

# VNCS WEB MONITORING

## Centralized monitoring website solution

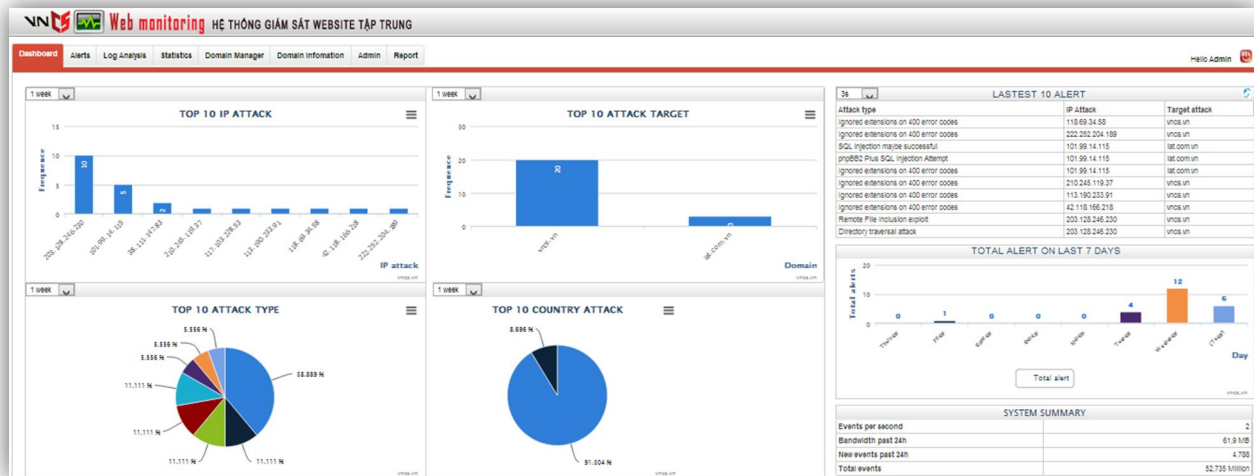
Almost of the cyber attacks againsts the websites of organizations. Especially, recently, there are many attacks on the websites of government agencies, business organizations of Vietnam.

However, on the world and Vietnam market have no centralized solution focus support monitoring multiple websites (Although there were solutions of HP, IBM... to monitor server, network with a very high cost).

So, Viet Nam Cyberspace Security Technology (VNCS), a member of Hanoi Telecom Corporation developed centralized monitoring website solution (VNCS Web Monitoring), one of the very first kind of security software in Vietnam, which is able to monitor simultaneously multiple websites while preventing attacks and displaying alerts in real time.

VNCS Web Monitoring is one of the security solutions for organizations and enterprises to manage and protect multiple websites at the same time, such as: IT center of state agencies, Datacenter, Hosting service providers, financial institutions...

