First Line of Defense®

FIRST LINE OF DEFENSE





KEY BENEFITS



Comprehensive Visibility

Gain comprehensive visibility into DDoS attacks and cyber-threats with easily accessible security focused dashboards



Stay ahead of threats by getting early warning signs of suspicious and malicious activity with alerts and scheduled reports



Capabilities

Create a virtual security operations center to deliver centrally managed security services in a turn-key manner

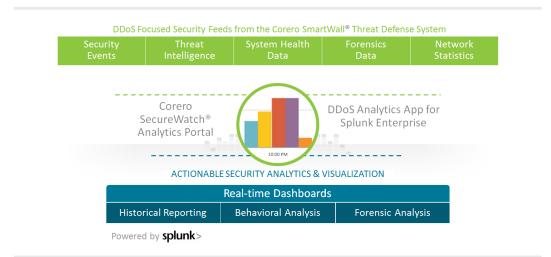
"The ability to uncover hidden patterns of data, identify emerging vulnerabilities within the massive streams of DDoS attack and security event data, and respond decisively with countermeasures, provides our team with the tools required to better protect our organization against the dynamic cyber threat landscape"

- Jay Naik, Assistant Director of Technical Services, Shubert Ticketing

TURN-KEY VISIBILITY INTO DDOS ATTACKS AND CYBER THREATS

A significant challenge facing many organizations is the inability to extract meaningful realtime information on DDoS attacks and cyber threats from volumes of security events. To date, only minimal visibility into these classes of security events has been available, and only to organizations with significant investments in analytics tools and expert security staff. In any case, security analysts are left to react to the threats after the damage has been done.

Corero SecureWatch[®] Analytics is a powerful web-based security analytics portal that delivers turn-key visibility into DDoS attacks and cyber threats with comprehensive and easy-to-read security dashboards. Large organizations can benefit from the DDoS focused granular security event data and augment their security event monitoring practice. All companies benefit from the turn-key SecureWatch Analytics portal that delivers unprecedented DDoS and cyber threat visibility without requiring dedicated security analysts to sift through reams of unintelligible log data.



SecureWatch Analytics is included with the purchase of the Corero First Line of Defense® products as a part of your DDoS defense investment. The portal transforms DDoS tailored security feeds from Corero SmartWall Threat Defense System deployments into dashboards of actionable security intelligence, exposing:

- Volumetric DDoS reflection, amplification, & flooding attacks
- Targeted resource exhaustion attacks
- Under the radar low and slow attacks
- Victim servers, ports, and services
- Malicious IP addresses and botnets

Empowered by this enhanced visibility, organizations can utilize SecureWatch Analytics as a single pane of glass to visualize and mitigate DDoS attacks and cyber threats, and ensure uninterrupted business continuity for their Internet facing services. Additionally, MSSPs can augment their existing Security Operations Center (SOC) with a virtual SOC to create customized dashboards that are relevant to specific industry verticals and deliver managed security services to their customers.

FEATURES AND FUNCTIONALITY

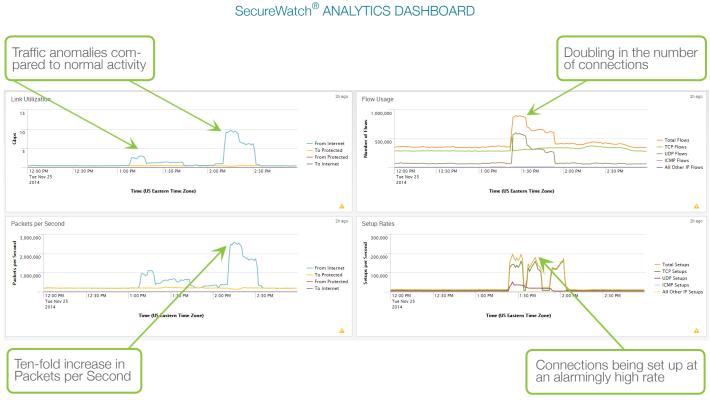
SecureWatch Analytics is easily accessible via any browser and provides real-time and historical dashboard views that summarize network and security activity in the datacenter. Users can view these dashboards at a site by site level or in an aggregate view that provides a consolidated security pricture. Likewise, MSSPs can manage reporting for all their customers from one central location.

