GIẢI PHÁP GIÁM SÁT WEBSITE TẬP TRUNG
VNCS WEB MONITORING

Trong thời gian qua, hầu hết các cuộc tấn công mạng nhằm vào website của các tổ chức, đặc biệt là gần đây, đã có nhiều cuộc tấn công nhằm vào website các cơ quan nhà nước, các tổ chức doanh nghiệp Việt Nam gây thiệt hại về mặt kinh tế và uy tín của các tổ chức.

Tuy nhiên, trên thị trường thế giới và Việt Nam hiện nay chưa có giải pháp nào tập trung hỗ trợ việc giám sát nhiều website một lúc với các tính năng hỗ trợ chuyên biệt (mặc dù đã có các giải pháp của HP, IBM... để giám sát một cách tổng thể cả máy chủ, cả mạng với chi phí rất cao).

Vì vậy, VNCS Web Monitoring là một trong những giải pháp an ninh hỗ trợ đắc lực cho các tổ chức, doanh nghiệp phải quản lý và đảm bảo bảo mật cho nhiều website cùng một lúc như Trung tâm CNTT các cơ quan nhà nước, các datacenter, các nhà cung cấp dịch vụ hosting, các tổ chức tài chính…

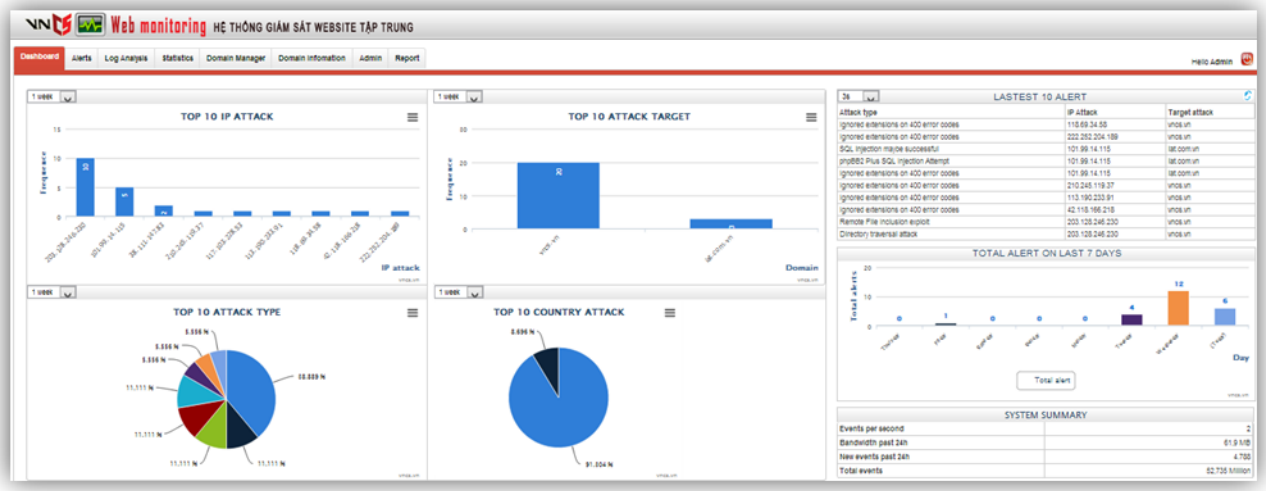
Giải pháp đạt danh hiệu Sao khuê, Nhân tài đất Việt 2014 và là giải pháp duy nhất của Việt Nam đạt giải ICT ASEAN do hội đồng Bộ trưởng CNTT ASEAN trao tặng.

VNCS Web Monitoring có khả năng giám sát web log tập trung (nhật ký truy cập web), khả năng phân tích tự động nhằm phát hiện tấn công và đưa ra cảnh báo qua SMS và email sử dụng giải thuật sáng tạo và các công nghệ tiên tiến như công nghệ nhận dạng IP, nhận dạng thay đổi cấu trúc website...