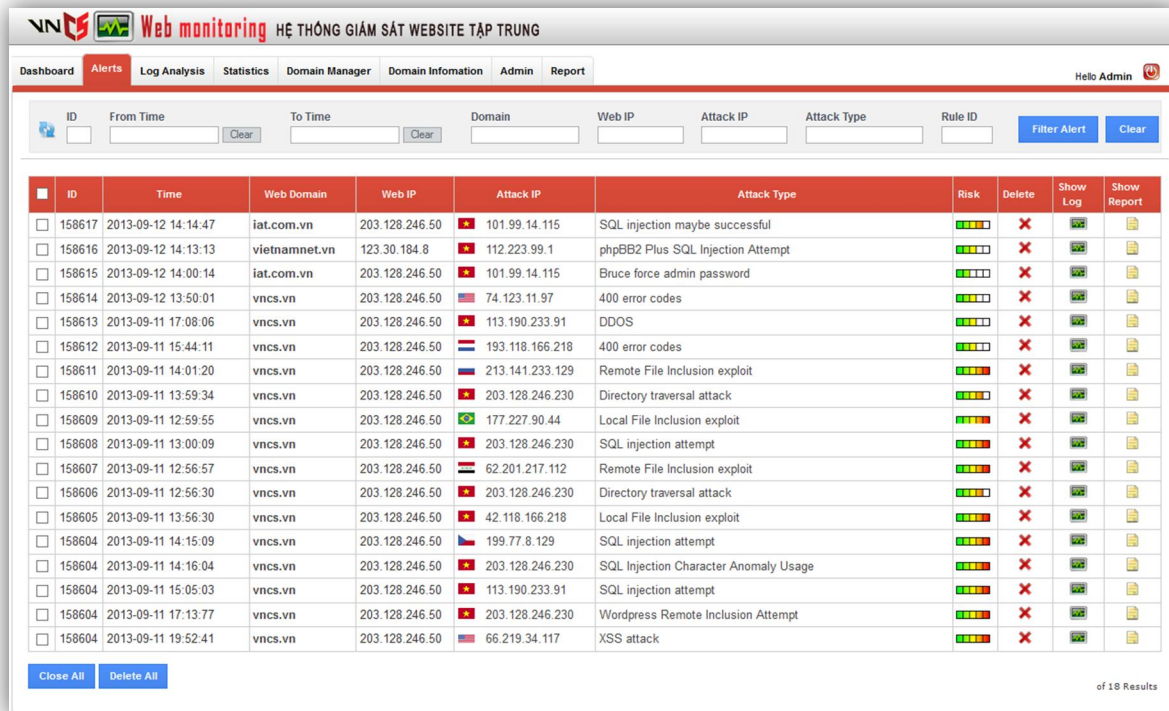
VNCS Web Monitoring focused on monitoring web logs, analyzing automatically to detect attacks and send alert via SMS and email using innovative algorithms and technologies such as advanced IP-recognition technology, structural changes identified website ... The solution also provides customized tools to assist administrators to manually analyze the attacks.



With the experience learned from the research and work with well-known security company in the world, we have updated the new technology to put into this product. In addition, with research &

development teams operate independently, we also applied a number of proprietary technologies in the field of information security and can improve the product to suit the security demand in Vietnam.

VNCS Web Monitoring also provides tools for manually analyze attacks. With the help of this system, the administrator can shorten web log analysis process, which takes a lot of time and effort, thus, can act quickly when system problems occur.



The screenshot displays the 'Web monitoring' interface with the title 'HỆ THỐNG GIÁM SÁT WEBSITE TẬP TRUNG'. The interface includes a navigation menu with 'Dashboard', 'Alerts', 'Log Analysis', 'Statistics', 'Domain Manager', 'Domain Information', 'Admin', and 'Report'. The user is logged in as 'Hello Admin'. Below the navigation is a search and filter section with fields for 'From Time', 'To Time', 'Domain', 'Web IP', 'Attack IP', 'Attack Type', and 'Rule ID', along with 'Filter Alert' and 'Clear' buttons. The main area contains a table of attack logs with the following columns: ID, Time, Web Domain, Web IP, Attack IP, Attack Type, Risk, Delete, Show Log, and Show Report. The table lists 18 attack events, including SQL injection attempts, DDOS, and directory traversal attacks. At the bottom, there are 'Close All' and 'Delete All' buttons, and a status indicator 'of 18 Results'.