NETWORK LEVEL VISIBILITY

Network level statistics are typically the leading indicators of detecting unusual activity targeting a network. Link utilization, packets per second rate, number of active flows, and flow set up rates provide insight into the following analysis:

- Is there any anomaly in the volume of network traffic as compared to normal activity?
- In which direction (inbound/outbound/bidirectional) is the traffic anomaly?
- Which other events can the anomaly be correlated to?

The charts in Figure 1 show an anomaly in network level activity during a 30-minute period in a hosting data center network.





In the example above, the link utilization jumps to 3 Gbps and then to almost 10Gbps. The packets per second (pps) rate spikes from 200K pps to over 2 million pps. Connection counts double and new connections are being set up at an alarmingly high rate. These indicators would cause security administrators to investigate security events in that time period in more detail. SecureWatch Analytics can greatly assist in this process, accelerating the response time for a network that is under attack.

ATTACK VECTOR VISIBILITY

DDoS attacks are generally comprised of targeted server attacks, reflective amplification attacks, and low and slow attacks that are difficult to detect. Figures in this section show examples of a variety of DDoS attacks that can be targeted at servers or can be generated from compromised servers and botnets.

Figure 2 shows security activity occurring at the same time as the anomalous network activity shown in Figure 1. The most notable is that the data center was targeted with a multi-vector attack consisting of volumetric NTP amplification attack, a universal plug-n-play reflection attack, and a SYN flood, all during a span of an hour. In addition, a variety of smaller attacks such as fragmented traffic, illegal headers, and bad checksums were blended in during this volumetric attack. Often, volumetric attacks are used as a smoke screen to hide low and slow application layer attacks. Hence, visibility into malicious activity at a granular level is another important feature of SecureWatch Analytics.

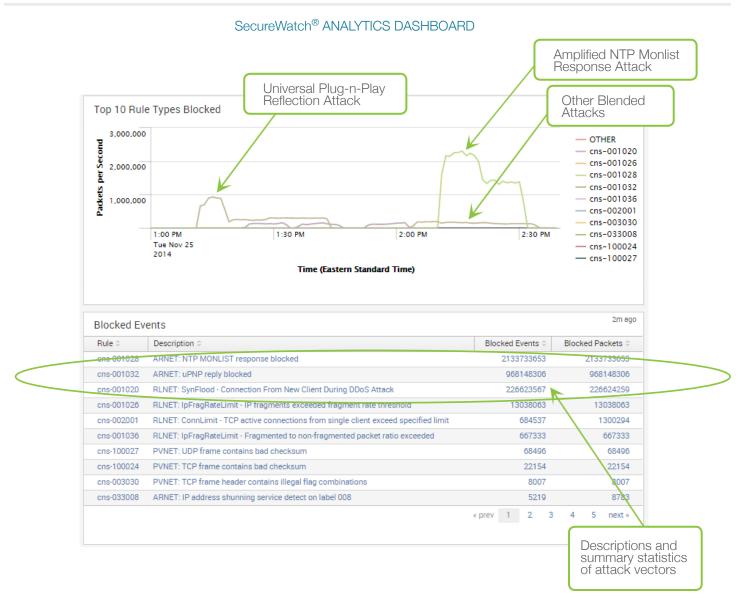


Figure 2 - Multi-vector attack from compromised servers & botnets

Figure 2 shows a classic example of a reflection attack where botnets spoof victim server IP addresses and send NTP monlist requests to compromised NTP servers on the Internet. The compromised NTP servers. send responses, which are amplified by a large factor as compared to the requests, back to the target servers, overwhelming them with large amounts of unsolicited traffic. Compromised servers on the Internet can be used as launch pads for sending large amounts of DDoS traffic.

SecureWatch® ANALYTICS DASHBOARD



Figure 3 – SYN Flood Attack

In Figure 3, the SecureWatch Analytics attack dashboard shows a SYN flood attack where half-open TCP connection requests are made by new clients during a DDoS attack. In Figure 4, the SecureWatch Analytics dashboard shows a large scale DDoS attack as a result of amplified NTP monlist responses generated from a compromised NTP server on the Internet. The dashboard also gives visibility into anomalies that are configured for detection only, which can provide guidance into possible configuration changes. SecureWatch Analytics provides granular visibility into each type of attack and tracks its behavior over time.

