UDC 004.056
doi:10.31799/1684-8853-2024-2-39-50
EDN: YXVAJI

Articles

Security assessment based on attack graphs using NVD and MITRE ATT & CK database for heterogeneous infrastructures

R. O. Kryukov[a], *PhD, Tech., Lecturer, orcid.org/0009-0008-3422-7234*
E. V. Fedorchenko[b], *PhD, Tech., Senior Researcher, orcid.org/0000-0001-6707-9153*
I. V. Kotenko[b], *Dr. Sc., Tech., Professor, orcid.org/0000-0001-6859-7120, ivkote@comsec.spb.ru*
E. S. Novikova[b], *PhD, Tech., Associate Professor, orcid.org/0000-0003-2923-4954*
V. M. Zima[a], *PhD, Tech., Professor, orcid.org/0009-0006-9412-4160*
[a]*A. F. Mozhaiskii Military Space Academy, 13, Zhdanovskaia Emb., 197198, Saint-Petersburg, Russian Federation*
[b]*St. Petersburg Federal Research Center of the RAS, 39, 14th Line, 199178, Saint-Petersburg, Russian Federation*

Introduction: *Security assessment of modern information systems is a challenging task. These systems incorporate heterogeneous objects, things, subjects and connections between them. They are continuously changing and generate a lot of events. As a result, the system security state is constantly changing.* ***Purpose:*** *To develop an approach for security assessment of the heterogeneous information systems.* ***Results:*** *We develop and present an approach to security assessment. It incorporates data gathering from various sources, log preprocessing, security incidents detection, mapping the security incidents to the nodes of the attack graph, security assessment and forecasting, and results representation. The novelty of the proposed approach is in the technique for mapping the detected incidents to the stages of the targeted cyber attacks. This technique uses the Emerging Threats correlation rules to output the security incidents based on the detected events. It also uses the Targeted Attack Analyzer (Indicators of Attack) rules that describe security incidents (signatures) using Sigma language to map the detected security incidents to the attack patterns from the MITRE ATT & CK database. Thus, the proposed technique allows one to map the detected events to the attack graph nodes and assess and forecast the targeted cyber attacks. The attack graph is generated using MITRE ATT & CK attack patterns and vulnerabilities from the National Vulnerability Database. The approach is implemented in the Python language. The test environment is deployed to test the mapping of the detected security incidents to the known attack patterns.* ***Practical relevance:*** *The investigation results can be used in the construction of security assessment systems that are aimed at strengthening cyber security of heterogeneous information systems.*

Keywords *— security assessment, cyber security incidents, event correlation, signature, cyber attack, attack graph, MITRE ATT & CK, National Vulnerability Database, targeted attack analyzer, indicators of attack, emerging threats.*

For citation: Kryukov R. O., Fedorchenko E. V., Kotenko I. V., Novikova E. S., Zima V. M. Security assessment based on attack graphs using NVD and MITRE ATT & CK database for heterogeneous infrastructures. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 39–50. doi:10.31799/1684-8853-2024-2-39-50, EDN: YXVAJI

Introduction

Currently, digitalization covers more and more areas of human life. Along with advantages, it leads to new threats. Thus, supporting information technology infrastructure is vulnerable to cyber threats. Their successful implementation can lead to such consequences as power outage that is uncomfortable for people and crucial for the industry, for example, water treatment, medical infrastructures, etc.

Modern information technology infrastructures are characterized by a high level of complexity and heterogeneity. Security information and event management systems (SIEM) were introduced to monitor the system's processes and to detect malicious ones. These systems allow early attack detection and forecasting and provide security incident forensics utilities. SIEM systems collect events from different sources and implement their correlation analysis to support these tasks. The event correlation in information security allows revealing the dependencies between the events relating to the same cyber security incident [1]. It incorporates the following stages: normalization, preprocessing, anonymization, aggregation, filtering, correlation itself, and prioritization [1]. The event correlation results are the cyber security incidents. They are used by the researchers to attribute the attacker [2–4], forecast the attack development, and select measures for countering cyber attacks.

In this paper, the authors focus on the targeted cyber attacks as multi-step and hard-to-detect attacks. A targeted attack is a type of cyber attack that is aimed at compromising a specific system or object. Such attacks can have different development vectors (techniques). They incorporate the following standard stages: reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense, evasion, credential access, and discovery. The stages may vary depending on

the object under attack. The consequences of the targeted cyber attack can be crucial. Detection of cyber attack at an early stage can help avoid considerable damage. Both attack detection and prevention require event correlation. It allows detection of the cyber security incident and mapping it to the appropriate attack stage and technique for further prevention.

The researchers proposed various event correlation techniques for the SIEM systems based on the manual [5], supervised [6], and unsupervised methods [7, 8]. Existing information security monitoring tools implement these techniques. At the same time, while most security monitoring tools allow detecting cyber security incidents using correlation techniques, they do not allow mapping the detected security incidents to the targeted cyber attack stages. To fill the gap, the paper [9] introduced the technique based on the set of Emerging Threats (https://rules.emergingthreats.net/open/suricata-5.0/rules/) correlation rules and on the set of Targeted Attack Analyzer (Indicators of Attack) (TAA (IOA)) rules (https://support.kaspersky.com/KATA/3.7.1/en-US/194907.htm). The set of Emerging Threats correlation rules is applied for events correlation to output cyber security incidents. The set of TAA (IOA) rules is used to map the detected security incidents to the stages of the targeted cyber attacks. The TAA (IOA) rules describe behavior in the system (signature) that could indicate a targeted attack (security incident) and can be validated in real time [10, 11]. The authors [9] use the open dataset of the TAA (IOA) rules specified in Sigma language (https://github.com/SigmaHQ/sigma/tree/master/rules) and integrated with the MITRE ATT & CK database (https://attack.mitre.org/). The IOA allows mapping the security incidents (signatures) to the attack stages from the MITRE ATT & CK database, namely, reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense, evasion, credential access, and discovery. The technique proposed in [9] allows detecting the security incidents based on the security events and mapping them to the IOA mapped to the MITRE ATT & CK tactics and techniques. The research was presented at the 5th International Workshop on Attacks and Defenses for the Internet-of-Things (ADIoT 2022).

In this paper, the authors describe the common approach to security assessment based on attack graphs using the National Vulnerability Database (NVD, https://nvd.nist.gov/) and MITRE ATT & CK database that incorporates the technique presented in [9] as one of the stages. The authors also introduce a novel attack graph model that integrates attack stages represented using MITRE ATT & CK objects and attack actions represented using the vulnerabilities from the NVD, and security assessment technique based on the proposed attack graph and mapping of the security incidents to this graph. The proposed approach allows forecasting of the next attack steps, and in prospect, it will allow timely responses against cyber attacks.

