved by conducting experiments on various cyber-attacks occurred in security operation center of Industrial Control System (ICS).

Keywords: *Blue team, Incident Handling, SOC, Cyber Security Model, Vulnerabilities, Threats, Attack.*

I. INTRODUCTION

Responding to cyber terrorism, the researchers and practitioners need to develop and analyze the cyber security prediction models and to serve as a framework to be used as resource into the scheme to support the decision. Due to the harshness of cyber security problem and the confusion which can be caused by cyber-attacks on the Enterprise's information infrastructure, we are induced to build up the prediction models. The critical factor for cyber threat problems will be expressed in excerpts from the following our SOC reports.

Security analyst which represents the Blue Team of Enterprise network always watching the SOC. As per duties and responsibilities of SOC analyst, there are many events in every times. When he finds the critical events he will report that events to red team and purple team at first [1]. And then he will fix or patch that critical vulnerabilities. After that security analyst had many questions. Which sectors still get vulnerabilities and need to change or manage for coming cyber-attacks? SOC shows events according in their security directive rules. But SOC cannot show which sectors need to change or manage not to damage for upcoming attacks [2]. We will focus beyond the SOC to develop the predictive cyber security model.

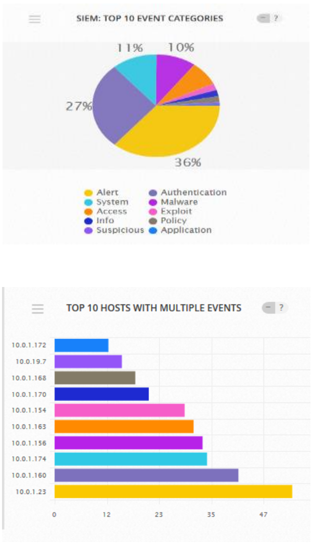

Figure 1. Top 10 events and hosts according SOC

Building up and knowledge of the theory of cyber security models is one of the important matters. Let us mention the types of cyber security models: the risk model and the exponential models. The risk model form one of the models can foresee the threat of attack in a weak position of indicated cyber security situation. It supports the incident handling including networking, log analysis, forensic and packet analysis. The exponential model called the second model, is time based and anticipate the duration between the probability of attacks for a given risk priority. It supports the incident response including logistic, communications, coordination and planning. The occasion happening during attacks is substitute measure of risks. When duration between attacks becomes longer, the risk of the user is becoming greater because of the result of a growing number of attacks. It is vital to note that we cannot be foreseeable the cyber-attacks which will happen in the near future. So the models mentioned above can be endorsed against the real-world attack. Illustration the important parameters and variables in the security operation center for researchers and SOC managers from Blue team can be only done.

There are the reasons why the experiments were conducted by solving with the help of cyber security. To get the occurring response the OODA Loop method, developed by US Air Force military strategist John Boy is needed to be employed. The OODA Loop method is aimed at attention to the crucial methods to be able to act in response to any information of security crisis: Observe, Orient, Decide, and Act (OODA). SOC can support various observation and orientation. Risk model can do decision making and exponential model can take response actions.

There may be coming up research questions that are crucial in response to cyber security crisis. These concerning questions are as below:

1) Can a variety of presentations and models of cyber security which is advanced provide the frame for researchers and practitioners to promote the field?
2) Can the models of hypothetical predictions be developed to evaluate the threat of different types of cyber-attacks?

Nonetheless, it is still useful to answer the upcoming questions after actions related to potential attacks if we provide explanations, equations, plots and analyses and synthesis. It stands to reason that we need to learn about the components of predictive models and their interactions to reflect objects and events in the enterprise network. The target of these models is for providing the SOC managers while investigating the assumption about how to take actions to cyber-attack prior to occurrence using risks, weakness, duration between attacks and interruption (number and time) concepts.

The rest of this paper is organized as follows. In section 2, we explored related works. Model structure of Risk Model was presented in section 3. Experiment and analysis were mentioned in section 4. We discussed and concluded our research in section 5. We left some future works in section 6.