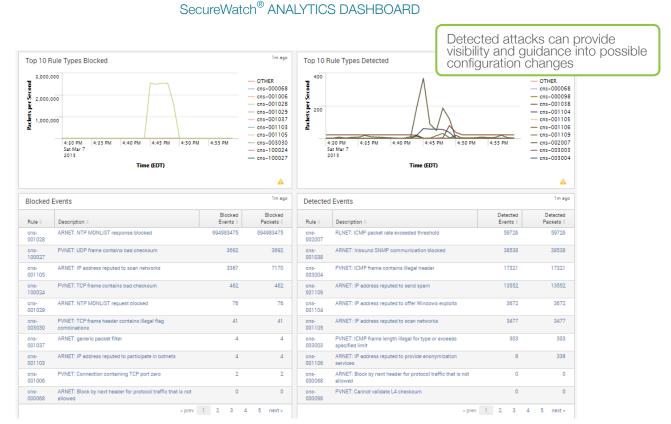


Figure 4 -SecureWatch Analytics provides visibility into both blocked malicious as well as detected suspicious activity

ATTACKER IDENTIFICATION

It is just as critical to know who is attacking you as it is to know that you are under attack. This is especially useful in reflection attacks where the source server addresses are real. SecureWatch Analytics gives you the ability to immediately drill down to see the offending addresses and hostnames associated with attackers targeting your infrastructure. These can then easily be incorporated into ACLs and blacklists to permanently or temporarily block access for devices with no legitimate reason to be accessing your network.

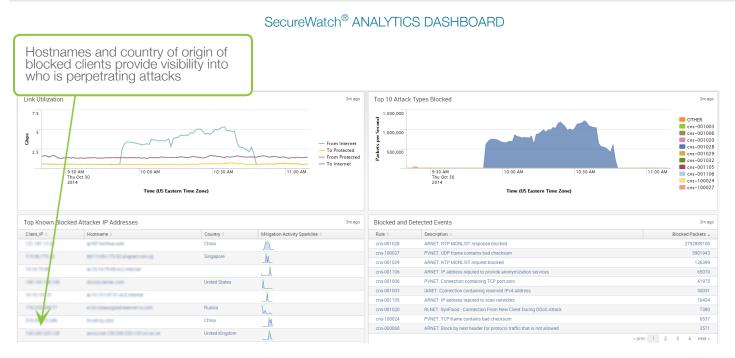


Figure 5 - Attacker visibility

TARGETED SERVER VISIBILITY

Organizations provide a variety of Internet facing services ranging from web, DNS, mail, and more, requiring open parts on the network. Malicious attackers seek out target servers to attack by scanning open ports. SecureWatch Analytics provides a detailed report of activity on server ports highlighting which ports are being accessed the most, how many clients are accessing them, and which protocols are being used.

SecureWatch® ANALYTICS DASHBOARD

Server_Port 0	# of Events 😄	# of Client IP's 🗧	# of Server IP's 🗧	Protocols Used 0	Rules Blocking Traffic ÷	Mitigation Activity Sparkline ÷	
53	347387	11579	5054	TCP UDP	5		
80	257940	7675	22022	TCP UDP	7		
25	40657	2514	5690	TCP	7		
22	24281	282	22241	TCP	7	man have the survey	
445	20228	772	17808	TCP	7	and have been been and	
1080	15258	10	14945	TCP	3	MMMMMMM	
8088	14673	2	14390	TCP	2	Mahammahalan	
29786	9997	64	76	TCP	5	man man	
30014	8414	1	1	TCP	1	month	
19786	4887	54	31	TCP	5	man	

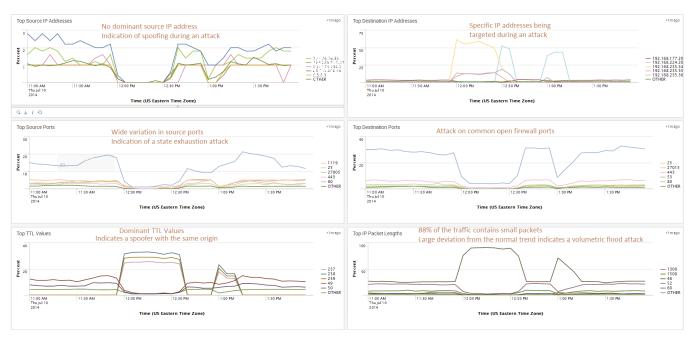


SAMPLE SFLOW NETWORK STATISTICS

SecureWatch Analytics displays a statistical view of the inbound traffic activity using IP sFlow samples collected from the Corero SmartWall Threat Defense System. These top charts contain reports about:

- Source IPs
- Destination IPs
- Source ports
- Destination ports
- TTL (time-to-live)
- Packet lengths
- Protected host groups

These top reports can provide additional data to analyze and determine if security policy changes are required.