The main *contributions* of the paper are as follows:

– the approach to security assessment of the information systems using NVD and MITRE ATT & CK database. It is based on attack graphs. The developed approach uses the technique for detecting and mapping the cyber security incidents presented in [9] as one of the stages;

– a novel attack model in the form of the attack graph, constructed considering cyber attack stages and vulnerabilities of the system under analysis;

– the security assessment technique. It is based on the developed attack graph and the mapping of the security incidents to the generated graph.

The *novelty* of the proposed solution is as follows:

– the comprehensive approach to the security assessment using NVD and MITRE ATT & CK and considering mapping of the security incidents to the cyber attack stages. It uses the technique for detecting and mapping the cyber security incidents presented in [9] as one of the stages;

– the attack graph that differs by the joint consideration of the attack stages and attack actions;

– the security assessment technique based on the proposed attack graph and mapping of the security incidents to the graph.

Related research

Currently, a wide variety of event correlation techniques has been proposed [8]. They could be classified into three main groups according to the knowledge extraction method: manual, supervised, and unsupervised. Rules and signature-based approaches form the first group, while the second and third groups include corresponding machine-learning techniques and algorithms. Despite their variety, their primary goal is to generate security incidents based on observed system, network, and application events.

Such techniques are used in SIEM systems to detect anomalous activity. Thus, Splunk Enterprise Security (https://www.splunk.com/en_us/products/enterprise-security.html) uses correlation based on the trained neural network to detect anomalies in the event stream using the trained neural network. QRadar SIEM (https://www.ibm.com/qradar/security-qradar-siem), HP ArcSight Security Intelligence (http://www.microfocus.com/en-us/cyberres/secops/arcsight-esm), and MaxPatrol SIEM (https://www.ptsecurity.com/ww-en/products/mpsiem/) use rule-based correlation methods.

Few security solutions implement further mapping of the security events and accidents to the indicators of attacks. This functionality is often implemented as an additional component, and is based on expert rules. For example, PT Network Attack Discovery component (https://mitre.ptsecurity.com/en-US/techniques?utm_source=pt-main-en&utm_medium=slider&utm_campaign=mitre) from Positive Technologies implements automated mapping of the detected incidents to a set of the attack techniques and tactics. SIEM QRadar from IBM includes QRadar Use Case Manager. It provides functionality for the generation of rules to map the detected incidents to specific tactics and techniques.

There is a public knowledge-based repository of adversary tactics and techniques — the MITRE ATT & CK repository. It incorporates more than 620 attack techniques for enterprise information platforms. The provided tactics, techniques, and procedures are classified by the attack stages. Another recent MITRE research effort, D3FEND, attempts to link known countermeasures to corresponding attack techniques. One of the most common ways to use MITRE ATT & CK matrix is modeling attack paths to determine missed attack steps and appropriate countermeasures [12–14]. For example, in [14], a methodology for a system security assessment based on the attacker's behaviour modeling is presented. The attacker's behaviour is represented as a sequence of techniques specified in the MITRE ATT & CK matrix.

In [12], authors propose a new structure that links the attack graph and attack kill chain steps. As the attack graph is constructed for a given system configuration, the proposed structure maps the given system to the possible attack steps and recommended countermeasures. The mapping of the MITRE ATT & CK techniques to the attack graph elements is implemented using a ruleset defined manually.

Xiong et al. developed a threat modeling language that allows modeling attacks in the system being analyzed [13]. It enables the specification of the information system entities. Then the textual descriptions of the MITRE ATT & CK techniques are manually mapped to language structures that link system entities, attack techniques, and countermeasures, making it possible to reveal available countermeasures for each attack step and define missed ones.

In [15], authors focused on the problem of the probabilistic generation of the attack steps represented by the MITRE ATT & CK tactics. They use a hidden Markov model to represent transitions between tactics and techniques and try to calculate transition probabilities based on the analysis of the observable events. A set of observables is extracted from over 25 documents and other materials relating to the incidents in the industrial control systems. This analysis allowed the authors to determine the frequency of transitions between tactics and techniques and to transform them in initial probabilities, transition probabilities, and observable emission probabilities. The authors demonstrated that it is possible to generate different attack scenarios by changing the probabilities.

In [16–18] MITRE ATT & CK matrix serves as a basis for stating and validating hypotheses about attacks and their paths based on observations revealed by an analyst and historical data about attacks and threat actions. For example, in [16] the authors construct a graph of attack tactics and evaluate different algorithms for predicting missing graph edges and vertices to discover missed attack steps. The source data for constructing such an attack graph are data about attacks that are available through the MITRE ATT & CK STIX repository. Al-Shaer et al. investigated the problem of the similarity of different attack scenarios to reveal inter-dependencies between techniques and tactics. They demonstrated that certain fine-grained associations between techniques and tactics could be used to forecast an attacker's behavior [18].

A. Nisioti et al. propose DISCLOSE, a framework targeted to support the forensics investigation and evaluate the severity of the security breaches [17]. Similarly to [16], the authors use the MITRE ATT & CK STIX repository to construct a knowledge graph that reflects the probabilistic dependencies between attack techniques and could be used to reveal missed attack steps and forecast attack steps. Moreover, the authors suggest evaluating the cost and benefit of each attack action. The benefit of the attack actions is determined based on their properties, such as required privileges and user interaction, using the Common Vulnerability Scoring System Base Score Calculator. The cost of the attack actions is calculated based on expert assessments. Thus, the analyst may understand the impact of the possible attack actions using numerical scores and select appropriate countermeasures.

In [19], Kim et al. adopt the MITRE ATT & CK matrix to implement mobile advanced persistent threat attribution. They propose to form a vectorized presentation of tactics based on the results of their similarity analysis. The authors demonstrated that such a solution allows a reduction of the false positive rate in task of malware author's attribution.

The approach proposed in this paper is close to the approach suggested in [17]. But unlike the approach [17], the introduced approach performs security incident mapping to attack patterns in real-time mode and considers the step of the event correlation and construction of the security incidents and alerts.

Approach for security assessment based on attack graphs using NVD and MITRE ATT & CK database

Cyber attack incorporates several stages that are called kill chain. As soon as we consider enterprise networks, the stages are as follows: reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact. Some of them can be missed. Besides, to implement each stage several techniques can be used.

