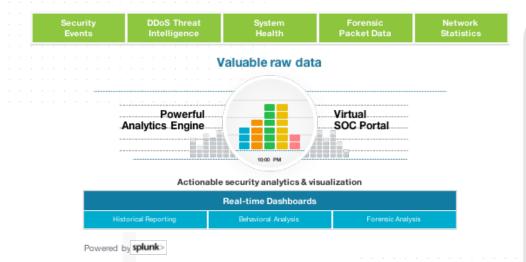
SecureWatch[®] Analytics

Comprehensive DDoS Attack Visibility

Corero SmartWall[®] SecureWatch[®] Analytics (SWA) solves a significant challenge facing many organizations; their inability to extract meaningful realtime information on DDoS attacks from volumes of security events. Typically, only minimal visibility into these classes of security events is possible, and only to organizations with significant investments in detailed analytics tools and expert security staff. Security analysts are often left reacting to DDoS threats after the damage has already been done.

SecureWatch Analytics is a powerful security tool that delivers comprehensive visibility into DDoS attacks with easy-to-read security dashboards. Organizations benefit from the DDoS focused granular security intelligence which can enhance their broader security event monitoring practices. The multi-user web UI of the SecureWatch Analytics application delivers unprecedented DDoS visibility and actionable intelligence, before, during, and after the attack, without requiring specialist security analysts to sift through reams of unintelligible log data.



SecureWatch Analytics is included as a key component of Corero's SmartWall® real-time, automatic, DDoS defense solutions. It transforms DDoS tailored security feeds from SmartWall deployments into autonomic defense actions and dashboards of actionable security intelligence, exposing:

- Volumetric DDoS reflection, amplification, & flooding attacks
- Targeted resource exhaustion attacks
- Under the radar non-saturating 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 DDoS attacks and help ensure uninterrupted business continuity for their Internet facing services.



Key Benefits



Comprehensive Visibility

Forensic-level visibility and analysis of DDoS; before, during and after attacks, via easy to use dashboards of actionable intelligence.

Ø

Automatic & Accurate

Accurate automatic mitigation delivers lowest TCO and enables your IT and security teams to spend more time defending

睝

Service Enablement

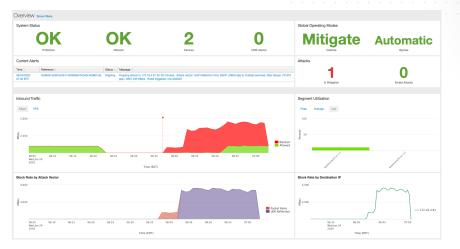
Comprehensive visibility with reporting and alerting for clear, actionable, intelligence on the DDoS attack activity across the network.



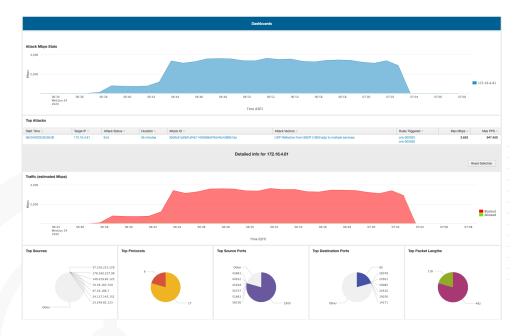
Multi-User NOC/SOC Dashboards

SecureWatch Analytics (SWA) is easily accessible via any browser and delivers real-time and historical dashboard views that summarize network and DDoS activity across the organization. Analysts can view these dashboards at a site by site level or in an aggregate view that provides a consolidated security picture.





SWA enables analysts to quickly understand the size and profile of each attack, in realtime, including the specific vectors used at any point in time. It also delivers, in a single pane of glass view, real-time monitoring and reporting on the overall SmartWall system health and protection status..



Drill-Down on Attacks

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 and destination IPs and Ports, Protocols, TTL (time-to-live), Packet lengths and Fragments. These top reports can provide additional data to analyze and determine if security policy changes or tuning is required.



Detailed Traffic Statistics

It is critical to know the details when you are under attack. SecureWatch Analytics gives you the ability to immediately drill down to see the offending addresses, ports, protocols and other key insight into the attackers targeting your infrastructure.