Sample sFlow Statistics Screen Shots

Figure 7 - sFlow statistics provide insight into deviations from normal baseline behavior

FORENSIC ANALYSIS AND REPORT GENERATION

SecureWatch Analytics archives security event data to enable forensic analysis of past threats and compliance reporting of security activity. Users can analyze event data based on preset times (last 24 hours, 7 days, 30 days) or select a more specific time frame.

SecureWatch[®] ANALYTICS DASHBOARD

lite	Т	ime Frame			
Corero Corporate Smartwall (95)	*	Last 30 days	~	Submit	
~ Presets					
Week to date La Business week to date La Month to date La Year to date La	st 15 mi st 60 mi st 4 hou st 24 ho st 24 ho st 7 day st 30 da	nutes irs vurs s			Preset time intervals for historical analysis
> Date Range		Date and time for more speci	fic attack analy	n /sis	
> Date & Time Range 🖌		within a time p	eriod		

Figure 8 - Historical Report Generation

In addition, PDU data from security and sflow events can be extracted to a file and imported into external applications, such as Wireshark for forensic analysis.

EXPORT Perform freeform queries against a sit	tes statistical and event data.		
Site	Time Frame	Search Modifier	
Corero Corporate Smartwall (_ 🖸	* Today	v *	Submit
Use the search modifier to filter the	events shown below. Refer to Co	rero's Syslog format document for additional de	tail on the supported fields

			Evenet Desuits		×														A
PD	U data		Export Results		×														2h eg
1	Time	Event	Format	Raw Events ~															
>	3/11/15 12:00:00.000 AM	03/11/15 00:00:00 000000 00 17 54 01 be 7e ad 50 10 02 92 cd 47 00 00 8a ea 79 55 47 85 25 08 bb 7b 9e ea 88 23 1e f9 a1 77 67 ca f7 86 69 a6 09 4a 01 45 1d .	File Name Number of Results	Hex_Dump_for_Wireshark_Analysis Unlimited Limited		5 87	5e Oc 94 49	cb e 22 9	3 92 9 74	46 e	a 63 1 ed	ea 82	50 c8 92 e1 a4 39 46 a0	1 a4 5 26	4 68 5 cf	8 1c F 73	58 96	bd bd	d 68 e 18
>	3/11/15 12:00:00.000 AM	03/11/15 00:00:00 000000 00 17 54 0 be 7e ad 50 10 02 92 9a 81 00 00 bf 20 62 19 5c 40 d9 b7 41 1a a9 9b 8e 58 ff 40 a4 1c d9 29 b4 64 2b e7 81 11 0b 77 80 .	Cancel	Exp	iort		42 ff e5 e3	77 c 20 c	c 79 b f5	a7 8 bc f	2 a7 4 0d	4d 75		7 c9 d b4	9 ff 4 00	f 25 0 64	80 e9	63 8a	3 150 a 81
>	3/11/15 12:00:00.000 AM	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	b7 c1 55 4e 30 9f 6d 02 10 09 ad cb ab b8 8b d8 e0 da	75 d7 ce f1 09 95 d8 56 be 75 1f 78 e3 3b 1c c6 4a 7d 30 ae	6d 7	9 47 9 1a	c5 51 2c 06	fd a Of 4	f cb 7 40	6b b 20 f	6 40 6 f1	87 2.a	ac 38 b1 20	8 96 d 7b	5 29 5 66	a4	89 a9) c1) ca	1 5d a 87
>	3/11/15 12:00:01:000 AM	03/11/15 00:00:01 000000 00 19 e2 3c 18 73 86 50 10 ff 37 ee 3e 00 00 00 00		00 45 00 00 28 03 69 40 00 7d	06 7	4 05	3f ef	23 0	c b8	1d 6	a 89	<8	a0 00	50	90	be	7e	ad	e 3
>	3/11/15 12:00:02:000 AM	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	b8 69 55 10 84 0a cc 5b 3b f1 ad 6c 1f ca 0f b4 ca 3f	af 1d c7 3c 1a 8b bb b3 ce ce 64 3f 50 1e 94 22 25 0a 79 c7	92 8 cb a	6 a0 d 55	64 fb f2 54	76 6 f6 3	3 7f b 14	c6 5 0f 8	b 88 3 6e	68 45	18 38 25 ea	8 5d a 6d	d 64 c a5	4 9a 5 5d	d0	0 0a	a 3b 4 b3
>	3/11/15 12:00:02.000 AM	03/11/15 00:00:02 000000 00 19 e2 3c ef 73 47 80 10 16 27 4f e9 00 00 01 01			06 9	d 9b	3f ef	23 0	2 ad	c2 7	'b 4f	f2	e9 01	bb	96	f5	4f	bd	96
>	3/11/15 12:00:02.000 AM	03/11/15 00:00:02 000000 00 19 e2 3c 35 d0 3e 50 10 ff 37 91 69 00 00 00 00		00 45 00 00 28 06 1b 40 00 7d	06 7	1 53	3f ef	23 0	c b8	1d 6	a 89	c8	a0 00	50	90	be	7e	ad	e3
>	3/11/15 12:00:03.000 AM	03/11/15 00:00:03 000000 00 17 54 01 be 7e ad 50 10 02 92 e9 at 00 00 c9 e7 ca 3f 7e c0 fd e6 3e 75 e7 72 00 ad 82 fe 8d 17 84 9a e3 eb aa 2d df 64 30 d4 6b .	72 54 ea 1e 0b 2c de ca 09 f7 e9 51 b1 fe 8b cb 10 24	2d b1 ac 1d ee 08 93 82 f8 7c ee 18 aa fa af 00 f1 14 71 e3	: 76 6 aa 2	1 b1 d 12	c3 a9 df 9d	59 9 45 4	a 4a 4 9a	d8 9 ba e	1 56 7 d5	94 e0	b9 d1 1f 6e	f 25 e e4	5 79 4 f8	9 38 8 c0	70 e4	b5 bc	5 5f 5 31
>	3/11/15 12:00:03:000 AM	03/11/15 00:00:03 000000 00 19 e2 3c 52 c6 4e 50 10 ff 37 9b 3c 00 00 00 00		00 45 00 00 28 08 da 40 00 7d	06 6	e 94	3f ef	23 0	c b8	1d 6	a 89	c8	a0 00	3 50	90	be	7e	ad	e3
>	3/11/15 12:00:03:000 AM	03/11/15 00:00:03 000000 00 19 e2 3c 53 04 ec 80 10 16 93 b4 4e 00 00 01 01			06 b	8 cf	3f ef	23 0	2 ad	c2 7	b 57	f2	e6 01	bb	98	63	6f	ed	s Sf
						< prev		2	3	4	5	6	7	8	в	9	10	0	next +