Giải pháp cũng cung cấp các công cụ tùy biến để hỗ trợ cho quản trị viên khi phân tích thủ công các cuộc tấn công. Với sự hỗ trợ của hệ thống này, quản trị

viên có thể rút ngắn quá trình phân tích web log, vốn tốn rất nhiều thời gian và công sức, từ đó, có thể hành động nhanh chóng khi hệ thống xảy ra sự cố.

VNCS Web monitoring cung cấp một kiến trúc thống nhất cho việc thu thập lưu trữ, các công cụ hỗ trợ việc phân tích và truy vấn dữ liệu thời gian thực liên quan đến các cuộc tấn công, các mối đe dọa trên hệ thống Website và đưa ra các cảnh báo tức thời.



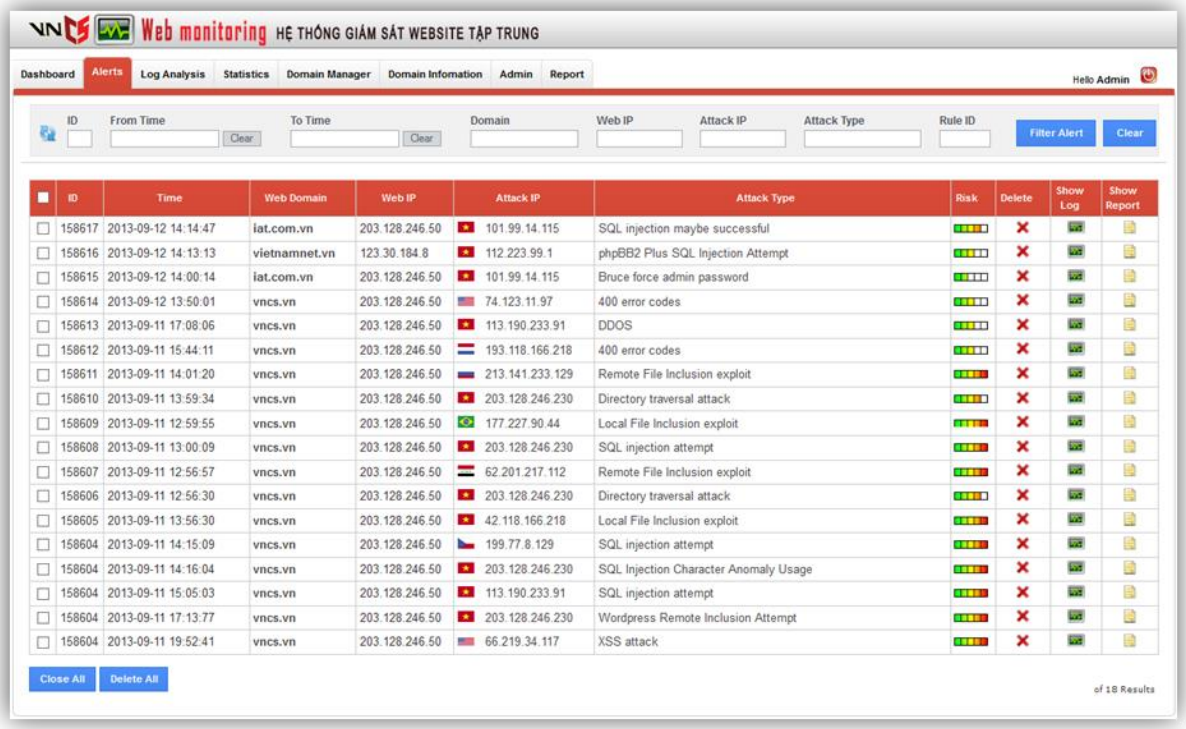
1. Quản lý giám sát log tập trung với giao diện thân thiện

Hệ thống VNCS Web monitoring có khả năng theo dõi, giám sát tất cả các sự kiện an ninh diễn ra trên nhiều website một lúc. Giải pháp đáp ứng các nhu cầu thực tế của người quản trị có thể quản lý được hệ thống website trên 1 giao diện đồng nhất. Trên giao diện này quản trị có thể dễ dàng quản lý, thêm bớt các website. Hệ thống giúp người quản trị có thể rút ngắn thời gian trong việc phân tích các log có trên từng hệ thống riêng rẽ.