II. RELATED WORK

Cyber security of Industry Control System (ICS) has become a major topic of active research [3]. It is of great importance and we need to realize the complexity and obstacles with these. They focused a main problem of cyber security research which means that it is supposed to concentrate on occurrence of security in dealing with the information and communication technology [4], while they barely calculate the real result of successful attacks. As a result, Access to risk of quantity is not that easy to get. Some of researches use Preliminary Interdependency Analysis (PIA) models that are well fitted for assessment of quantity of risk, as Both ICT and ICS are widely employed in. Even though PIA had not been used to explicitly express and inform cyber security concerns.

In [5] the researchers extended the risk assessments method Risk = (Asset Value * Event Priority * Event Reliability) / 25. There are several domains within cyber security end users related models, or organizational level modeling, therefore it supposed to narrow down his focus and then start work on it. It also give introduction the perception of cyber security according to its framework, workforces and other related information of personal data in the computer. Their works give results from an efficient audit of time based attacks which ruled with SOC's Host-based Intrusion Detection System (HIDS) and Network-based Intrusion Detection System (NIDS) correlation directives countermeasure. They calculated and correspondence the risk and exponential model under time based attacks. In their study they explore the attack parameters (sensitivity analysis) and time. As a result, the competitor would decide the same even if attacker is addressed at several times the same choice during the violence. That’s why studying the behavior of one attacker and attack-strategy at a time will be enough to find out; comparison of the impact of multiple, different classes of intruders and various attack-strategies require building separated models and studies.

In this research [6] cyber security operations center installment of models are proposed to provide better and advancing awareness to situation in order to detect common and frequent advantage, and also approached and cross-channel exploits. 0 (Zero) day exploits are now common and frequent, and impacts far much greater than before. This situation is further made worse by the lack of sufficient and well deployed security operations centers to watch organizational cyber investments to get perimeter defense.

In this research paper we used Open Source Security Information Management (OSSIM) which was provided AlienVault. It includes HIDS and NIDS.

III. MODEL STRUCTURE OF RISK MODEL

This model relates the basic theory of information security which is probability of attack, likelihood of weak points and outcome of an attack. We assume that risk can be accurately calculated by using equation (1).The justification is that risk in intuitive way would increase as all three quantities comprising equation (1) increase.

Risk (R) = Relative Probability of Attack (A) * Probability of Vulnerability (V) * Consequence (C)

As the symbol, we can assume their identification

$$R_1 = P_{ai} * P_{vi} * C \qquad (1)$$

Examples of (2) include:

$R_1 = P_{ai}$ (Malware) * P_{v1} (AD server down) * C_1 (Consequence of Risk priority 1) (2)

$R_2 = R_{a2}$ (Hash dump) * P_{v2} (SMB open) * C_2 (Consequence of Risk Priority 2) (3)

The measure for probability of attack, relative probability of attack, is estimating using the following equation.

$$P_{ai} = \frac{T_L(i)}{\sum_{i=1}^{n} T_L(i)} \qquad (4)$$

P_{ai} = Relative probability of risk priority i (attack types).

$T_L(i)$ - Relative threat level of attack of risk priority i

IV. CYBER SECURITY IN ENTERPRISE INFRASTRUCTURE

TABLE I. CYBER SECURITY IN CRITICAL ENTERPRISE INFRASTRUCTURE

Vulnerability V_i	Consequence C_i	Attack Vectors,Risk Priority A_i
V_1 - Network Firewall	C_1 - Firewall down	A_1 - Denial of Service (DoS)
V_2 -Host firewall	C_2 - AD server down	A_2 - Man in the Middle (MITM)
V_3 - Password Capture Protection (https)	C_3 - Web server down	A_3 - Information disclosure
V_4 - Web Application Firewall (WAF)	C_4 - Operating System crash	A_4 - Malware (Ransomware)
V_5 - Host Malware Protection	C_5 - Application corrupted	A_5 - Virus (damage Database and OS)
V_6 - Host Endpoint Security	C_6 - Hardware Failure	A_6 - Trojan
V_7 - (Network Instruction Detection System (NIDS)	C_7 -Router Misconfiguration	A_7 - Remote Code Execution (RCE)
V_8 - Data Loss Prevention (DLP)	C_8 - Transmission Link Down (ISP down)	-
V_9 - IP security	C_9 - Proxy server down	-
	C_{10} -Power failure	-

R_i - Risk of priority i. Risk priority is the consequence of a given types of attack (DoS, Virus. Malware,etc.)

