General approach to automating the process of responding to computer security incidents

A V Pilitsky, O E Prokopenko and V N Halizev
Kuban State Technological University, Krasnodar, Moscovskaya str., 2, 350072, Russia
E-mail pilitsky.alex@yandex.ru

Abstract. The article considers the process of responding to information security incidents as a cyclical process divided into several stages. The main approaches to automating response processes are presented, as well as cases in which automation is not effective.

Keywords: information security; investigation; response; automation; information security incident.

1. Introduction
Now it is impossible to imagine any organization without its own information system, whether it is a large Corporation or a small private business, the only difference is in the scale of this system. And every year the economic losses of enterprises due to computer security incidents only grow. We can't say that there were no such incidents before. No, they were, but not in such quantity.

At the moment, there are no organizations or people who are not victims of hacking or, for example, a computer virus. Yes, now, probably, everyone has an idea about an antivirus program, and it is possible that almost every enterprise has it installed, but there is no such thing as "absolutely protected system". Any system can be hacked, regardless of the degree of its security, it only needs funds, sometimes not only of an intellectual nature, but also financial. With these two components, you can get around everything. This is when computer security incidents occur. If your system does not provide protection against this type of incident, then you can only protect yourself from it in the future.

to do this, you need to investigate the computer security incident that occurred, and take appropriate measures so that the security system will prevent such a case in the future.

Now we live in the age of information technology, and where the means and methods of protecting information are being strengthened, the capabilities of hackers (intruders) are also growing. It is worth noting that the development of the second is faster. Every year there are more and more targeted attacks that require a large amount of resources, both material and human, to investigate them. This is due to the fact that, as a rule, such attacks affect a large number of enterprise assets using advanced penetration techniques and anchoring in the information infrastructure. Investigating these types of incidents requires experienced specialists who take years to prepare. At the same time, in addition to complex attacks, there are also simple attacks, but also require the response of specialists. It becomes impossible to provide sufficient incident response specialists. The solution to this problem was the use of automation tools for investigating computer security incidents.
This approach allows you to reduce the number of specialists involved in the investigation of an incident, increase the speed of response, and allow automation tools to resolve simple incidents that do not require human intervention on their own.

As mentioned above, first of all, automation processes allow specialists to focus their attention on cases where human intervention is required, but this approach is not always correct. Automation of some processes can lead to an increase of cases in false positives, and sometimes cause important indicators that show a more serious and complex attack to be missed. Just like any other software, automation tools may contain errors in the code that may lead to the leakage of critical information [1].

General approaches to investigating computer security incidents.

There is no one-size-fits-all method for investigation, each organization must adapt standard recommendations based on its own characteristics and priorities. The approach to investigating computer security incidents in a particular company will depend on many factors, whether it is the role of the Information security Department, Information security policy, acceptable risk level, and others. But if you study international standards and best global practices, the General approach to responding to computer security incidents can look like the one shown in the Figure 1 [2].

![General approach to incident response](image)

Figure 1. General approach to incident response

2. The need to automate the investigation of computer security incidents

SOC (Security Operations Center) analysts perform two types of work: investigating template incidents that often do not deviate from the standard scenario, or reviewing tasks that require special analysis and often a lot of experience to investigate such an incident. Based on this, a problem arises: the necessary specialists with sufficient skills are not enough to solve the second type of work, while the first requires a large number of employees, which is very expensive.

Routine analysis can be automated, which is advisable on the bases of financial and human costs. This process of automating the investigation of computer security incidents has a number of advantages and disadvantages.

Based on the fact that many organizations have huge information systems, it will be impossible to hire the necessary number of employees to effectively investigate incidents. Firstly, it is economically inefficient, and secondly, a person processes simple requests slower than a machine.

Thus, the advantages of automating the investigation of incidents will be:
1. more appropriate (logical) response to notifications and requests;
2. Higher volume of application closing and incident response;
3. more careful attention of analysts to higher priority issues;
4. Improved visibility of what is happening;
5. Coverage of a larger area and a larger number of applications [3].

But also in any situation, in addition to the pros, there are a number of disadvantages. If you take, for example, critical infrastructure systems, then false positives can lead to disastrous results, especially if you take healthcare or communications. In such systems, disabling critical components will lead not only to economic damage, but also to the loss of human lives.

Disadvantages of automation:
1. Incorrect classification of the attack, so the wrong actions are taken;
2. Automation of requests that should have been processed manually;
3. Omission of key information or data;
4. The adoption of incorrect or inappropriate decisions;
5. The creation of excessive and expensive dependencies [3].

These days, organizations use the automation process because, in their opinion, without it, the probability of missing an attack that will cause huge damage is worse than the possibility of negative consequences of the automation process.

Basically, the process of automating the investigation of computer security incidents is considered as automation of everything. But companies can only upgrade some of the most relevant and secure stages of the incident investigation process. The idea is to find a balance between the elements that are best automated and the parts that will be processed by analysts.

3. Automating investigation of incidents of computer security

3.1. Preparation

The preparation phase includes activities to create a system for protecting the information infrastructure from attacks. At this stage, security policies are formed, information security tools and monitoring systems are adjusted based on knowledge about the types of possible attacks and potential violators. Collecting and correlating information about threats and sources, as well as information about past incidents, can greatly simplify the task of specialists in the field of building a security system, as well as increase efficiency by using the most relevant information from a large number of sources. The main types of such information are:

1. SIEM data and log Files
2. checking the reputation of IP, URLs, files, and domains
3. Search in the white and black list
4. IP Geolocation
5. Similar events, same goals, and critical resource checks
6. Threat analysis

Threat analysis platforms collect data about cyber threats and make it available to your organization. There are many useful channels, including HPE Threat Central, FireEye iSIGHT, and IBM X-Force. Integrating with one or more of these channels for automatic enrichment is a great way to immediately put each incident in context.