Figure 9 - PCAP Export for Forensic Analysis

BROWSER REQUIREMENTS FOR CORERO SecureWatch ANALYTICS

Corero SecureWatch Analytics is accessible to all Corero customers with an operational SecureWatch Server (included with your purchase of SecureWatch Analytics) and an active support contract. The access is supported via the following browsers:

- Firefox latest release
- Internet Explorer 9 and higher
- Safari latest release
- Chrome latest release

LEARN MORE ABOUT CORERO SECUREWATCH ANALYTICS

SecureWatch Analytics was developed with the deep security experience and knowledge base obtained by our security analysts that deliver our market leading SecureWatch PLUS service. SecureWatch PLUS is a comprehensive suite of DDoS configuration optimization, monitoring and response services. As your trusted advisor, Corero is extending the lessons from this security expertise to our customers and partners to better defend against cyber-crime.

To learn more and see a demonstration of SecureWatch Analytics, please visit http://www.corero.com/SecureWatch_Analytics or contact us at info@corero.com.

ABOUT CORERO NETWORK SECURITY

Corero Network Security, an organization's First Line of Defense[®] against DDoS attacks and cyber threats, is a pioneer in global network security. Corero products and services provide online enterprises, service providers, hosting providers, and Managed Security Service Providers with an additional layer of security capable of inspecting Internet traffic and enforcing real-time access and monitoring policies designed to match the needs of the protected business. Corero technology enhances any defense-in-depth security architecture with a scalable, flexible and responsive defense against DDoS attacks and cyber threats before they reach the targeted IT infrastructure allowing online services to perform as intended. For more information, visit www.corero.com.

Corporate Headquarters 1 Cabot Road Hudson, MA 01749 USA Phone: +1.978.212.1500 Web: www.corero.com EMEA Headquarters Regus House, Highbridge, Oxford Road Uxbridge, England UB8 1HR, UK Phone: +44.0.1895.876579

Copyright 2015 Corero Network Security, Inc. All rights reserved. 867-5309-003