Detection of cyber attacks at the early stages of the kill chain allows for a reduced impact on the target system. In this paper, we propose an approach to security assessment based on attack graphs using NVD and MITRE ATT & CK database. The goal is to enhance the results of the security assessment via enhancement of the targeted attack detection. It can be specified as follows: $Res_{PA} \geq Res_{EA}$, where *Res* is defined as the number of the detected attack stages for the proposed approach (Res_{PA}) and existing approaches (Res_{EA}).

The proposed approach incorporates data gathering from various sources; log preprocessing; security incidents detection using correlation analysis; mapping the security incidents to the nodes of the attack graph constructed considering the kill chain using NVD and MITRE ATT & CK database; security assessment and forecasting based on the constructed graph; and results representation (Fig. 1). It takes as input the security incidents and outputs the risk scores for the resources of the analyzed system. The stages of the approach are detailed in the subsections below.

Data gathering and log preprocessing

First, in the data gathering stage, the raw data from the network log *net_log* and the internal log *syslog* (or other) are gathered. These data enter the preprocessing stage.

In the preprocessing stage, the raw data D_r are normalized, preprocessed, filtered, and aggregated (Fig. 2) using the following algorithm.

Step 1. The raw data D_r, i. e. the set of network and internal events, enter the normalization process *Norm*. D_r are converted to the normalized format in terms of length and syntax:

$$D_r \overset{read}{\rightarrow} Norm(len, syn),$$

where *len* — the fixed length; *syn* — the normalized event syntax.

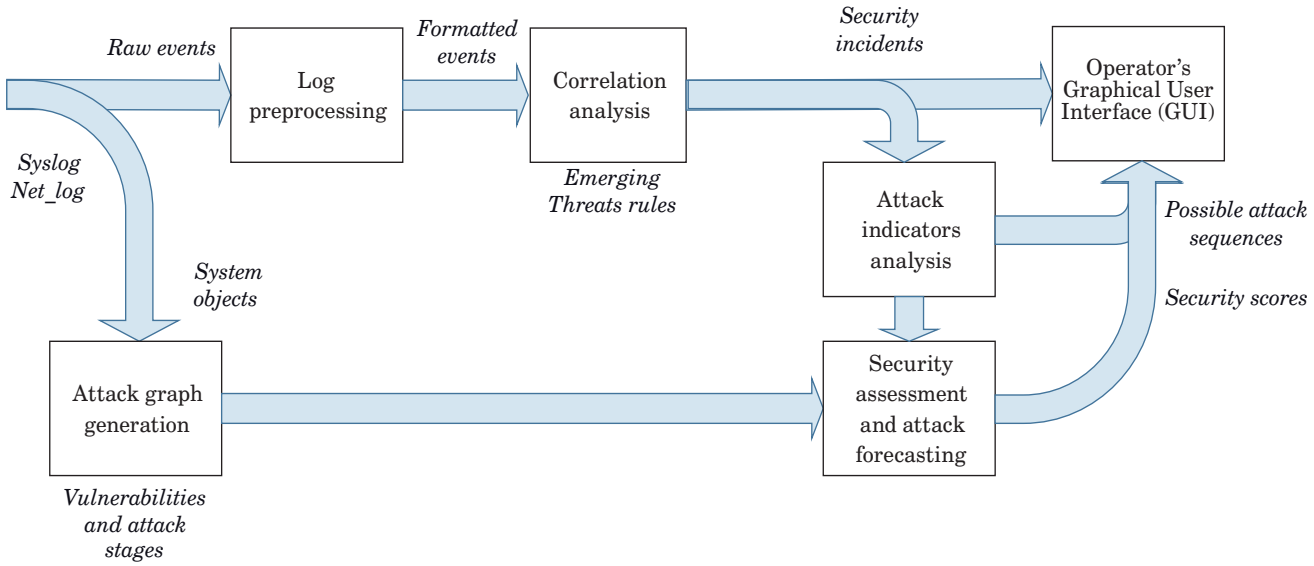
Step 2. The normalized events enter the preprocessing *Proc*. The events are supplemented by the fields essential for the correlation: *time_start*, *time_end*, *list*:

$$D_r \overset{read}{\rightarrow} Proc(time\_start, time\_end, list),$$

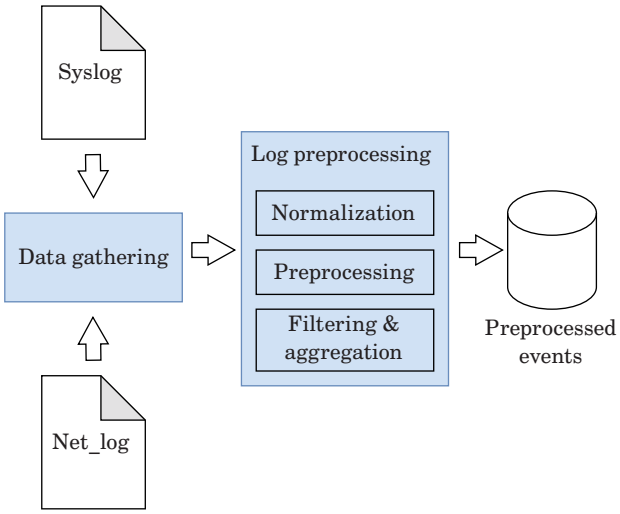
where *time_start* — event start time; *time_end* — event end time; *list* — event source.

Step 3. The preprocessed events enter the filtering and aggregation process *Filter*. It is required to remove the repeated events and aggregate similar events:

$$D_r \overset{read}{\rightarrow} Filter(del\_attr, meta),$$



■ ***Fig. 1.*** The generalized scheme of the proposed approach



■ ***Fig. 2.*** The scheme of the data gathering and log preprocessing process

where *del_atr* – a function for the removal of repeated events; *meta* – a function for aggregation of similar events.

Limitations:

$$\{C_1, C_2, ..., C_n\} \cup \{L_1, L_2, ..., L_k\} \in D,$$

where C – network events; L – internal events (events from operation system log); D – preprocessed events.

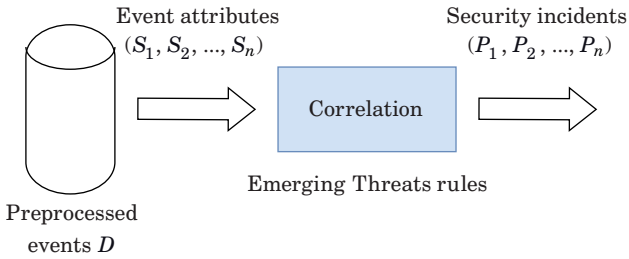
Security incident detection using correlation analysis

Correlation allows security incident detection. At this stage, the Emerging Threats correlation rules are used for events correlation (Fig. 3).