P_{ai} - Relative probability of risk priority i.

P_{vi} - Probability of vulnerability of risk priority i. we must count or scan this probability in each endpoint.

C_i - Consequence associated with risk priority i. The numbers of network objects that affected (AD Server, WEB server, UPS for power failure, etc.)

$T_L(i)$ - Relative threat level of attack of risk priority i.

N – Total numbers of various attacks.

V. EXPERIMENT AND ANALYSIS OF MODELS

In this section, we calculate Risk Model and Exponential Model. Then analyze Time based attacks and Rate of change of Time between Attack events.

A. Calculation for Risk Model

We will calculate and plot that demonstrate risk model outputs. The sensitive data in the Table I was developed as follows. The first column of the table shows 10 major types of attacks in our Enterprise network. Starting with Alert – the most severe and ending with Application the least severe.T_L (i) also represent a subjective assessments of the relative threat level of various types of attacks, starting with Alert = 68,700 which was 37% of the whole critical security events, and ending with corrupt of Application = 704 is computed from (4).

Data is not still available for P_{ai} .We calculate the relative threat level (P_{ai}) from real time SOC system. The desired output risk = R_i is computed from Eq (1). The bold values in the table emphasize the significant results. Figure 2 shows how risks differ from the probability of attack. The plot is made notes with the types of attacks associated with the major risk values. As [7] a practical matter, the plot indicates that risk would rise rapidly at a value of $P_{ai} \cong 0.15$.

This could be assumed a major risk and that the blue team should prepare to incident response plan for weak security policy.

TABLE II. ATTACK TYPES AND DATA FOR RISK MODEL

	Attack Type	$T_L(i)$	Related Threat Level = Relative Probability of Attack P_{ai}
1	Alert	68,700 (37%)	0.322
2	System	20,615 (11%)	0.096
3	Access	13,687	0.064
4	Info	3,475	0.016
5	Suspicious	1,288	0.006
6	Authenticat ion	49,044 (26%)	0.230
7	Malware	18,230 (10%)	0.085
8	Exploit	3,734	0.017
9	Policy	3,3436	0.157
10	Application	704	0.003
		$\sum_{i=1}^{a} T_L(i)$	$\frac{T_L(i)}{\sum_{i=1}^{a} T_L(i)}$

TABLE III. ATTACKED HOST AND DATA FOR CALCULATION RISK MODEL

	Attacked Host	Rate of Attack (N(T))	Vulnerabilities which is scanning from each endpoint host P_{vi}	$R_1 = P_{ai} + P_{vi} + C_i$	C_i
1	10.0.1.172	12	0.66	0.21	1
2	10.0.19.7	15	0.55	0.21	4
3	10.0.1.168	18	0.44	0.16	6
4	10.0.1.170	21	0.77	0.03	3
5	10.0.1.154	29	0.55	0.01	2
6	10.0.1.163	31	0.77	0.17	1
7	10.0.1.156	33	0.88	0.15	2
8	10.0.1.174	34	0.33	0.01	2
9	**10.0.1.160**	**41**	0.33	**0.25**	5
10	10.0.1.23	53	0.11	0.01	1

However we note in Table II that R_i is significantly a function of consequences C_i. Thus the analysis of the assignment of C_i to the relative threat levels could be performed.

