

Generalized Net Model of an Automated System for Monitoring, Analysing and Managing Events Related to Information Security

Ivelina Vardeva 

Assen Zlatarov University, Burgas, Bulgaria, <http://btu.bg>

ABSTRACT:

With the increase of information flows transmitted between different information systems, organizations using these systems are increasingly dependent on ensuring the continuity and accuracy of ongoing processes in these systems. It is necessary to have tools for analyzing the large number of real-time events in order to respond adequately to security threats emerging in information systems. The field of application of SIEM systems is primarily for detecting and preventing network intrusion, but it can also be used to analyze traffic whether it is useful or malicious.

ARTICLE INFO:

RECEIVED: 02 JUL 2019

REVISED: 08 SEP 2019

ONLINE: 22 SEP 2019

KEYWORDS:

security information and event management, information security, security tools, security services



Creative Commons BY-NC 4.0

Introduction

Every day cyber attackers break into networks disguising as employees and delete their tracks as they go. With time against you and with inadequate tools it can take an average of eight months to filter through such massive volumes of data in order to detect and contain the attack. The IBM QRadar Security Intelligence Platform is designed to automatically identify and analyse threads earlier in the attack cycle providing the necessary time to respond.

Methods

Is computer security a problem? Today we are completely dependent on computer networks and information. Business, industry, utilities, and strategic sites bind their processes to computer networks and the Internet. Technology alone cannot solve the problem; they are the only tool we manage.

People creating technology and managing information systems and computer networks are not mature, human errors create prerequisites for security breaches. The use of security information and event management (SIEM) systems increases the level of information security in already existing architectures that provide the ability to manipulate the flow of information and manage incidents and events in real-life mode of these systems. In order to manage real-time security incidents, it is necessary to make a decision before the situation becomes critical. To perform such control and analysis, automated forecasting mechanisms are used based on the accumulated data for the normal operating state of these systems.

The automation of real-time decision making is based on mechanisms that determine the state of information security. To enable security analysts to perform investigations, SIEM correlates information such as these examples: Point in time, Offending users, Origins, Targets, Vulnerabilities, Asset information, Known threats.²⁻⁴

Overview of key SIEM capabilities

The key SIEM capabilities include:

- Ability to process security-relevant data from a wide variety of sources, such as:
 - Firewalls
 - User directories
 - Proxies
 - Applications
 - Routers;
- Collection, normalization, correlation, and secure storage of raw events, vulnerabilities, network flows, assets, and threat intelligence data;
- Layer 7 payload capture up to a configurable number of bytes from un-encrypted traffic;
- Comprehensive search capabilities;
- Monitor network and host behaviour changes that could indicate an attack or policy breach such as these examples;
- Off hours or excessive usage of an application or network activity patterns inconsistent with historical user profiles;
- Prioritization of suspected attacks and policy breaches;
- Notification by email, SNMP, and others;

- Provision of a variety of generic reporting templates.

Based on these key capabilities of SIEM, intelligent automated security solutions are taken. They also include automation, dashboard, visualizations, workflows, reporting capabilities.

Security intelligence platforms incorporate:

- use cases – advanced threat detection, insider threat detection, risk and vulnerability management, critical data and GDPR, incident response, cloud security, compliance;
- analytics engine – security analytics, real time detection and user driven analytics (machine learning, powerful search, behavioural analytics, artificial intelligence, threat hunting);
- unlimited logging – data store (endpoint network, applications identity vulnerabilities, configuration assets 3th party data stores);
- deployment model, that can be on the premise, as a service, cloud, or hybrid.

All SIEM tools are an important part of the data security: they aggregate data from multiple systems (described above) and analyse that data to catch abnormal/unconventional behaviour or potential cyberattacks. What the SIEM processes involve is shown in Figure 1.

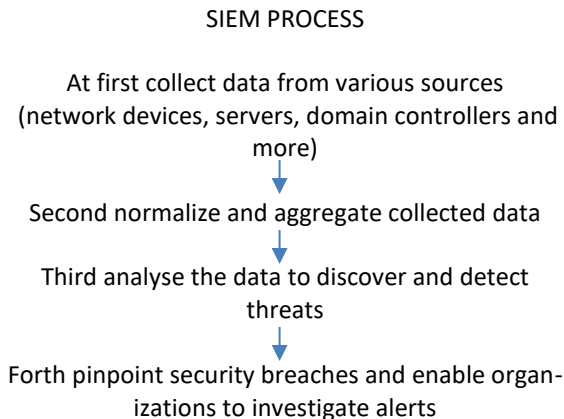


Figure 1: Four step describe SIEM processes.