The authors specify the correlation rule as the following mathematical object:

$$< Rule\_type > [< TriG > (S_1, S_2, ..., S_n) \overset{impact}{\rightarrow} (P_1, P_2, ..., P_k) \overset{display}{\rightarrow} < Alert >, < Severity >],$$

where <*Rule_type*> – a type of the correlation rule that depends on the event source *list*. We outline the following types of correlation rules: *App-layer*, *Decoder*, *Dhcp*, *Dnp3*, *DNS*, *Files*, *http2*, *http*, *Ipsec*, *Kerberos*, *Modbus*, *Mqtt*, *Nfs*, *Smb*, *Tls*; <*TriG*> – the security incidents signatures, several signatures can exist for the same type of correlation rule; (S_1, S_2, ..., S_n) – event attributes indicating the security incidents; (P_1, P_2, ..., P_k) – detected security incidents; <*Alert*> – alert for the cyber security incident; <*Severity*> – severity of the alert (low, medium, or high).



■ ***Fig. 3.*** The scheme of security incident detection using log correlation analysis

This is the production model that uses IF-THEN rules to represent an operation. The preprocessed events D enter the correlation analysis (see Fig. 3). The event source *list* is used to select the correlation rule. The event attributes S trigger alert *Alert* if they correspond to one or several signatures *TriG* of the security incidents P. The severity of the alert depends on the number of security incidents. The algorithm for correlation can be specified as follows.

Step 1. Events D enter the correlation rule depending on their source *list*:

$$D \overset{read}{\rightarrow} Rule\_type.$$

Step 2. The events syntax represented by the event attributes S, is mapped to the features specified within the cyber security incident signature *TriG*:

$$D \overset{read}{\rightarrow} < Rule\_type >< TriG > (S_1, S_2, ..., S_n).$$

Step 3. If the events D contain at least one attribute corresponding to the feature specified in the cyber security incident signature, then the incident is detected:

$$D \overset{read}{\rightarrow} < Rule\_type >< TriG > (S_1, S_2, ..., S_n) \overset{impact}{\rightarrow} (P_1, P_2, ..., P_k).$$

Step 4. The alert *Alert* is generated and sent to the operator's GUI together with its severity:

$$D \overset{read}{\rightarrow} < Rule\_type > [< TriG > (S_1, S_2, ..., S_n) \overset{impact}{\rightarrow} (P_1, P_2, ..., P_k) \overset{display}{\rightarrow} < Alert >, < Severity >].$$

The obtained security incidents are passed to the attack indicators analysis stage.

Technique for mapping the security incidents to the nodes of the attack graph

At this stage, the security incidents obtained using events correlation are mapped to the cyber attack stages represented as an attack graph. The graph is generated considering the MITRE ATT & CK tactics and techniques, i. e. to the stages of the targeted cyber attacks.

The cyber attacks model represented as an attack graph, and a set of TAA (IOA) rules are used for this goal.

The attack graph is specified considering the analyzed system and cyber attack stages.

The analyzed system is specified based on its objects *Obj* and relations between them *Rel* as follows:

$$S = \{Obj, Rel\}.$$

Each object $obj \in Obj$ is specified as follows:

$$obj = \{ip\_addr, type, software, hardware\}.$$

Object type *type* is specified considering the submatrices of the Enterprise matrix of the MITRE ATT & CK (https://attack.mitre.org/matrices/enterprise/) as follows:

$$type \in \{PRE, Windows, macOS, Linux, Cloud, Network, Containers\}.$$

It is used to specify applicable attack stages and to determine the object's criticality.

Software *software* and hardware *hardware* are used to detect the object's vulnerabilities and generate attack subgraphs.

Rel specifies relations between objects.

The generalized attack graph *GAG* is specified as the set of attack subgraphs *ASG* and connections *Con* between them:

$$GAG = \{ASG, Con\}.$$

Each subgraph *ASG* is specified depending on the type *type* of the system object *Obj* under attack as the set of the attack stage nodes *stage*:

$$ASG = \bigcup_{i=1}^{n} stage_i,$$

where n — is the number of the attack stages that depend on *type*. For example, for the *type* = *Windows* (https://attack.mitre.org/matrices/enterprise/windows/), *ASG* = {*Initial Access*, *Execution*, *Persistence*, *Privilege Escalation*, *Defense*, *Evasion*, *Credential Access*, *Discovery*, *Lateral Movement*, *Collection*, *Command and Control*, *Exfiltration*, *Impact*}, while for the *type* = *PRE* (https://attack.mitre.org/matrices/enterprise/pre/), *ASG* = {*Reconnaissance*, *Resource*, *Development*}.

Each stage *stage* is specified as a stage attack subgraph considering *type*:

$$stage = \{N, Con, Pr\},$$

where N — the set of stage attack graph nodes; *Con* — the set of connections between them; *Pr* — probability of successful stage implementation.

Each node $n \in N$ represents an attack action. It is specified as follows:

$$n = \{V, Pr\},$$

where V — the set of vulnerabilities that can be used to implement the attack action; *Pr* — probability of successful attack action implementation.

The set of vulnerabilities is specified considering the *type* of the system *obj*, its *hardware*, and *software*. The vulnerabilities are related to attack *stages* if an appropriate connection exists in the MITRE ATT & CK database. Analysis of the MITRE ATT & CK databases demonstrated the low connectivity between this database and vulnerability databases (such as NVD). Thus, this research proposes using the technique for classification of the vulnerabilities by the MITRE ATT & CK stages using machine learning methods.

The TAA (IOA) rules describe security incidents (signatures) using Sigma language. The IOA allows mapping the security incidents to the attack stages from the MITRE ATT & CK database, for example, reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense, evasion, credential access, and discovery. The mapping is specified as follows:

$$< Sign > [< attack > (P_1, P_2, ..., P_n) \overset{display}{\rightarrow} < 0, 1 >, < R, MITRE_{obj} >],$$

where ⟨*Sign*⟩ — TAA (IOA) signatures of the security incidents; ⟨*attack*⟩ — attack techniques according to the MITRE ATT & CK. For example, it can take the following values: *Ddos_attack*, *Malv_attack*, *Scan_attack*, *Web_attack*, *Sql_attack*, *XSS_attack*, *Shell_attack*, *Dos_attack*, *Brut_attack*, *Pass_attack*, *Inject_attack*; (P_1, P_2, ..., P_n) — cyber security incidents corresponding to the attack technique; <0, 1> — the result of mapping of the security incidents (P_1, P_2, ..., P_n) to the MITRE ATT & CK techniques ⟨*attack*⟩ based on the signature ⟨*Sign*⟩: 0 — the set of the detected incidents (P_1, P_2, ..., P_n) do not correspond to the ⟨*Sign*⟩, 1 — the set of the detected incidents (P_1, P_2, ..., P_n) correspond to the ⟨*Sign*⟩; $MITRE_{obj}$ — attack description, its stage, possible

next steps, and attack responses according to the MITRE ATT & CK.