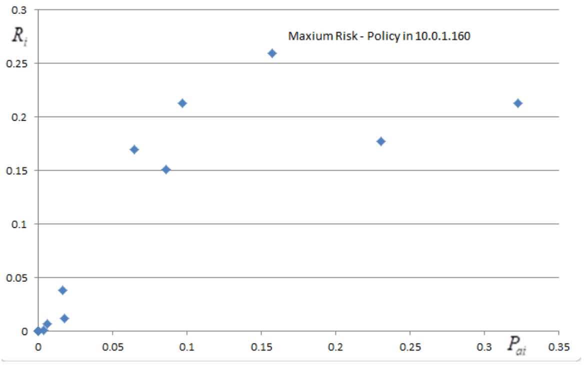

Figure 2. Risk R_i and probability of attack P_{ai}

Figure (1) and (2) shows us the relationships among risk, probability and consequences. We analyzed to have more than one view of the relationships to prove the others. (i.e Figure (3) make proves that the Figure (2) show the Security Policy weakness being the major risks.)

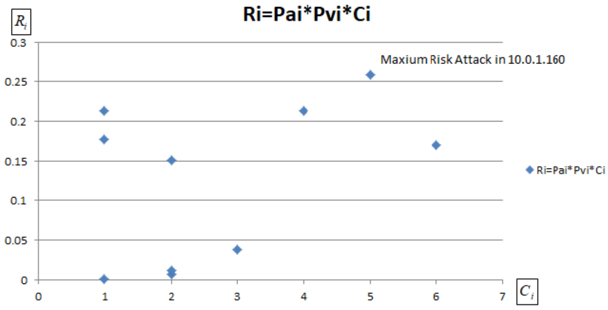

Figure 3. Risk R_i and consequence C_i

Figure (3) shows that risk increases with consequences, as we would expect and again the diagram is annotated with the major risk attacks of Security Policy weakness.

B. Calculation for exponential model

The basic of this predictive cyber security model is that the time between attacks, t_a is a key changeable in working against attacks. P_{ai} is data on probability of attack. We measure relating level of threats, T_L to estimate P_{ai}. t_a can measure the risk because of the smaller the value of t_a which can happen the growing frequency of attack. (i.e. the higher risk). This cyber security model opposed the accounts of risk priority (i) and specific types of attacks and attacked hosts from the events of SOC.

$$P_{ai} = f(T_L) \qquad (5)$$

In the above equation, to develop the model, we formulate probability of attack as a function of relative threat level.

Where, T_L = relative threat level;

t_a = time between attack of type a day.

N (T) = number of attacks in Time T. (we gets that data from our enterprise SOC)

T = specified attack time period in 365 days

$$\lambda = \frac{N(T)}{T} \text{ = rate of attack per day} \tag{6}$$

$$P_{ai} = \lambda e^{-\lambda t} a \tag{7}$$

In the above Eq means the probability of density function for the exponential distribution by assuming for P_{ai}. We calculate the Eq (7) to produce the following equations (8) and (9)

$$\log(P_{ai}) = \log\lambda - \lambda t_a \tag{8}$$

$$\lambda t_a = \log\lambda - \log(P_{ai}) \tag{9}$$

By solving equation (9) for t_a, we obtain equation (10)

$$t_a = \frac{1}{\lambda}\log(\frac{\lambda}{P_{ai}}) \tag{10}$$

C. Analyzing Time Based Attack

The plot of time between attacks t_a and probability of attack P_{ai} is shown in Fig (4). In our events data, there is no saturation t_a > *24* hours. Because of low value of t_a imply high frequency of attack.

Growing time of attack may also occur high risk. This security policy would exclude all attacks vectors except Denial of Service (DoS) / Distributed Denial of Services (DDoS). This plot shows us how much we can manage incident handling response as quickly as possible.

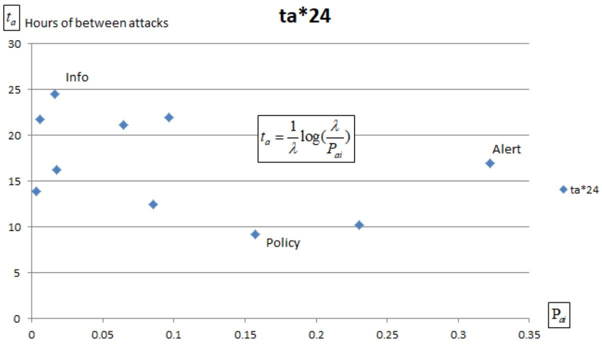

Figure 4. Expected frequency of attack and probable attack *Pa(t)* at time t 24 hours**

If our enterprise network gets DDoS attack. We can measure the increasing traffic based on . By seeing upcoming NetFlow results, Firewall throughputs and DDoS Protectors throughputs, we can countermeasure the stability of DDoS protector live.