ID	Time	Web Domain	Web IP	Attack IP	Attack Type	Risk	Delete	Show Log	Show Report
158617	2013-09-12 14:14:47	iat.com.vn	203.128.246.50	101.99.14.115	SQL injection maybe successful	High	X	Log	Report
158616	2013-09-12 14:13:13	vietnamnet.vn	123.30.184.8	112.223.99.1	phpBB2 Plus SQL Injection Attempt	High	X	Log	Report
158615	2013-09-12 14:00:14	iat.com.vn	203.128.246.50	101.99.14.115	Bruce force admin password	High	X	Log	Report
158614	2013-09-12 13:50:01	vnics.vn	203.128.246.50	74.123.11.97	400 error codes	High	X	Log	Report
158613	2013-09-11 17:08:06	vnics.vn	203.128.246.50	113.190.233.91	DDOS	High	X	Log	Report
158612	2013-09-11 15:44:11	vnics.vn	203.128.246.50	193.118.166.218	400 error codes	High	X	Log	Report
158611	2013-09-11 14:01:20	vnics.vn	203.128.246.50	213.141.233.129	Remote File Inclusion exploit	High	X	Log	Report
158610	2013-09-11 13:59:34	vnics.vn	203.128.246.50	203.128.246.230	Directory traversal attack	High	X	Log	Report
158609	2013-09-11 12:59:55	vnics.vn	203.128.246.50	177.227.90.44	Local File Inclusion exploit	High	X	Log	Report
158608	2013-09-11 13:00:09	vnics.vn	203.128.246.50	203.128.246.230	SQL injection attempt	High	X	Log	Report
158607	2013-09-11 12:56:57	vnics.vn	203.128.246.50	62.201.217.112	Remote File Inclusion exploit	High	X	Log	Report
158606	2013-09-11 12:56:30	vnics.vn	203.128.246.50	203.128.246.230	Directory traversal attack	High	X	Log	Report
158605	2013-09-11 13:56:30	vnics.vn	203.128.246.50	42.118.166.218	Local File Inclusion exploit	High	X	Log	Report
158604	2013-09-11 14:15:09	vnics.vn	203.128.246.50	199.77.8.129	SQL injection attempt	High	X	Log	Report
158604	2013-09-11 14:16:04	vnics.vn	203.128.246.50	203.128.246.230	SQL Injection Character Anomaly Usage	High	X	Log	Report
158604	2013-09-11 15:05:03	vnics.vn	203.128.246.50	113.190.233.91	SQL injection attempt	High	X	Log	Report
158604	2013-09-11 17:13:77	vnics.vn	203.128.246.50	203.128.246.230	Wordpress Remote Inclusion Attempt	High	X	Log	Report
158604	2013-09-11 19:52:41	vnics.vn	203.128.246.50	66.219.34.117	XSS attack	High	X	Log	Report

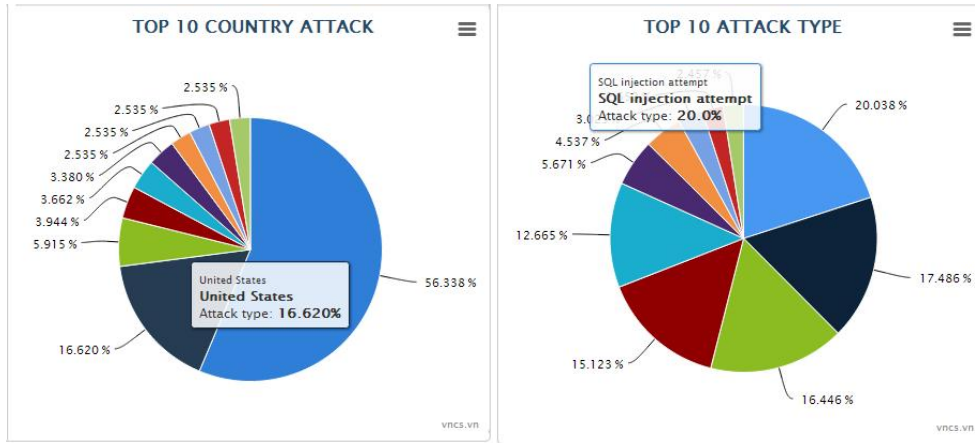
## Manage centralized log monitoring with user-friendly interface

Web VNCS monitoring system monitor and supervise events happening on all websites. It meets actual demands of administrators: manage system on one homogeneous web interface. On this interface, Administrator can easily manage, add or remove Websites. It can help Administrator shorten the time of the log analysis.

## Automatic analysis and real-time alerts

The solution is updated pattern identification of latest attacks. VNCS also have a dedicate team for research and development Web VNCS monitoring. By the intelligent and creative algorithms, website monitoring system can automatically analyze the situation attack and sends instant alerts (Email, SMS) to the administrator when detecting attacks on websites. This solution helps the administrator does not

need to intervene in the system log that still receive reports attack. The new attacks are being early researched and updated. Therefore, the system can accurately detect and timely new attack.