This process can be briefly described as follows. The signatures of the security incidents detected on the correlation stage are compared with the TAA (IOA) signatures of the same incidents. The targeted attack represented using MITRE ATT & CK techniques is detected if they match. Otherwise, the detected incident can't be mapped to the multi-step targeted attack represented with the path of the attack graph GAG. The attack responses depend on the attack stage and used tactics and techniques. Mapping the security incidents to the attack stages allows for assessing security, attack forecasting, and, in the future, selection of efficient attack responses.

The corresponding algorithm is as follows.

Step 1. Comparison of the signatures of the security incidents P_1, P_2, ..., P_n obtained from the D attributes using the Emerging Threats correlation rules with TAA (IOA) signatures. The TAA (IOA) signatures *Sign* of the incidents P_1, P_2, ..., P_n correspond to the tactics, techniques and procedures *attack* from the MITRE ATT & CK database. The comparison is specified as follows:

$$D(P_1, P_2, ..., P_k) \overset{compare}{\rightarrow}$$
$$< Sign >< attack > (P_1, P_2, ..., P_n).$$

Step 2. Displaying the $MITRE_{obj}$ if the signatures match:

$$D(P_1, P_2, ..., P_k) \overset{compare}{\rightarrow}$$
$$< Sign > [< attack > (P_1, P_2, \ ..., \ P_n) \overset{display}{\rightarrow}$$
$$< 1 > , \ < MITRE_{obj} >],$$

where 1 indicates that the set of the detected incidents P_1, P_2, ..., P_n correspond to the *Sign*. Go to Step 3. Otherwise, go to Step 4.

Step 3. Starting security assessment process.

Step 4. The security incident can not be mapped to the MITRE ATT & CK stages.

Security assessment

This research proposes a hierarchical security assessment process using a security risk score. A security risk score is calculated considering the probability of the security incident and the impact of the incident. It incorporates the following levels of hierarchy (from the lowest to the highest): 1) stage *stage* attack subgraph level — incorporates security risk scores for the *stage* attack subgraph nodes that are represented with attack actions n implemented using vulnerabilities; 2) *ASG* level — incorporates security risk scores for the *ASG* nodes that are represented with kill chain stages *stage*; 3) *GAG* level — incorporates security risk scores for the nodes of the *GAG* that are represented with *ASG*.

On the attack subgraph level, the approach described in [1] is used to calculate probabilities of successful attack actions *Pr*. The probability of attack is calculated using the equation for the unconditional probability:

$$\Pr(n_k) = \prod_{i=1}^{k} Pc(n_i \mid Pa[n_i]),$$

where n_k — the successful implementation of the k-th attack action represented using the attack graph node; *Pc* — local conditional probability distributions, i. e. the probability of compromise of a node considering the states of its parents; $Pa[n_k]$ — all parents of node n_k.

The graph traversal is used to calculate *Pr*.

Calculation of the unconditional probability requires the local conditional probability. To calculate local conditional probability distributions *Pc*, the approach proposed in [20] is used (the first equation for OR relations, the second equation — for AND relations):

$$Pc(n_k) = \begin{cases} 0 \text{ if } \forall n_i \in Pa[n_k] \mid n_i = \\ = 0 \text{ and } \left(1 - \prod_{i=1}^{k-1} (1 - Pc(n_i))\right) \text{ otherwise} \\ 0 \text{ if } \exists n_i \in Pa[n_k] \mid n_i = \\ = 0 \text{ and } \left(\prod_{i=1}^{k-1} (Pc(n_i))\right) \text{ otherwise} \end{cases},$$

where $n_i = 0$ means that attack action is not successful.

OR relations of the graph nodes (i. e. attack actions) represent the case when the successful implementation of the attack action requires the successful implementation of at least one of its parent nodes. AND relations of the graph nodes represent the case when the successful implementation of the attack action requires the successful implementation of all its parent nodes.

For the root node of the graph *Pc* is calculated using local probability $p(n)$ for this node:

$$Pc(n) = \begin{cases} p(n) & \text{for successful attack action} \\ 0 & \text{otherwise} \end{cases}.$$

The reverse depth-first traversal is used to calculate conditional probability distributions for all nodes.

The approach based on Common Vulnerability Scoring System metrics is used to calculate local

probabilities for the attack graph nodes and impact scores [1].

On the *ASG* level, the same approach is used but nodes are represented with kill chain stages *stage*. The local probabilities for the *stage* are calculated as probabilities *Pr* for the leaf nodes of the stage attack subgraph if it exists. If there is no stage attack subgraph for the *stage* (no corresponding vulnerabilities) then the local probability is calculated considering the complexity of the stage implementation according to the MITRE ATT & CK. Impact on this level is calculated as the maximum impact from the stage attack subgraph.

On the *GAG* level, the nodes are represented as *ASG*. Thus local probabilities are calculated as probabilities *Pr* for the leaf nodes of the *ASG*. Impacts are calculated considering the criticalities of the objects *Obj*.

In the case of security incidents, the probabilities for the nodes on all levels are recalculated considering Bayes' theorem.

Experiments

The authors implemented the proposed approach in Python programming language using the Flask framework (https://flask.palletsprojects.com/en/2.1.x/). Figure 4 provides the general architecture of the developed prototype.

The authors deployed the testing environment for the experiments. As the test case the small fragment of computer network was selected that can be the part of any supporting information technology infrastructure of power generation system. It is represented in Fig. 5. The developed prototype and the tested SIEM tools were installed on the Administrator's workstation.

The attacks were conducted against the user's workstation using internal tools of the Kali Linux operation system (https://www.kali.org/). The conducted attacks are provided in Table 1.