TABLE IV. CALCULATION OF TIME BETWEEN ATTACKS

Rates of Attack in 365 days (N(T))	P_{ai}	**Attack by Day** $\frac{N(T)}{T}$	**Days between Attack** $\frac{1}{\lambda}\log(\frac{\lambda}{P_{ai}})$	**Hours between Attack** $(t_a * 24)$	**Hours between Attack** $\frac{d(t_a)}{d(P_{ai})}$
1200	0.322	3.287671	2.321313915	16.94559158	-0.286727058
1500	0.096	4.109589	3.748187699	21.88941616	-0.611536032
1800	0.064	4.931507	4.340081745	21.12173116	-0.639638551
2100	0.016	5.753425	5.865084423	24.46578073	-1.850949244
2900	0.006	7.945205	7.180361666	21.68964421	-2.618641519
3100	0.230	8.493151	3.607425814	10.19388714	-0.060183666
3300	0.085	9.041096	4.659595437	12.36910789	-0.142880631
3400	0.017	9.315068	6.275036943	16.16744812	-0.657136758
4100	**0.157**	11.23288	4.270095367	9.123423272	-0.050466813
5300	0.003	14.52055	8.3874253	13.86298974	-1.434377651

D. Rate of change of Time between Attacks events

The rate of change of time between attacks is related to the possibility of attack is obtained by making a distinction (10).

$$\frac{d(t_a)}{d(P_{ai})} = -\frac{1}{\lambda}(\frac{1}{P_{ai}^2})(\frac{P_{ai}}{\lambda}) = -(\frac{1}{\lambda^2})(\frac{1}{P_{ai}}) \tag{11}$$

It gives the (11) which tabulates in Table IV.

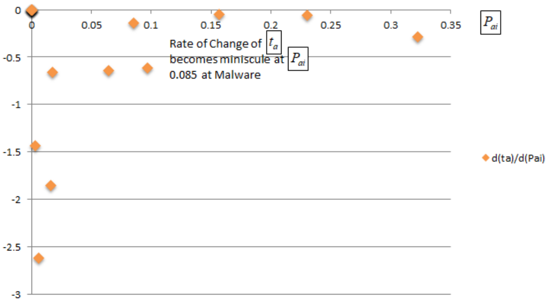

Figure 5. Rate of change of time between attacks *d(t_a) / d(P_a)* and probability of attacks P_{ai}

That quantity is of interest because we can see when the rate of change of t_a which is a replacement for risk. t_a becomes small that the threat is virtually nonexistent. That saturation is demonstrated in Fig (5), where P_{ai} = 0.085 corresponds to a Malware attack. At that point, the pace of change is too tiny, meaning that the pace of change of risk is of little.

VI. Discussion and Conclusion

Having stated that time between attacks t_a is a delegate for risk R_i. We analyze and investigate this hypothesis by scheming the former against latter. The result is shown in Fig (6).

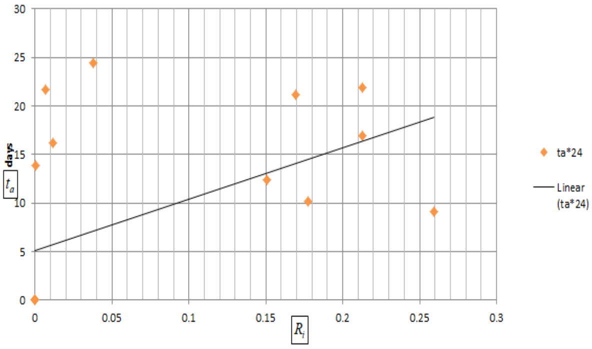

Figure 6. Time between Attacks t_a and Risk R_i

It shows a fairly good correspondence. The fact that the proponent model called exponential in another way is much easier to execute than the risk model is of importance. The former could use the SOC manager's prediction model of choice [8].