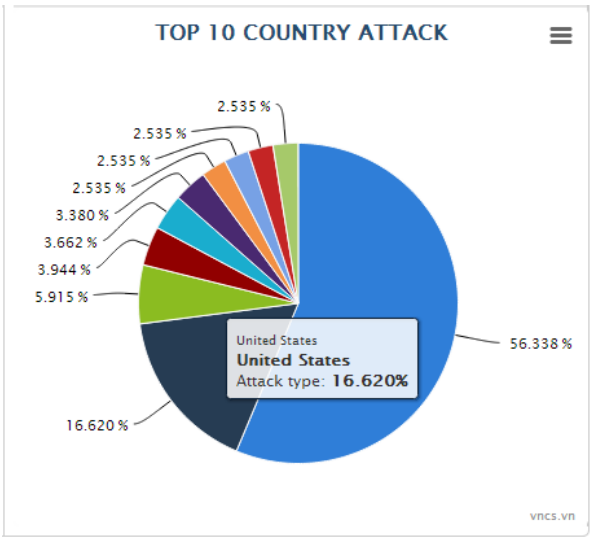
2. Khả năng phân tích tự động và cảnh báo theo thời gian thực

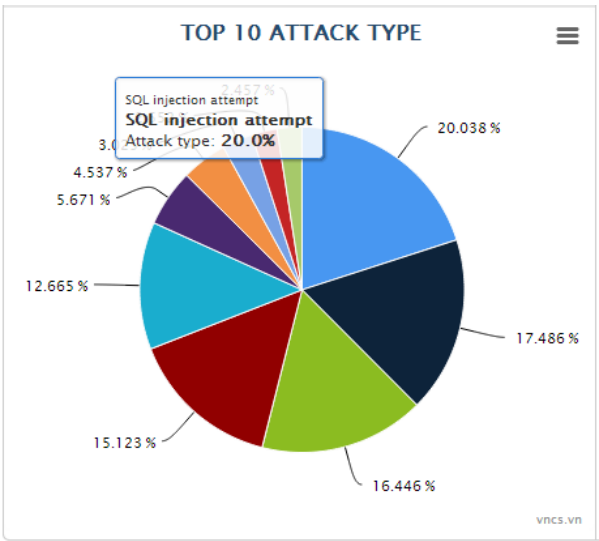
Giải pháp được cập nhật đặc điểm nhận dạng liên quan đến các cuộc tấn công mới nhất hiện có trên thế giới. Đồng thời VNCS có 1 đội ngũ nghiên cứu và phát triển riêng cho sản phẩm VNCS Web monitoring. Bằng các thuật toán thông minh, hệ thống giám sát website có thể tự động phân tích các tình huống

tấn công và sẽ gửi cảnh báo tức thời (qua Email, SMS) đến người quản trị khi phát hiện có tấn công vào website. Giải pháp này giúp người quản trị không cần can thiệp vào hệ thống log mà vẫn nhận được các báo cáo tấn công. Các hình thức tấn công mới luôn được đội R&D nghiên cứu và cập nhật sớm nhất để tích hợp vào hệ thống. Vì thế hệ thống có thể phát hiện chính xác và kịp thời các tấn công mới.