Ime Selector: P	Pan across the chart to se	ect a differe	nt timeframe											
_														
0.00	02:00 04:00		6.00 08.00	10:00	12:00	14:00	16.00	18:00	20.00 22.00	00:	on.	02:00 04:00	06:00	
led Jun 24 020	01.00		0.00	10.00	12.00	14.00	10.02	10.00	10.00 21.00		i Jun 25	04.00	00.00	
							Time (EDT)							
													0	2 minut
mpled Events	s Timeline													
5,000														1,600,
0		٨			4					J 6		4		
1.000	> O N	N.				M		0 0		\mathbb{N}	0 1	. 14	0	\$00.0
				1 11 1	A 11							1 11	11	
	ΠΠΛ	11 .	<u>, </u>		$1 \land 1$	\ \r	117 🗖			hin. In				
00.00	02:00	100	06:00 08:00	10.00	12:00	14:00	16.00	8:00	20.00 22:00	00:00	02.00	04:00 06:0		
Wed Jun 2 2020	24		00.00	10.00	11.00	14.00	10.07		10.00	Thu Jun 25	44.00	04.00 00.0	·	
2020						T	me (EDT)							
						Sampled Events - B		Detected Packet	13					
						Sampled Events - 8		Detected Packet	13					
ìon			Direction			Sampled Events — 8 Protocols		- Detected Packet	Fragmented Packet			Packet Length		
	count 0	percent 0	Direction O	count :	percent 0			percent :		count o	percent o	Packet Length Packet Length :	count 0	p
o ne	count 0 202777	percent 0 95.048574		count 0 211119		Protocols	locked Packets —		Fragmented Packet	oount 0 172011	percent 0 81.475850		count 0 129801	
on o k			Direction 0	211119	percent o	Protocols	ocked Packets -	percent o	Fragmented Packet			Packet Length :		61
an o k ct	202777 8342	95.048574	Direction 0		percent o	Protocols Protocol 17 6	count 0 147819 65300	percent 0 70.016910	Fragmented Packet Pragmented Packet 0	172011	81.475850	Packet Length : 482 60 1482	129801 39109 18017	61 18 8
n o k ct	202777	95.048574	Direction 0	211119	percent o	Protocols Protocol 17 6	count 0 147819	percent 0 70.016910	Fragmented Packet 0 Pragmented Packet 0 1 2	172011 20969 18139	81.475850 9.932313	Packet Length 0 482 60 1482 118	129801 39109 18017 15851	61 18 8
n o k ct	202777 8342	95.048574	Direction 0	211119	percent o	Protocols Protocol 17 6	count 0 147819 65300	percent 0 70.016910	Fragmented Packet Fragmented Packet 0 1	172011 20969 18139	81.475850 9.932313	Packet Length : 482 60 1482	129801 39109 18017	61 18 8
an o k ct	202777 8342	95.048574	Direction 0	211119	percent o	Protocols Protocol 17 6	count 0 147819 65300	percent 0 70.016910	Fragmented Packet 0 Pragmented Packet 0 1 2	172011 20969 18139	81.475850 9.932313	Packet Length 0 482 60 1482 118	129801 39109 18017 15851	61 18 8 1
ion : sk ect	202777 8342	95.048574	Direction 0	211119	percent o	Protocols Protocol 17 6	count 0 147819 65300	percent 0 70.016910	Fragmented Packet 0 Pragmented Packet 0 1 2	172011 20969 18139	81.475850 9.932313	Packet Length 0 482 60 1482 118 1514	129801 39109 18017 15851 8175 - prev 1	61 18 8 1
ion : sk ect	202777 8342	95.048574	Direction 0	211119	percent o	Protocols Protocol 17 6	count 0 147819 65300	percent 0 70.016910	Fragmented Packet 0 Pragmented Packet 0 1 2	172011 20969 18139	81.475850 9.932313	Packet Length 0 482 60 1482 118 1514	129801 39109 18017 15851 8175	61 18 8 7 3
k k ct	202777 8342	95.048574	Direction 0 Inbound Perset	211119	percent o	Protocols Protocol 3 17 6 Resot 5	count 0 147819 65300	percent 0 70.016910	Fragmented Packet Pragmented Packet 0 1 2 Reservator	172011 20969 18139	81.475850 9.932313	Packet Lingth : 482 60 1.682 118 1514	129801 39109 18017 15851 8175 - prev 1	61 18 8 1