Support manually analyze incidents for administrators

**Web monitoring** HỆ THỐNG GIÁM SÁT WEBSITE TẬP TRUNG

Dashboard Alerts **Log Analysis** Statistics Domain Manager Domain Information Admin Report Hello Admin

Domain (\* Required):  Time: From  To  Attack IP:  Method:  POST URI:  Reference:  Status:  Len:  User-agent:

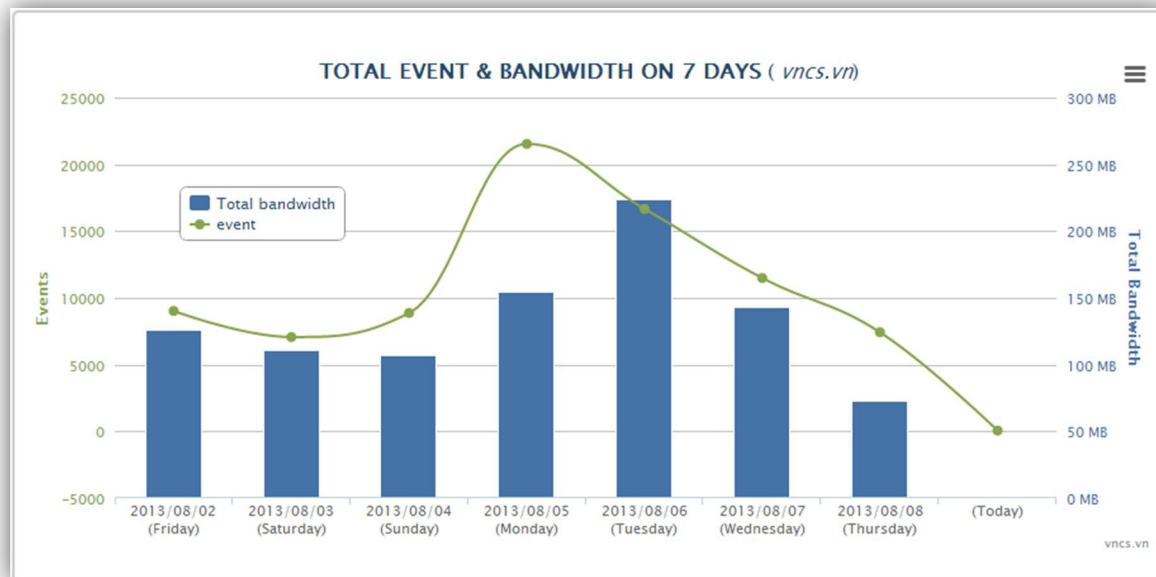
ID	Time	Website Domain	Attack IP	Method	URI	Status	Len
921176	2013-09-12 22:06:51	vncs.vn	91.200.14.59	POST	/index.php	200	7300
921175	2013-09-12 22:06:51	vncs.vn	91.200.14.59	POST	/index.php	200	7300
903187	2013-09-09 12:23:29	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_content&layout=edit&id=149	303	0
903186	2013-09-09 12:23:29	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_content&layout=edit&id=149	303	0
903085	2013-09-09 12:21:04	vncs.vn	171.251.7.154	POST	/administrator/index.php?j3action=clearCache&j3type=plugin	200	20
903084	2013-09-09 12:21:04	vncs.vn	171.251.7.154	POST	/administrator/index.php?j3action=clearCache&j3type=plugin	200	20
903081	2013-09-09 12:20:54	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_menus&layout=edit&id=0	303	0
903080	2013-09-09 12:20:54	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_menus&layout=edit&id=0	303	0
903079	2013-09-09 12:20:37	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_content&view=articles&layout=modal&tmpl=component&function=jQuerySelectArticle_iform_request_id&cc8e2dce8506146376c413db3e334388=1	200	3043
903078	2013-09-09 12:20:37	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_content&view=articles&layout=modal&tmpl=component&function=jQuerySelectArticle_iform_request_id&cc8e2dce8506146376c413db3e334388=1	200	3043
903077	2013-09-09 12:20:32	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_content&view=articles&layout=modal&tmpl=component&function=jQuerySelectArticle_iform_request_id&cc8e2dce8506146376c413db3e334388=1	200	2922
903076	2013-09-09 12:20:32	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_content&view=articles&layout=modal&tmpl=component&function=jQuerySelectArticle_iform_request_id&cc8e2dce8506146376c413db3e334388=1	200	2922
903071	2013-09-09 12:19:50	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_menus&layout=edit&id=0	303	0
903070	2013-09-09 12:19:50	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_menus&layout=edit&id=0	303	0
903039	2013-09-09 12:19:31	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_menus&view=items	303	0