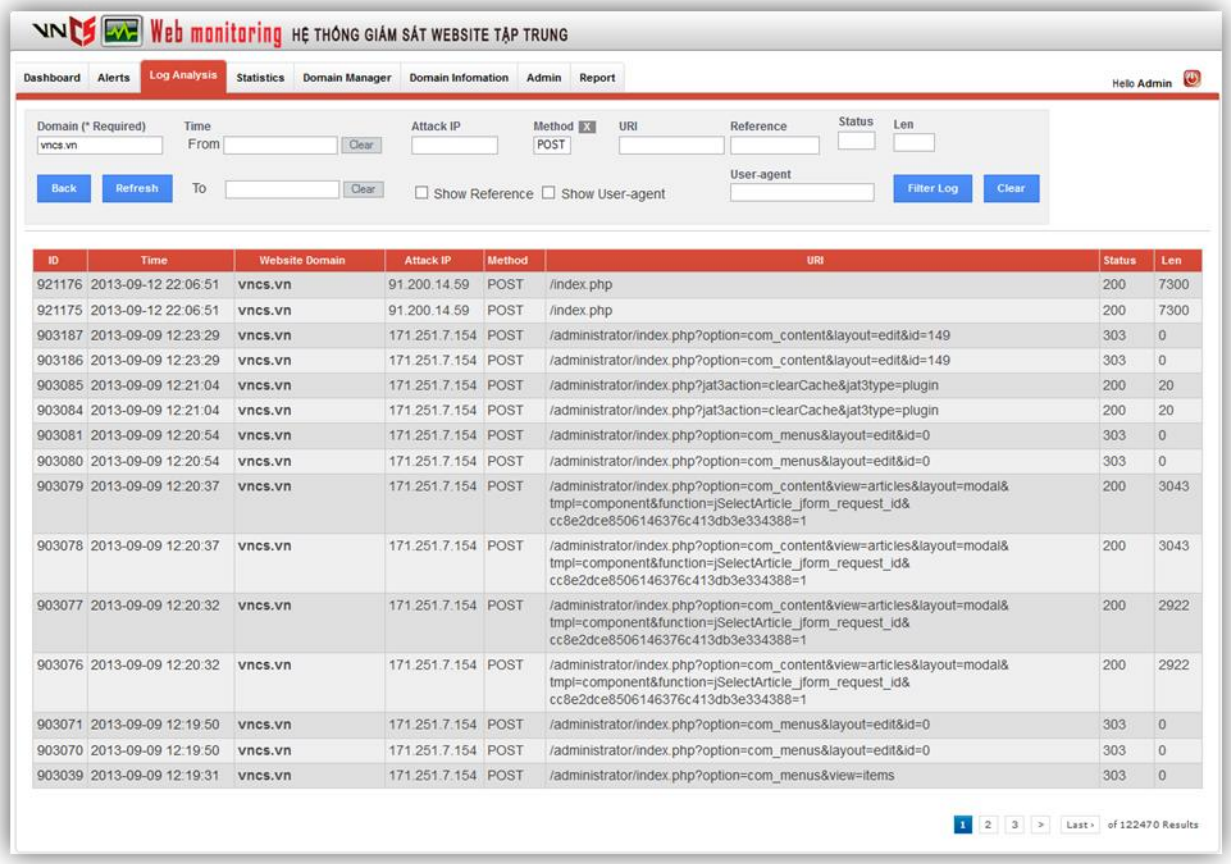
ID	Time	Web Domain	Web IP	Attack IP	Attack Type	Risk	Delete	Show Log	Show Report
158617	2013-09-12 14:14:47	iat.com.vn	203.128.246.50	101.99.14.115	SQL injection maybe successful				
158616	2013-09-12 14:13:13	vietnamnet.vn	123.30.184.8	112.223.99.1	phpBB2 Plus SQL Injection Attempt				
158615	2013-09-12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





3. Hỗ trợ tối đa cho quản trị phân tích sự cố bằng tay

Cung cấp cho người quản trị, công cụ để phân tích chi tiết các cuộc tấn công, người quản trị có thể xem và tùy biến bộ lọc để cô đọng các thông tin họ cần. Hệ thống có thể lọc các cuộc tấn công theo thời gian, domain, các IP liên quan đến các cuộc tấn công và các kiểu tấn công. Qua đó có thể truy tìm được kẻ tấn công vào hệ thống. Xuất ra các báo cáo theo ý muốn của mình.