3.2. Detection and analysis

The promise of security automation lies in the ability to automate not only the collection of information, but also entire processes. Some automation providers have a vision of a SOC that addresses threats and responds to warnings without human intervention. This type of automation can be useful, but there are also negative aspects to this approach. They will be discussed further.

As a rule, at this stage, detection is performed by automated tools that use certain rules formed by the analyst at the preparation stage. The success of the response depends on how well these rules were drawn up, and whether they correspond to current threats.

Among the automated analysis tools, it is worth highlighting sandboxes. These tools allow you to dynamically analyze files that enter the system and identify malicious software based on signatures and behavioral analysis. Using such solutions allows you to switch the attention of analysts to cases where atypical exploitation and infection techniques are used.
When a particular trigger has worked, the system must perform a certain number of actions to prevent an attack. These actions are also prescribed by a specialist. However, it is important that not all actions are performed automatically. If the system sees deviations from the specified pattern, this incident should be passed to analysts, so that they can analyze the data manually to understand the reason for its occurrence, and form a new rule or exception based on the received data.

3.3. Prompt response to an incident
At the incident response stage, it is important that tasks are quickly distributed so that the workload of specialists is uniform. It is also important to establish communication between departments so that employees do not spend extra time providing and receiving information.

Automatic notifications make status updates, collaboration, reporting, and task management more streamlined and error-free. This provides a big operational advantage over manual processes that force analysts to search for contact information, prepare reports, and delegate responsibilities manually—all during the chaos of a security breach. Examples of valuable automated communications include:

- Reports
- Assign tasks on the basis of the playbooks
- Notification of the action

Warning fatigue is a serious problem for most corporate SOCs. Analysts are clogged with thousands of warnings, and most of them are false. Automation allows analysts to focus on warnings that pose a real threat to the company. Using prediction criteria, the system can automatically set priority levels in analyst queues to reduce the number of most likely false positives. This can take the form of a percentage of the probability of a false positive assigned by the system, or a more General risk assessment. If designed correctly, this type of incident response automation can significantly increase the productivity of your SOC.

3.4. Securing the results of the investigation
At this stage, new or old security policies are formed based on the received information about the incident. Here, automating the collection of statistics and correlating the results obtained with existing ones will allow you to look at the situation much more broadly and may allow you to identify larger chains of attacks on specific resources, which in the future will allow you to form a strategy for protecting specific assets based on the context of possible previous attacks.

4. Processes that do not require automation
Despite all the advantages of automation, there is a number of cases in which this approach may not only be ineffective, but also lead to a threat to the security of the infrastructure.

When automating, it is important that all necessary actions that can affect the interaction of infrastructure elements, or their integrity, are confirmed by a specialist. An error in the processing of input parameters or the logic of the system can paralyze the operation of the enterprise by, for example, blocking critical resources. Such an error can cause damage equal to the actual attack.

It is also important that the investigation is not fully automated. The participation of specialists is due not only to the existence of complex cases, but also to the fact that the incident response system must be flexible and meet both information security trends and regulatory requirements of global and local regulators. And it is the specialists who ensure the updating of the system.

It is important that automation tools do not restrict the incident response system in any way in the field of its modernization. The system should not only solve strictly typed tasks, but also maintain a database of past incidents and decisions. All this is necessary so that in the future I can dynamically make decisions based on similar cases.

Integration with third-party sources is a significant aspect in building an automated response system. Some automation platforms get all their functionality by connecting to external data sources, which often overlap with each other or with data from existing internal sources. Not to mention that these external data sources often require expensive subscriptions, and in some cases even require creating or
maintaining integration. The cost of this approach can scale very quickly, while your ability to respond to incidents depends on the uptime of a dozen different integrations and companies. Therefore, you should avoid this type of dependency if it doesn't pay off.

5. Conclusion
Thus, we can say that large and medium-sized companies cannot do without automating the investigation of computer security incidents. This will allow companies not only to compensate a huge number of employees, but also to quickly respond to incidents that cause material and sometimes reputational damage. But automation should not be 100%. every step of this process should be considered - whether there is a need to improve this stage of the investigation. It is also necessary to take into account the individual factors of your company when automating a particular step.

References
[1] Security Orchestration and Automation Benefits: How SOAR Helps Improve Incident Response: https://securityboulevard.com/2020/04/9-security-orchestration-and-automation-benefits-how-soar-helps-improve-incident-response/
[2] Incident Response Steps and Frameworks for SANS and NIST: https://cybersecurity.att.com/blogs/security-essentials/incident-response-steps-comparison-guide
[3] SOC Automation-Deliverance or Disaster (A SANS Spotlight Paper Written by Eric Cole, PhD December 2017)
[4] Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2)
[5] Automating security events management (FabianLibeau(EMEA marketing director, ArcSight)) https://doi.org/10.1016/S1353-4858(08)70139-9
[6] Automated systems only: why CISOs should switch off their dumb machines (Spencer Young) https://doi.org/10.1016/S1353-4858(19)30106-0
[7] The future of information security incident management training: A case study of electrical power companies (Maria Bartnes, Nils Brede Moe, Poul E.Heegaarda) https://doi.org/10.1016/j.cose.2016.05.004
[8] Linux Forensics (Published by Pentester Academy, a division of Binary Security Innovative Solutions Pvt. Ltd)
[9] Actionable Information for Security Incident Response (European Union Agency for Network and Information Security, November 2014)
[10] A methodology for improving informationsecurity incident identification and response (Master Thesis Informatics & Economics By Nanno Zegers)