One such SIEM tool is QRadar, facilitating the response to the following key questions:

- What is being attacked?
- What is the security impact?
- Who is attacking?
- Where should the investigation be focused?

- When are the attacks taking place?
- How is the attack penetrating the system?
- Is the suspected attack or policy breach real or a false alarm?

To enable security analysts to perform investigations, QRadar SIEM correlates information such as: point in time, offending users, origins, target, vulnerabilities, asset information, known threats.

How QRadar works

Having received traffic flows, QRadar builds traffic patterns and stores them for future analysis performed by a security administrator. The administrator has to configure behavioural rules which are determined by the security policy of a company to monitor data exchange between network devices. Behavioural rules are a subtype of anomaly detection rules, which compare the real traffic against the baseline to detect volume changes in regular traffic patterns.⁵

Generalized net model

The generalized net model presented on Figure 2 describes the parallel operation of the QRadar application tool.¹ IBM Security QRadar Risk Manager is a separately installed appliance for monitoring device configurations, simulating changes to your network environment, and prioritizing risks and vulnerabilities in your network. IBM Security QRadar Risk Manager uses data that is collected by configuration data from network and security device, such as firewalls, routers, switches, or IPSs, vulnerability feeds, and vendor security sources. This data is used to identify security, policy, and compliance risks within your network security infrastructure and the probability of those risks that are being exploited.²⁻⁴

QRadar SIEM correlates information such as: Point in time, Offending users, Origins, Targets, Vulnerabilities, Asset information, Known threats.

Initially the following tokens enter the generalized net with the respective information characteristics:

In places $l_{11} \dots l_{1n}$, tokens enter with a characteristic “new data about security, network activity, application activity, system monitoring, and compliance”;

In places $l_{21} \dots l_{2n}$, tokens enter with a characteristic “new offences”;

In places $l_{31} \dots l_{3n}$, tokens enter with a characteristic “new events log”;

In places $l_{41} \dots l_{4n}$, tokens enter with a characteristic “network flows sent in real-time”;

In places $l_{51} \dots l_{5n}$, tokens enter with a characteristic “new asset”;

A generalized net model is developed with an introduced set of transitions A:

$$A = \{Z_1, \dots, Z_n, Z_r, Z_g\},$$

where the transitions describe the following processes, respectively:

Z_1, \dots, Z_n – processes related to collecting five default dashboards that are focused on security, network activity, application activity, system monitoring, and

compliance; determining magnitude rating of an offence is calculated based on relevance, severity and credibility; monitoring and investigate events in real time; collecting network activity; assets information;

Z_r – processes related to Security Analytics (including Data correlation, Pattern identification, Thresholds, Policies, Anomaly detection, Prioritization), Security Analysts (Manage alerts, Research security events and anomalies, Evaluate user activity and vulnerabilities, Configuration, Other) of Z_1 to Z_n . At each transition of the transition cores of Z_1 , to Z_n , a number of actions are performed depending on the tool configuration;

Z_g – processes related to analysing the attack and spreading to all participants for the particular attack.

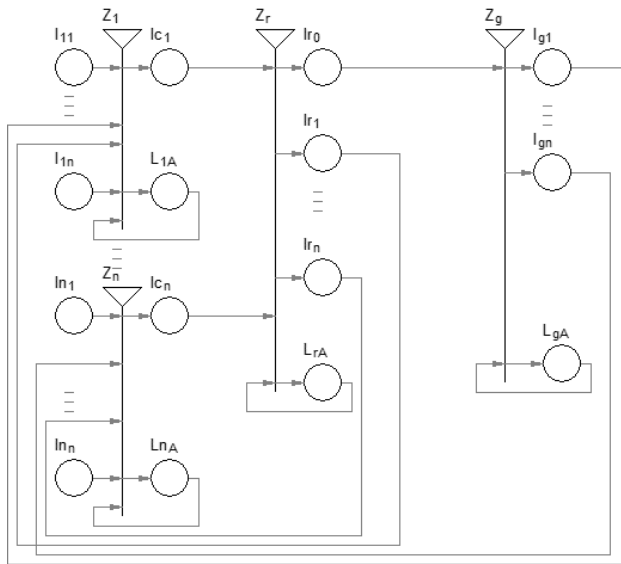


Figure 2: GN model of base QRadar application tool.