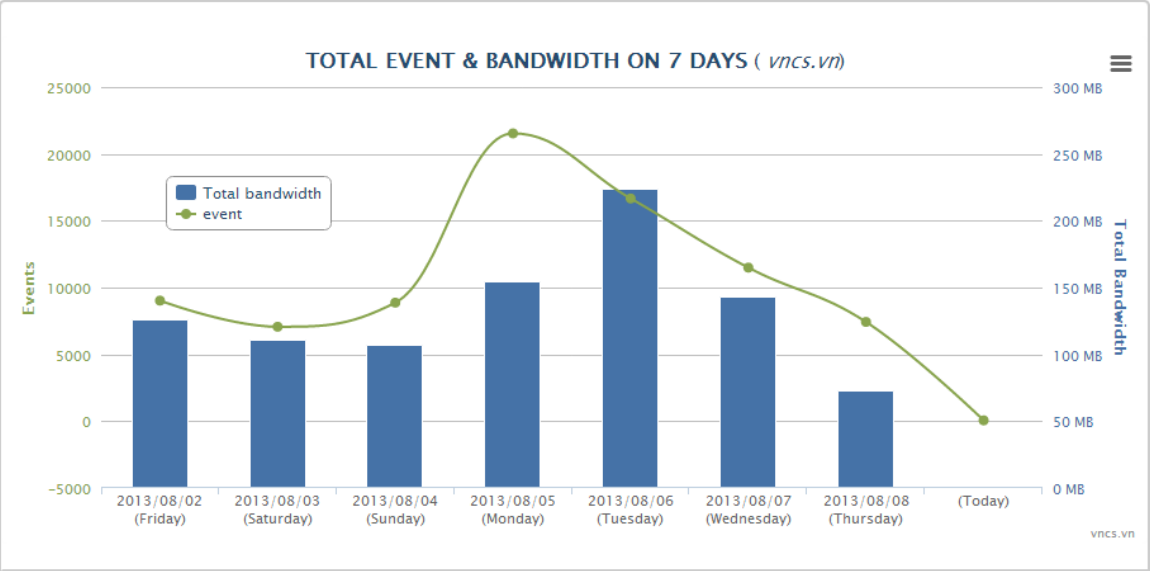


ID	Time	Website Domain	Attack IP	Method	URI	Status	Len
921176	2013-09-12 22:06:51	vncs.vn	91.200.14.59	POST	/index.php	200	7300
921175	2013-09-12 22:06:51	vncs.vn	91.200.14.59	POST	/index.php	200	7300
903187	2013-09-09 12:23:29	vncs.vn	171.251.7.154	POST	/administrator/index.php?option=com_content&layout=edit&id=149	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?jat3action=clearCache&jat3type=plugin	200	20
903084	2013-09-09 12:21:04	vncs.vn	171.251.7.154	POST	/administrator/index.php?jat3action=clearCache&jat3type=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=jSelectArticle_jform_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=jSelectArticle_jform_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=jSelectArticle_jform_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=jSelectArticle_jform_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

4. Khả năng theo dõi và thống kê

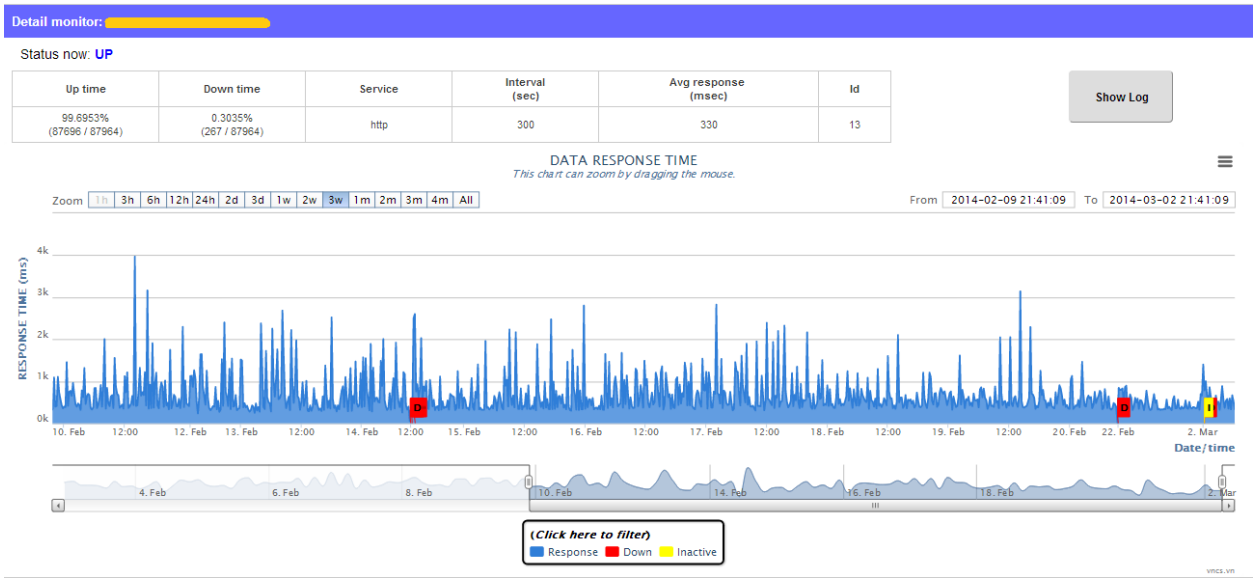
Với một giao diện thân thiện và trực quan. VNCS Web monitoring đưa ra các thống kê về các hình thức tấn công, các địa chỉ tấn công. Đưa ra cái nhìn tổng quan nhất về hệ thống cũng như các sự kiện mới, số log gửi về trên hệ thống. Thông qua các hình thức tấn công, người quản trị có thể lần ra các dấu vết tấn