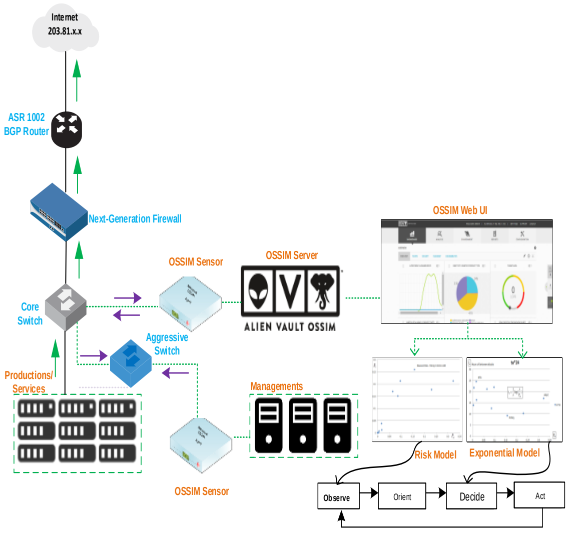

Figure 7. Big picture of SOC analyst for incident handling and response

There are many huge cyber attacks daily in real world. SOC analyst should handle the top major attacks which are pushed by the security policy and best practice for infrastructure security. Risk and Exponential models are fully effectiveness for priority of incident handling and response as OODA loop among that many huge cyber attacks: What is critical and How is it protected ?

In the research question section, we suggested the following questions were answered by this research paper:

1) Can different show off and models of cyber security which is advanced provide the frame for researchers and practitioners to promote the ICT/ICS security research field?

Our paper suggests that, explanation, equations, plots, tables which comprise a frame work depending on our blue team for ICT/ICS security research, the answer is "true".

2) Can the models of hypothetical predictions be developed to evaluate the threat of various and sophisticated types of cyber security attacks?

For answering this question is also "true" we calculate and demonstrate as evidence relevant scheme. (i.e. The Risk Model in Figure-2 identifies the maximum risk attacks, which was security weakness policy. Furthermore, with respect to the Exponential model, Figure-4 provides us with the probability of attack and Time between Attacks threshold.

VII. Future Study

We left some works to do as future research. We are still developing in writing of SOC directive rules to do as future research. Our study is limited to the effect of a malware type of attack on system behavior: a cyber-attack via the Ransomware of a sub-station. According detective of SOC, cyber security model need to extend for multiple stations..

Acknowledgments

This work was partially provided by the private data center under the development of open source Security Operation Center (SOC) project that is called Open Source Security Information Management (OSSIM). We collected the required data for our analysis.

References

[1] SAN SEC450: Blue Team Fundamentals: Security Operations and Analysis

[2] SAN SEC511: Continuous Monitoring and Security Operations.

[3] O. Netkachov, P. Popov, and K. Salako, "Model-Based Evaluation of the Resilience of Critical Infrastructures Under Cyber Attacks", 9th International Conference on Critical Information Infrastructures Security

[4] C. Onwubiko, “Security operations centre: Situation awareness, threat intelligence and cybercrime”, International Conference on Cyber Security And Protection Of Digital Services (Cyber Security), 2017

[5] K. Thakur, M. Qiu, K. Gai and M.L. Ali, “An Investigation on Cyber Security Threats and Security Models”, IEEE 2nd International Conference on Cyber Security and Cloud Computing, 2015

[6] ICS410: ICS/SCADA Security Essentials

[7] L.Janczewski and A. M. Colarik, “Cyber warfare and Cyber Terrorism”, ISBN- 9781591409922

[8] D. Murdoch, “A Condensed Guide for the Security Operations Team and Threat Hunter”, Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1.02), ISBN-10: 1091493898