First Line of Defense®

SecureWatch® ANALYTICS

corero
FIRST LINE OF DEFENSE

OVERVIEW

KEY BENEFITS

Comprehensive Visibility

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

Proactive Protection

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

Services Capabilities

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

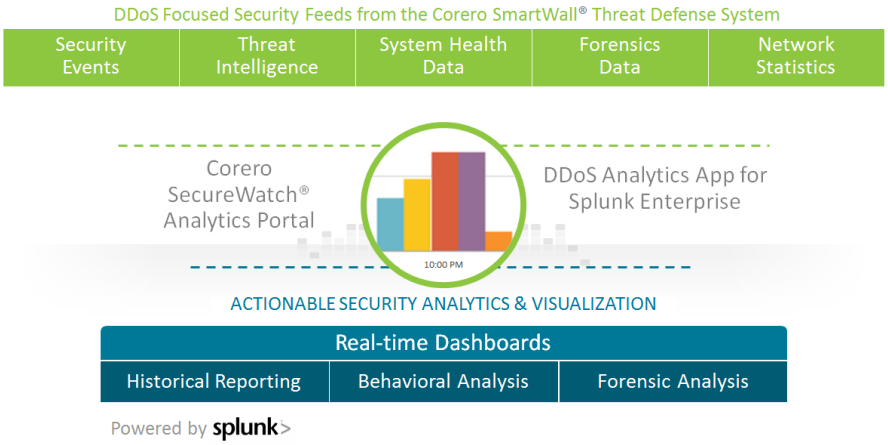
"The ability to uncover hidden patterns of data, identify emerging vulnerabilities within the massive streams of DDoS attack and security event data, and respond decisively with countermeasures, provides our team with the tools required to better protect our organization against the dynamic cyber threat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

SecureWatch® ANALYTICS DASHBOARD

Figure 1 - Network Level Visibility

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.