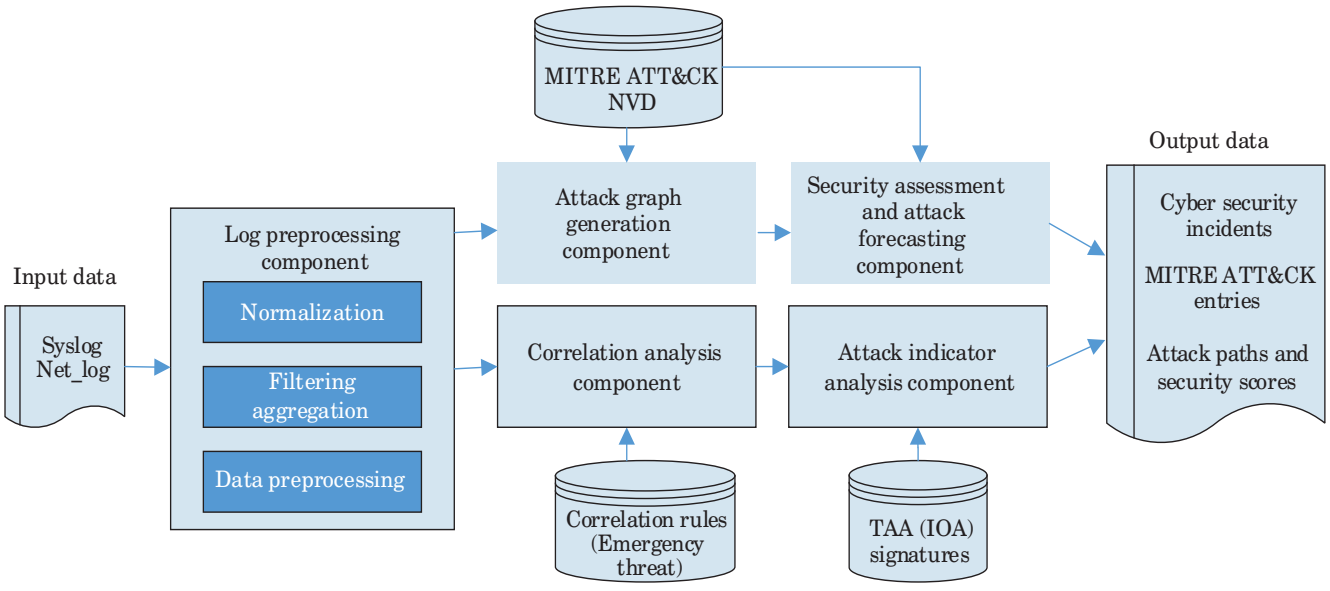
The Scan_attack is the first stage of the following attacks sequence (*TestSequence*): Reconnaissance (Scan_attack), Resource Development (Develop Capabilities), Initial Access (Exploit Public-Facing Application), Execution (Command and Scripting Interpreter), Persistence (Account Manipulation), Privilege Escalation (Scheduled Task), Defense Evasion (BITS Jobs), and Credential Access (Account Manipulation).

Table 2 contains the results of the experiments. It represents the following characteristics:

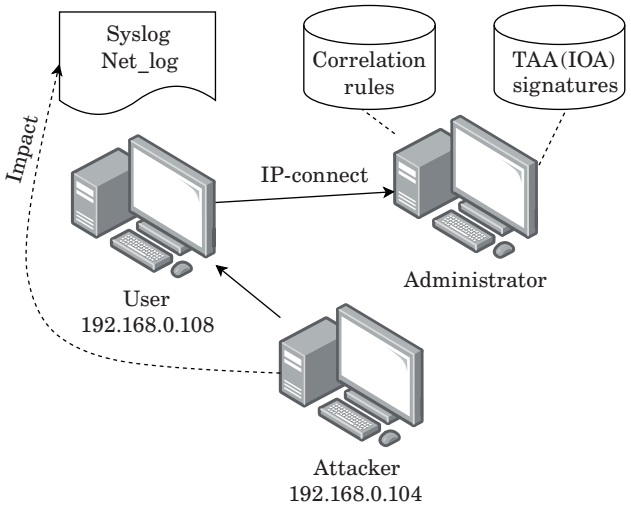
– the target IP-address;
– the conducted attacks;
– the types of events corresponding to the attacks (*C* – network events, *L* – operation system's log events);
– the TAA signatures corresponding to the attacks;
– the administrator IP-address;
– if the attack was detected and mapped.

Table 3 details the detected techniques for each attack according to the MITRE ATT & CK.

After detection and mapping of the attack to the attack sequence on the attack graph, the security risks are recalculated. Thus, the security risks for the TestSequence are provided in Fig. 6, where red color indicates high risk, yellow color – medium risk, and green color – low risk.



■ ***Fig. 4.*** General architecture of the developed prototype



■ ***Fig. 5.*** Deployed test environment

■ ***Table 1.*** The cyber attacks conducted within the test environment

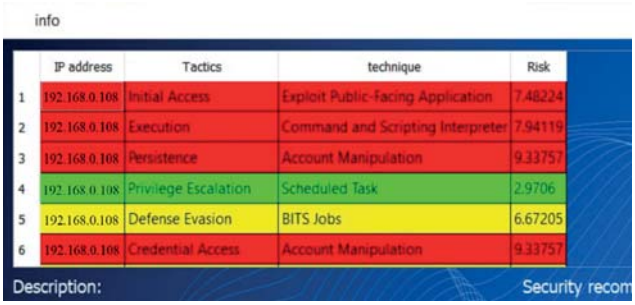
Attack	Source IP-address	Target IP-address	Success
Dos_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+
Shell_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+
Scan_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+
Inject_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+
Brut_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+

■ ***Table 2.*** Successfully detected and mapped attacks

Attack	Event type	TAA signature	User IP-address	Administrator IP-address
Dos_ impact	*C*	Dos_ attack	192.168.0.108 (User)	127.0.0.1
Shell_ impact	*L*	Shell_attack	192.168.0.108 (User)	127.0.0.1
Scan_ impact	*C*	Scan_attack	192.168.0.108 (User)	127.0.0.1
Inject_ impact	*L*	Inject_ attack	192.168.0.108 (User)	127.0.0.1
Brut_ impact	*C* & *L*	Brut_attack	192.168.0.108 (User)	127.0.0.1

■ ***Table 3.*** The detected techniques of the conducted cyber attacks

Attack	Techniques according to the MITRE ATT & CK
Dos_impact	T1499.001, T1499.002, T1499.003, T1499.004
Shell_impact	T1505.001, T1505.002, T1505.003
Scan_impact	T1595.001, T1595.002



■ ***Fig. 6.*** The security risks for the TestSequence

Discussion and conclusion

The authors analyzed the modern SIEM systems and found out that they do not provide the functionality of the accurate mapping of the detected incidents to the attack stage for further security assessment and attack prevention. To fill this gap, the authors proposed a new approach to the security assessment incorporating a comprehensive technique for correlating the raw events into the security incidents and mapping the incidents to the attacks and attack stages. The information on the detected and mapped security incidents is further used in the scope of the security assessment technique. In the research, the authors used open source tools. The Emerging Threats correlation rules were used for event correlation. Mapping of the security incidents to the attack stages was implemented using the TAA (IOA) integrated with the MITRE ATT & CK database. NVD and MITRE ATT & CK databases were used for attack model generation. The authors developed their models and algorithms based on production rules, graph theory, probability theory, and machine learning. The developed approach was implemented using Python language. The testing environment was deployed for the experiments. The experiments proved that the developed tool allows the detection of security incidents and mapping them to the attack stages.