1 2 3 > Last of 122470 Results

Provides tools for analysis attacks, administrator can view and customize the filters necessary information. The system can filter based on time, domain, IP relate attack, and types attack. Through which can be traced to the attacker and export related reports.

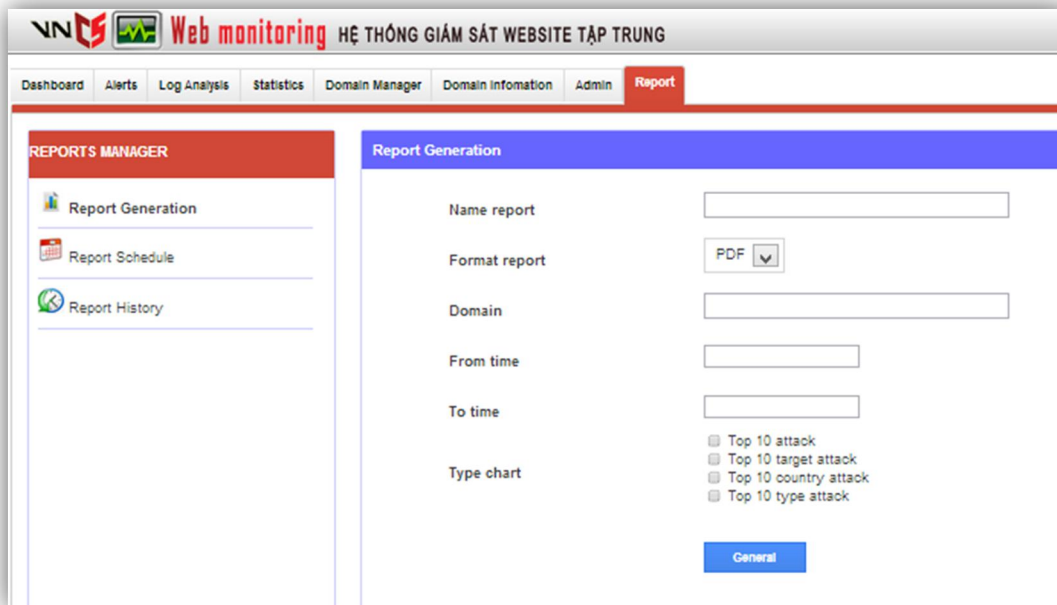
### Ability to monitor and statistics

With a user-friendly and visual interface, VNCS Web monitoring give statistics on the types of attack, address of attacker... Giving an overview of the system as well as a new event, the number of logs be sent to the system. Through these types of attacks, the administrator can trace the trail and make the treatment appropriate.



## Report for high level and status of the system

VNCS Web monitoring system give alert attacks and warn the user, through which, administrator have best overview of the system and export to the overview report for high level.



## Appropriate cost

This solution is implemented in the form of SaaS 2 (services) and hardware devices. Pricing is dependent on the number and bandwidth of the monitored sites.

Currently VNCS have 3 VNCS Web monitoring model with the ability to handle up to :

- 500 logs in 1 second (500 Eps)
- 1000 logs in 1 second (1000 Eps)
- Over 1000 Eps



(According to statistics, a normal Viet Nam website of an average organization has 20 log in 1 second or 20 Eps)