công, để đưa ra các hình thức xử lý thích hợp. Thông qua các hệ thống này quản trị có thể sơ bộ phát hiện ra các cuộc tấn công vượt qua giới hạn cho phép như DoS.



5. Khả năng giám sát hiện trạng website

Tình trạng website up/down được theo dõi thường xuyên, với giao diện biểu đồ trực quan, cho phép người quản trị theo dõi xem trong 1 khoảng thời gian (6h, 12h, 24h, 1 tuần, 2 tuần, 1 tháng, 2 tháng,…) website bị down bao nhiêu lần. Điều này cho phép đánh giá hiện trạng cũng như đường truyền các website.



6. Khả năng phát hiện tấn công thay đổi giao diện (deface)

Deface Monitor tính năng phát hiện website bị tấn công thay đổi nội dung (deface). Deface là hiện tượng tin tặc chiếm quyền trên website và tiến hành thay đổi các hình ảnh, thông tin trên website. Deface không chỉ gây thiệt hại về kinh tế, mà còn ảnh hưởng rất lớn uy tín và hình ảnh của các cơ quan, tổ chức khi tin tức đưa các hình ảnh, thông tin xấu lên website. Đây là một tính năng thực sự rất hữu ích cho người quản trị hệ thống. Trên thị trường hiện nay, rất ít các sản phẩm có tính năng này, hoặc như có cũng chưa được tối ưu hoặc tiện lợi cho người sử dụng. Với tính năng phát hiện tấn công deface website, người quản trị hệ thống hoàn toàn có thể yên tâm khi có bất kì sự thay đổi nào bất thường trên hệ thống, VNCS Webmonitoring sẽ gửi ngay cảnh báo cho quản trị viên (Email, SMS) kèm với ảnh chụp website để xác minh.

7. Báo cáo về thực trạng hệ thống

Hệ thống VNCS Web monitoring đưa ra các cuộc tấn công, và cảnh báo đến người dùng, thông qua đó có cái nhìn tổng quan nhất về hệ thống. Xuất ra các

báo cáo tổng quan nhất. Đưa ra các báo cáo cho người quản trị cũng như các báo cáo cho lãnh đạo cấp trên.

8. Triển khai đơn giản & Chi phí phù hợp

VNCS Web monitoring được tích hợp toàn bộ vào một thiết bị phần cứng (appliance). Appliance được triển khai dễ dàng bằng cách đặt sau và nhận thông tin từ các web server. Giá thành của sản phẩm được tính tùy thuộc vào số lượng và băng thông các website cần giám sát.

Hiện tại VNCS Web monitoring có 3 dòng sản phẩm có khả năng xử lý lên tới:

- 500 Log trong 1 giây (500 Eps)
- 1000 Log trên 1 giây (1000 Eps)
- Trên 1000 Eps

(Theo thống kê, một website bình thường của một tổ chức, doanh nghiệp trung bình có khoảng 20 Log trên 1 giây tức 20 Eps)

VNCS cũng cung cấp dưới dạng dịch vụ tại http://wm.vncs.vn