Besides, the authors compared the proposed tool with existing open solutions, namely, Splunk Enterprise Security, IBM QRadar SIEM, and HP ArcSight Security Intelligence. The comparison re-

■ ***Table 4.*** Comparison of the developed tool with known SIEMs

Tool	Dos_attack	Scan_attack	Shell_attack
Attack detected			
Developed tool	+	+	+
Other tools	+	+	+
Attack mapped			
Developed tool	T1499.001[1] T1499.002[2] T1499.003[3] T1499.004[4]	T1595.001[5] T1595.002[6]	T1505.001[7] T1505.002[8] T1505.003[9]
Other tools	–	–	–

[1] https://attack.mitre.org/techniques/T1499/001/
[2] https://attack.mitre.org/techniques/T1499/002/
[3] https://attack.mitre.org/techniques/T1499/003/
[4] https://attack.mitre.org/techniques/T1499/004/
[5] https://attack.mitre.org/techniques/T1595/001/
[6] https://attack.mitre.org/techniques/T1595/002/
[7] https://attack.mitre.org/techniques/T1505/001/
[8] https://attack.mitre.org/techniques/T1505/002/
[9] https://attack.mitre.org/techniques/T1505/003/

sults are given in Table 4. Existing tools as well as the developed tool can detect all the conducted attacks. But unlike existing tools that are not able to map the detected attacks to the MITRE ATT & CK techniques and tactics, the developed tool is also able to detect techniques and tactics corresponding to the detected incident according to the MITRE ATT & CK. Thus, $Res_{PA} \geq Res_{EA}$, and the goal of the research is accomplished.

There are some limitations of the approach. Thus, the event correlation stage requires the correlation rules. We used the Emerging Threats correlation rules. If the rule for the security incident doesn't exist, the proposed solution won't detect the security incident. The same limitation exists for the incident mapping functionality. We implement mapping to the MITRE ATT & CK tactics and techniques using the TAA (IOA) rules. If the rule for the MITRE ATT & CK tactics or techniques doesn't exist, the proposed solution won't map the detected security incident to the attack sequence. Besides, there are some performance limitations. Thus, for the attack graph generation and probability calculation within the security assessment the resource consuming traversal algorithms are used. As soon as the attack graph is generated in the static mode before the system operation, this is not a drawback. To solve the probability calculation challenge in the real time mode we limit the number of the processed graph nodes.

Detection of the attack stage requires additional time and resources as well. However, automation of the cyber incident analysis will allow for saving the resources in future. Thus, this is essential for prevention of the targeted multi-step attacks. Their detection at an early stage, further assessment, and correct forecasting of the attack goal allow avoid the attack's success and impact from its successful implementation. The proposed solution can be implemented to protect heterogeneous infrastructures from cyber attacks.

In further research, the authors plan to enhance the proposed approach and corresponding tool in the following aspects:

— extending covered cyber attack scenarios using more complex correlation rules for the detection of cyber security incidents;

— considering attack scenarios that are not included to the MITRE ATT & CK database, such as generating targeted attacks using artificial neural networks;

— conducting other types of attacks to map other types of cyber security incidents to the MITRE ATT & CK tactics and techniques;

— adding the technique for the prospective countermeasures selection to the developed approach.

References

1. Kotenko I., Fedorchenko A., Doynikova E. *Data Analytics for Security Management of Complex Heterogeneous Systems: Event Correlation and Security Assessment Tasks*. In: *Advances in Cyber Security Analytics and Decision Systems*. Eds. S. K. Shandilya, N. Wagner, A. K. Nagar. Springer International Publishing, Cham, 2020, pp. 79–116. https://doi.org/10.1007/978-3-030-19353-9_5. 455
2. Doynikova E., Novikova E., Gaifulina D., Kotenko I. Towards attacker attribution for risk analysis. *Proc. of the 15th Intern. Conf. "Risks and Security of Internet and Systems CRiSIS 2020"*. Springer-Verlag, Berlin, Heidelberg, 2020, pp. 347–353. https://doi.org/10.1007/978-3-030-68887-5_22
3. Kovačević I., Groš S., Slovenec K. Systematic review and quantitative comparison of cyberattack scenario detection and projection. *Electronics*, 2020, vol. 9, no. 10, pp. 1722.
4. Pavlov A., Voloshina N. Analysis of IDS alert correlation techniques for attacker group recognition in distributed systems. *Proc. of the 20th Intern. Conf. "Internet of Things, Smart Spaces and Next Generation Networks and Systems NEW2AN 2020", and 13th Conf. ruSMART 2020*. Springer-Verlag, Berlin, Heidelberg, 2020, pp. 32–42. https://doi.org/10.1007/978-3-030-65726-0_4

5. Bajtoš T., Sokol P., Mézešová M. *Multi-stage Cyber-attacks Detection in the Industrial Control Systems*. In: *Recent Developments on Industrial Control Systems Resilience*. Eds. E. Pricop, J. Fattahi, N. Dutta, M. Ibrahim. Springer, 2020, pp. 151–173.

6. Stroeh K., Mauro Madeira E. R., Goldenstein S. K. An approach to the correlation of security events based on machine learning techniques. *Journal of Internet Services and Application*s, 2013, vol. 4, no. 7. https://doi.org/10.1186/1869-0238-4-7

7. Khosravi M., Ladani B. T. Alerts correlation and causal analysis for APT based cyber attack detection. *IEEE Access*, 2020, vol. 8, pp. 162642–162656. doi:10.1109/ACCESS.2020.3021499

8. Kotenko I., Gaifulina D., Zelichenok I. Systematic literature review of security event correlation methods. *IEEE Access*, 2022, no. 10, pp. 43387–43420. https://doi.org/10.1109/ACCESS.2022.3168976

9. Kryukov R., Zima V., Fedorchenko E., Novikova E., Kotenko I. Mapping the security events to the MITRE ATT&CK attack patterns to forecast attack propagation (extended abstract). *Proc. of the 5th Intern. Workshop "Attacks and Defenses for the Internet-of-Things ADIoT 2022"*. Springer Nature Switzerland, Cham, 2022, pp. 165–176.