on :: At lict	202777 8342	95.048574	Direction 0	211119	percent o	Protocols Protocol 17 6	count 0 147819 65300	percent 0 70.016910	Fragmented Packet 0 Pragmented Packet 0 1 2	172011 20969 18139	81.475850 9.932313	Packet Length 0 482 60 1482 118 1514	129801 39109 18017 15851 8175 - prev 1	61. 18 8 7. 3
on 0 k et	202777 8342	95.048574	Direction 0 Inbound Perset	211119	percent o	Protocols Protocol 3 17 6 Resot 5	count 0 147819 65300	percent 0 70.016910	Fragmented Packet Pragmented Packet 0 1 2 Reservator	172011 20969 18139	81.475850 9.932313	Packet Lingth : 482 60 1.682 118 1514	129801 39109 18017 15851 8175 - prev 1	61. 18 8 7. 3
ion :: :k ect urce IP	202777 8342 Reset selection(current-')	96.049674	Direction : Inbound Result Source Port	211119 selection(currents*)	percent 0	Protocols Protocol 77 6 Protocol Recot 9 Protocol Protoco	count :	percent 0 70.016910 29.935020	Fragmented Packet Pragmented Packet 0 0 1 2 Reset sealed	172011 20669 18139 on(current=")	81.475850 9.902313 8.591837	Packet Lingth : 482 60 1.682 118 1514	129801 39109 18017 15851 8175 - prev 1	61. 18 8 7. 3
urce IP	202777 8542 Reset selection(surrens-') Country © count. ©	96.048674 3.961326	Directon : hourd Prease Reset Source Port Bource Port	211119 selection(ourrent="") count :	percent 0 100.000000	Protocols Protocol IT 6 Read a Read a Destination IP Locatination IP :	court 0 147919 65300 eelection(ourrent=")	percent 0 70.016910 29.953090	Pragmented Packet 0 0 1 2 Reset select Destination Port Destination Port 0	172011 20689 18139 on(current=")	81.475850 9.932313 8.591837 percent 0	Packet Lingth : 482 60 1.682 118 1514	129801 39109 18017 15851 8175 - prev 1	94 61. 18. 8. 7. 3. 2
urce IP	20277 8542 Reset salection(current=') Country : count : 8542	95.048674 3.961328 parcent : 3.961328	Deveton : Infound Perset Perset Source Port Source Port 100 100 100	211119 selection(ourrent=*) count : 59461	percent 0 100.000000 percent 0 20.812001	Protocols Protocol : 17 6 Preset s Preset	locked Packets	percent 0 70.016910 29.985000 percent 0 74.034549	Fragmented Packet Pragmented Packet Pragmented Packet 1 Pragmented Packet 1 Pragmented Packet Pragmented Pragmented Packet Pragmented Pragmented Packet Prag	172011 20069 18139 on(current=*) count 0 36620	81.475850 9.932313 8.091837 percent 0 19.079697	Packet Lingth : 482 60 1.682 118 1514	129801 39109 18017 15851 8175 - prev 1	61. 18 8 7. 3
an 0 k kt sce P 0 10.4.71 18.4.95	202777 8342 Peost selection(summers-7) Country = court = 6342 8342	95.048674 3.961328 pascent 0 3.961326 1.836879	Devetor : Hourd Read Source Port Source Port 1900 19	21119 selection(current=") count : 39401 38524	percent 3 100.000000 percent 3 30.010001 20.160966	Protocols Protocol 17 6 Rest Rest	court 0 147319 65300 65500 666c10n)0umerts-7 155501 155501 166776	percent 2 70.016910 28.085070 percent 2 74.036569 22.014125	Programated Packet Programated Packet Programmered Packet Programmered Packet Programmered Pr	172011 20009 18139 on(current=*) 00(current=*) 38820 8341	61.475850 9.932313 8.591837 percent 0 18.079697 4.322210	Packet Lingth : 482 60 1.682 118 1514	129801 39109 18017 15851 8175 - prev 1	61. 18 8 7. 3