The $Z_1 = \{I_{11}, \dots, I_{1n}, L_{1A}\}, \{I_{c1}, L_{1A}\}, R_1, \wedge (I_1, L_{1A})$ index matrix of the transition conditions is:

	I_{c1}	L_{1A}
I_{11}	false	true
I_{r1}	false	true
$R_1 = I_g$	false	true
...		
I_{1n}	false	true
L_{1A}	$W_{1A,c1}$	true

where:

$W_{l_{A,c1}} = \dots = W_{n_{A,cn}} =$ “are available analysis activities.”

The token entering place l_{c1} obtains new characteristics “send data to Security Analytics and Security Analysts.”

where: $Z_i, 1 \leq i \leq n$

The $Z_r = \{l_{c1}, \dots, l_{cn}, L_{1A}\}, \{l_{r0}, l_{r1}, \dots, l_{rn}, L_{1A}\}, R_r, \wedge (l_{c1}, \dots, l_{cn}, L_{1A})$ index matrix of the transition conditions is:

$$R_r = \begin{array}{c|ccccc} & l_{r0} & l_{r1} & \dots & l_{rn} & L_{rA} \\ \hline l_{c1} & false & false & \dots & false & true \\ l_{cn} & false & false & \dots & false & true \\ L_{rA} & W_{rA,r0} & W_{rA,r1} & \dots & W_{rA,rn} & true \end{array}$$

where:

$W_{rA,r0} =$ “an attack has been detected”;

$W_{rA,r1} = \dots = W_{rA,rn} =$ “synced data between the applications used.”

The token entering place l_{p0} obtains new characteristics “an attack has been committed”;

The tokens entering place l_{p1}, \dots, l_{pn} obtains new characteristics “synchronization data has been sent.”

The $Z_g = \{l_{r0}, L_{gA}\}, \{l_{r0}, l_{r1}, \dots, l_{rn}, L_{1A}\}, R_g, \wedge (l_{r0}, L_{gA})$ index matrix of the transition conditions is:

$$R_g = \begin{array}{c|cccc} & l_{g1} & \dots & l_{gn} & L_{gA} \\ \hline l_{r0} & false & \dots & false & true \\ L_{gA} & W_{gA,g1} & \dots & W_{gA,gn} & true \end{array}$$

where:

$W_{gA,g1} = \dots = W_{gA,gn} =$ “new data on attacks.”

The tokens entering place l_{g1}, \dots, l_{gn} obtains new characteristics “update data has been sent.”

Conclusions

The present model can be elaborated with a more detailed looks into different directions. As it was noted above, QRadar uses rules to monitor the events and flows in your network to detect security threats. When the events and flows meet the test criteria that is defined in the rules, an offense is created to show that a security attack or policy breach is suspected. But knowing that an offense occurred is only the first step; identifying how it happened, where it happened,

and who did it requires some investigation. The Offense Summary helps you begin your offense investigation by providing context to help you understand what happened and determine how to isolate and resolve the problem.


Using advanced analytics and machine learning it automatically analyses log and flow data across multiple environments to detect suspicious events in real time. It then correlates them against vulnerability data and threat intelligence to generate prioritized alerts based on impact and severity. Once a threat is detected QRadar can uniquely connect the entire chains of events for you. And together with QRadar advisor with Watson automatically start investigation to determine the root cause and scope of the attack. With pre-packaged rules more than 500 out of the box integrations and easily downloadable apps you can gain deeper visibility into user behaviour endpoint activity, network traffic and more all from one platform and managed from a single pane of glass now time is back on your side for attackers before they complete their mission.

References

- ¹ Krassimir Atanassov, *Generalized Nets* (Singapore, New Jersey, London, World Scientific, 1991).
- ² IBM Security, "Frequently asked How-To questions – IBM QRadar Network Security," IBM, December 7, 2017.
- ³ IBM Security, "QRadar Version 7.3.1 User guide," IBM, 2017.
- ⁴ IBM Security, "QRadar Version 7.3.1 Administration Guide," IBM, 2017.
- ⁵ Serguei Tchesnokov, "Traffic Pattern Analysis Inside Out," *ScienceSoft*, 2017.

About the Author

Dr. Ivelina Vardeva is Associate Professor and Head of the Department of Computer Systems and Technologies at the "Prof. Dr. Assen Zlatarov" University, Burgas, Bulgaria. Her current research is focused on intelligent control systems and the application of intuitionistic fuzzy sets.

 <https://orcid.org/0000-0001-5421-4758>