10. Gao P., Shao F., Liu X., Xiao X., Qin Z., Xu F., Mittal P., Kulkarni S. R., Song D. Enabling efficient cyber threat hunting with cyber threat intelligence. *Proc. of the 2021 IEEE 37th Intern. Conf. on Data Engineering (ICDE)*. IEEE Computer Society, 2021, pp. 193–204. https://doi.org/10.1109/ICDE51399.2021.00024

11. Kurniawan K., Ekelhart A., Kiesling E., Quirchmayr G., Tjoa A. M. KRYSTAL: Knowledge graph-based framework for tactical attack discovery in audit data. *Computers & Security*, 2022, vol. 121, pp. 102828. https://doi.org/10.1016/j.cose.2022.102828

12. Sadlek L., Čeleda P., Tovarňák D. Identification of attack paths using kill chain and attack graphs. *Proc. of the NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symp*. IEEE, 2022, pp. 1–6. https://doi.org/10.1109/NOMS54207.2022.9789803

13. Xiong W., Legrand E., Åberg O., Lagerström R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, 2022, vol. 21, pp. 157–177. https://doi.org/10.1007/s10270-021-00898-7

14. Ajmal A. B., Shah M. A., Maple C., Asghar M. N., Islam S. U. Offensive security: Towards proactive threat hunting via adversary emulation. *IEEE Access*, 2021, no. 9, pp. 126023–126033. https://doi.org/10.1109/ACCESS.2021.3104260

15. Choi S., Yun J. H., Min B. G. Probabilistic attack sequence generation and execution based on MITRE ATT&CK for ICS datasets. *Proc. of the Cyber Security Experimentation and Test Workshop CSET'21*. New York, USA, 2021, pp. 41–48. https://doi.org/10.1145/3474718.3474722

16. Elitzur A., Puzis, R., Zilberman P. Attack hypothesis generation. *Proc. of the 2019 European Intelligence and Security Informatics Conf. (EISIC 2019)*. Institute of Electrical and Electronics Engineers, 2019, pp. 40–47. https://doi.org/10.1109/EISIC49498.2019.9108886

17. Nisioti A., Loukas G., Laszka A., Panaousis E. Data-driven decision support for optimizing cyber forensic investigations. *IEEE Transactions on Information Forensics and Security*, 2021, vol. 16, pp. 2397–2412. https://doi.org/10.1109/TIFS.2021.3054966

18. Al-Shaer R., Spring J. M., Christou E. Learning the associations of MITRE ATT&CK adversarial techniques. *Proc. of the 2020 IEEE Conf. on Communications and Network Security (CNS)*, 2020, pp. 1–9. https://doi.org/10.1109/CNS48642.2020.9162207

19. Kim K., Shin Y., Lee J., Lee K. Automatically attributing mobile threat actors by vectorized ATT&CK Matrix and paired indicator. *Sensors*, 2021, vol. 21, iss. 19. https://doi.org/10.3390/s21196522

20. Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 2012, vol. 9, iss. 1, pp. 61–74. https://doi.org/10.1109/TDSC.2011.34

УДК 004.056
doi:10.31799/1684-8853-2024-2-39-50
EDN: YXVAJI

Оценивание защищенности гетерогенных инфраструктур на основе графов атак с использованием баз данных NVD и MITRE ATT & CK

Р. О. Крюков[а], канд. техн. наук, преподаватель, orcid.org/0009-0008-3422-7234
Е. В. Федорченко[б], канд. техн. наук, старший научный сотрудник, orcid.org/0000-0001-6707-9153
И. В. Котенко[б], доктор техн. наук, профессор, orcid.org/0000-0001-6859-7120, ivkote@comsec.spb.ru
Е. С. Новикова[б], канд. техн. наук, доцент, orcid.org/0000-0003-2923-4954
В. М. Зима[а], канд. техн. наук, профессор, orcid.org/0009-0006-9412-4160
[а]Военно-космическая академия им. А. Ф. Можайского, Ждановская наб., 13, Санкт-Петербург, 197198, РФ
[б]Санкт-Петербургский Федеральный исследовательский центр РАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ

Введение: оценивание защищенности современных информационных систем является нетривиальной задачей. Такие системы объединяют различные объекты, «вещи», субъекты и связи между ними, при этом они постоянно меняются и генерируют большое количество событий. В результате постоянно меняется состояние защищенности системы. **Цель:** разработать подход к оценке защищенности гетерогенных информационных систем. **Результаты:** разработан подход к оцениванию защищенности, который включает сбор данных из различных открытых источников, предобработку журналов событий, обнаружение инцидентов безопасности, отображение инцидентов безопасности на узлы графа атак, оценивание и прогнозирование уровня защищенности и представление результатов. Новизна предложенного подхода заключается в разработанной методике отображения инцидентов на этапы целевых кибератак. Эта методика использует правила корреляции Emerging Threats для обнаружения инцидентов безопасности. Для отображения обнаруженных инцидентов безопасности на шаблоны атак из базы данных MITRE ATT & CK методика использует правила Targeted Attack Analyzer (Indicators of Attack), которые описывают инциденты безопасности (сигнатуры) с использованием языка Sigma. Методика позволяет отобразить обнаруженные события на граф атак и оценить и спрогнозировать целевые кибератаки. Для генерации графа атак предлагается использовать шаблоны атак из MITRE ATT & CK и уязвимости из National Vulnerability Database (Национальной базы данных уязвимостей). Предложенный подход реализован в рамках программного средства, написанного на языке Python. Для тестирования отображения обнаруженных инцидентов безопасности на известные шаблоны атак развернута тестовая среда. **Практическая значимость:** результаты исследования могут быть использованы при построении систем оценивания защищенности, которые направлены на повышение защищенности гетерогенных информационных систем от кибератак.

Ключевые слова — оценивание защищенности, инциденты кибербезопасности, корреляция событий, сигнатура, кибератака, граф атак, MITRE ATT & CK, National Vulnerability Database, анализатор целевых атак, индикаторы атаки, киберугроза.

Для цитирования: Kryukov R. O., Fedorchenko E. V., Kotenko I. V., Novikova E. S., Zima V. M. Security assessment based on attack graphs using NVD and MITRE ATT & CK database for heterogeneous infrastructures. *Информационно-управляющие системы*, 2024, № 2, с. 39–50. doi:10.31799/1684-8853-2024-2-39-50, EDN: YXVAJI

For citation: Kryukov R. O., Fedorchenko E. V., Kotenko I. V., Novikova E. S., Zima V. M. Security assessment based on attack graphs using NVD and MITRE ATT & CK database for heterogeneous infrastructures. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 39–50. doi:10.31799/1684-8853-2024-2-39-50, EDN: YXVAJI