These can then easily be reported on, or incorporated into ACLs and blacklists to permanently or temporarily block access for devices with no legitimate reason to be accessing your network.

Packet-Level Forensics

SecureWatch Analytics archives security event data down to the power distribution unit (PDU) level, enabling forensic analysis of ongoing and past threats for greater intelligence and compliance reporting on security activity. Authorized Users can analyze event data based on preset timescales (e.g. last day, week, or month) or select a very specific timeframe when investigating past events, for example.

Dashtarark																		
n	Time Selector: Pan across the chart to select a different timeframe																	
1																		
1	0:00 fed Jun 24 020	02:00	04:	00 0	06:00	08:00	10:00	12:00	14:00	16:00	18:00	20:00	22:00	00:00 Thu Jun 25	02:00	04:00	06:00	08:00
										Time (EDT)								
	Raw Event / sPiow Data																	
D	Detailed event three-event. Max 100000 events.																	
	nt source			ch string				myDev										
5	ecurity Events	0	w •			PDU (exp	ort) format	•	© ,									
1	Time	Event																
>	25/06/2020 08:00:34.221		mp=xe-1.				1.168.100.4 cat=se lle=cns-001040.tim											
>	25/06/2020 08:00:34.221						1.168.100.4 cat-se ile=cns-001040.tim											
>	25/06/2020 08:00:34.221	,dir=inbound	mp=xe-1.	/1,act=detect,	dm=mitigate.p:	c=16,1b=0,ru	1.168.100.4 cat=se ile=cns-001040,tim 163432372e32363233	e=159308641866669										
>	25/06/2020 08:00:34.221	Jun 25 08:00 ,dir=inbound d0193da1c,	:34 127.) ,mp=xe=1.	0.0.1 2020-06- /1,act=detect,	25T08:00:34.2 dm=mitigate,p	21-04:00 192 c=16,1b=0,ru	1.168.100.4 cat=se ile=cns-001040,tim	curity,type=event e=159308641866666	,v=1,cl=WebOemo 4,plen=66,icn+6	,device=WebDemoN ,scl=0,pdu=000c2	TD,profile="Core 9b5f616000c29133	ro SW Demo",aip c0b080045000034	=192.168.100.201 0d4d40004006ccc	l,fp=0,prot=6,ipv Fac100447ac100448	=4,sip=172.16.4 b958145112e383	1.71,sprt=47448,c 531e307c9801000e	ip=172.16.4.72.dp 5e75000000101080a	ort=5201 1255c8ee
>	25/06/2020 08:00:34.221		mp=xe-1.	/1,act=detect,			1.168.100.4 cat=se ile=cns-001040,tim											
>	25/06/2020 07:03:33.221	24834,dir=in 0000000000000	bound, mp 12bd01ac	=xe-1/1,act=b1 6d761588f70000	ock,dm=mitiga 0001754e07020	te,px=14,1b=	1.168.100.4 cat=set 1,rule=cns-002033 00000000000000000000000000000000	time=15930829969	42344,plen=482, 00000000000000000	icn=5,scl=0,pdu= 000000000000000000	000c291f24bc000c	2935b98a0800450	001d49c110000f91	12c786fc5d768ac1	00451076c61020	c076f5d720032a00	06004800000000000	00000000
>	25/06/2020 07:03:33.221	3114, dir=inb 000000000000	ound, np+: 2bd01ac6	xe-1/1,act=blo d761588f700000	ck,dm=mitigat 001754e070200	e,px=13,1b=1	168.100.4 cat=set ,rule=cns-002033; 00000000000000000000000000000000	time=1593082996943 000000000000000000000	2352,plen=482,i	cn+5,scl=0,pdu+0	00c291f24bc000c2	96417a008004500	01d4d0ed00004611	b435757bc819ac10	0451076c333a01i	:0ae56d720032a000	600480000000000000	00000000

Events include all the metadata extracted by the SmartWall system as well as the first 128 bytes of the packet which the attack comprised of. In addition, PDU data from security and sFlow events can be extracted to a file for import to third-party applications, such as Wireshark for further forensic analysis.



Open Integration

SecureWatch Analytics (SWA) leverages the APIs and JSON formatted syslog event feeds of SmartWall's open architecture to deliver forensic-level attack analysis and closed-loop autonomic protection. It is built on top of a self-contained Splunk instance, which is included with every SmartWall soliution, to deliver its powerful, flexible and easily customisable attack analysis and reporting.

Users with their own Splunk Enteprise instance can leverage that directly by running the SWA application on it and consuming the SmartWall feeds directly. Users with alternate an SIEM or other security platforms can directly consume the SmartWall JSON formatted syslog feed which delivers all the same detailed information which is available from SWA.

Technical Specifications

Management

Web-Based GUI HTTPS Access through Portal Login Page Programmatic API JSON-Based REST Secure Authentication Role-Based Access via LDAP

Physical Environment

Hypervisors

KVM Running on RedHat Enterprise 7+, CentOS 7+ or Ubuntu 16.04+, VMware ESXi 6.5+

Minimum Requirements

12 Cores, 12GB Memory, 400GB Disk

Learn more About SecureWatch Analytics

SecureWatch Analytics was developed with the deep security experience and knowledge of Corero's security analysts that deliver our market leading SecureWatch service. SecureWatch Managed is a comprehensive suite of DDoS configuration optimization, monitoring and response services. As a trusted advisor, Corero extends this security expertise to our customers and partners to better defend against cyber-crime.

To learn more, please visit https://www.corero.com/product/managed-ddosprotection-services/ or contact us at info@corero.com.

About Corero Network Security

Corero is the leader in real-time, high-performance, automatic DDoS defense solutions. Enterprises, Service Providers, Hosting & Co-Location Providers, Edge Providers and the MSSP/MSP's across the globe increasingly rely on Corero's award winning DDoS solutions. Our SmartWall solutions are the highest performing and most accurate in the industry, delivering the most automatic coverage, at scale, with the lowest total cost of ownership.

This, industry leading technology delivers scalable protection capabilities against DDoS attacks in the most complex environments, without the downtime associated with other solutions, while enabling a more cost-effective economic model than previously available. For more information, visit www.corero.com

Contact Us

US Headquarters

293 Boston Post Road West Suite 310 Marlborough, MA 01752 Tel: +1 978 212 1500 Web: www.corero.com

EMEA Headquarters

Regus House, Highbridge, Oxford Road Uxbridge, England UB8 1HR, UK Tel: +44 (0) 1895 87657

Scotland Office

53 Hanover St, 3rd Floor Edinburgh, EH2 2PJ, UK Tel: +44 (0) 1895 87657