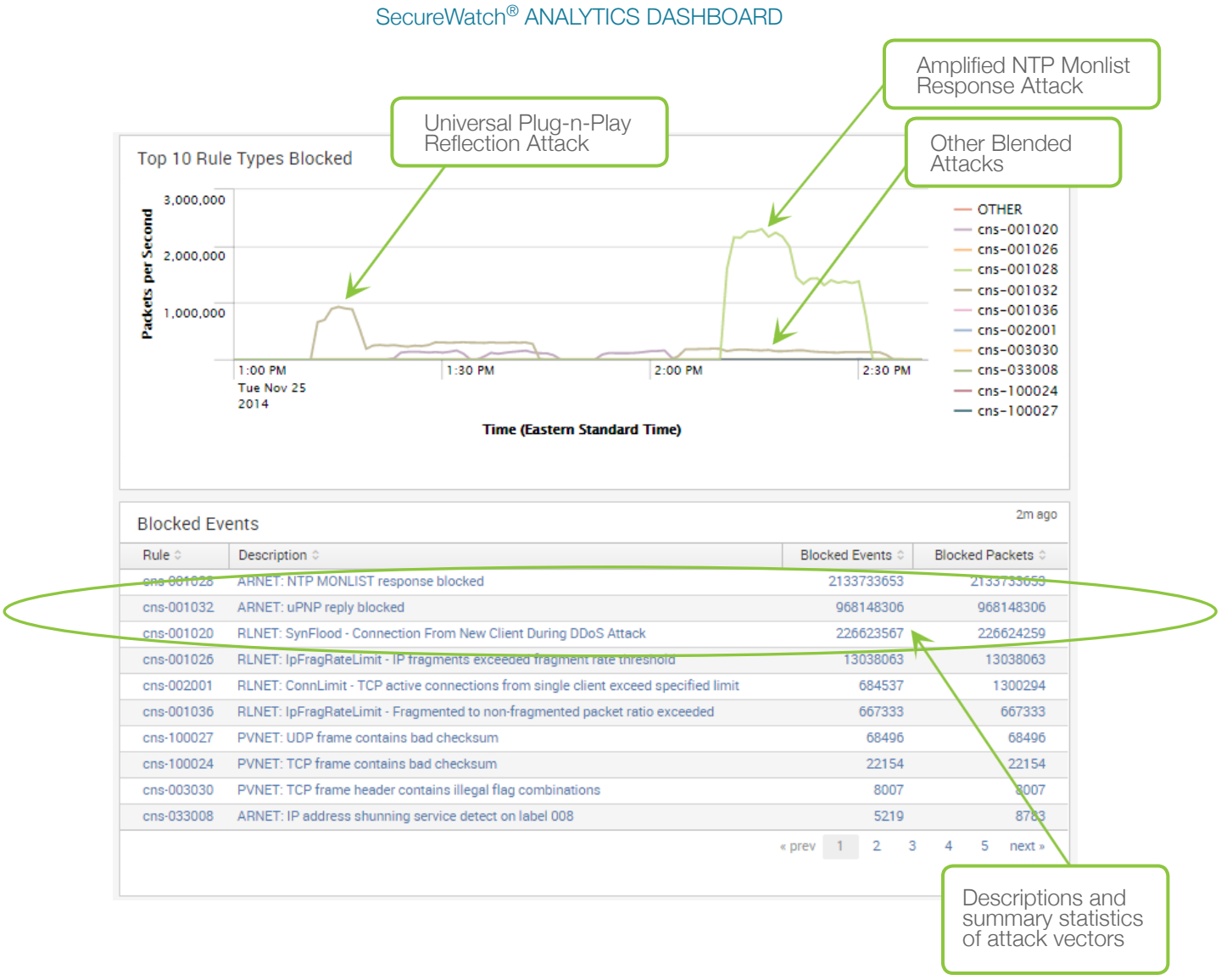


Figure 2 - Multi-vector attack from compromised servers & botnets

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

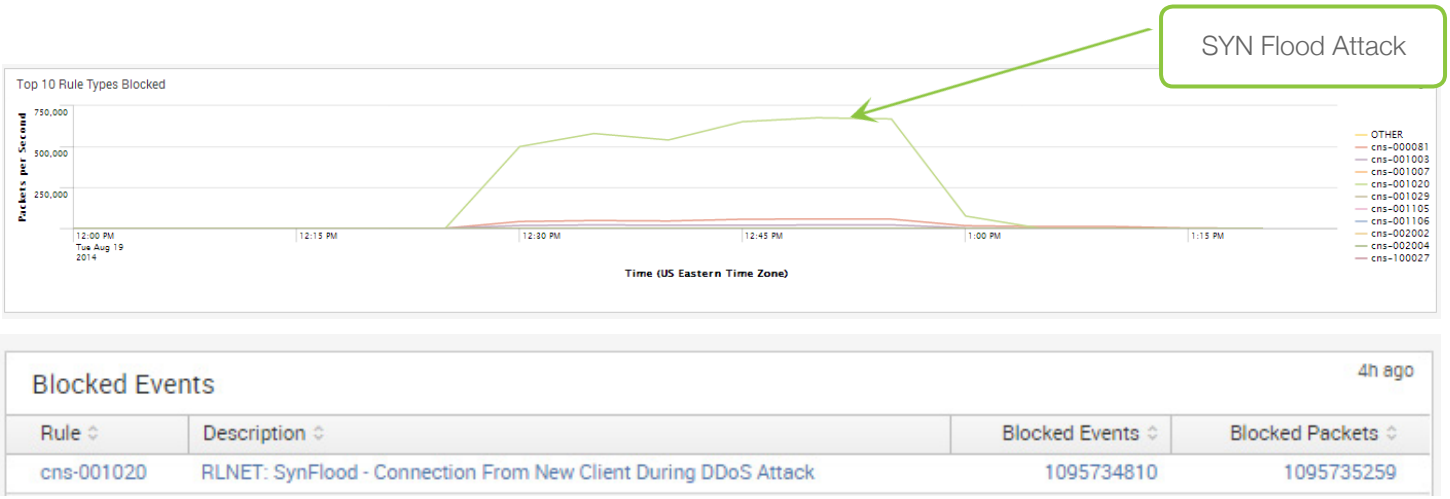


Figure 3 – SYN Flood Attack

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.

SecureWatch® ANALYTICS DASHBOARD

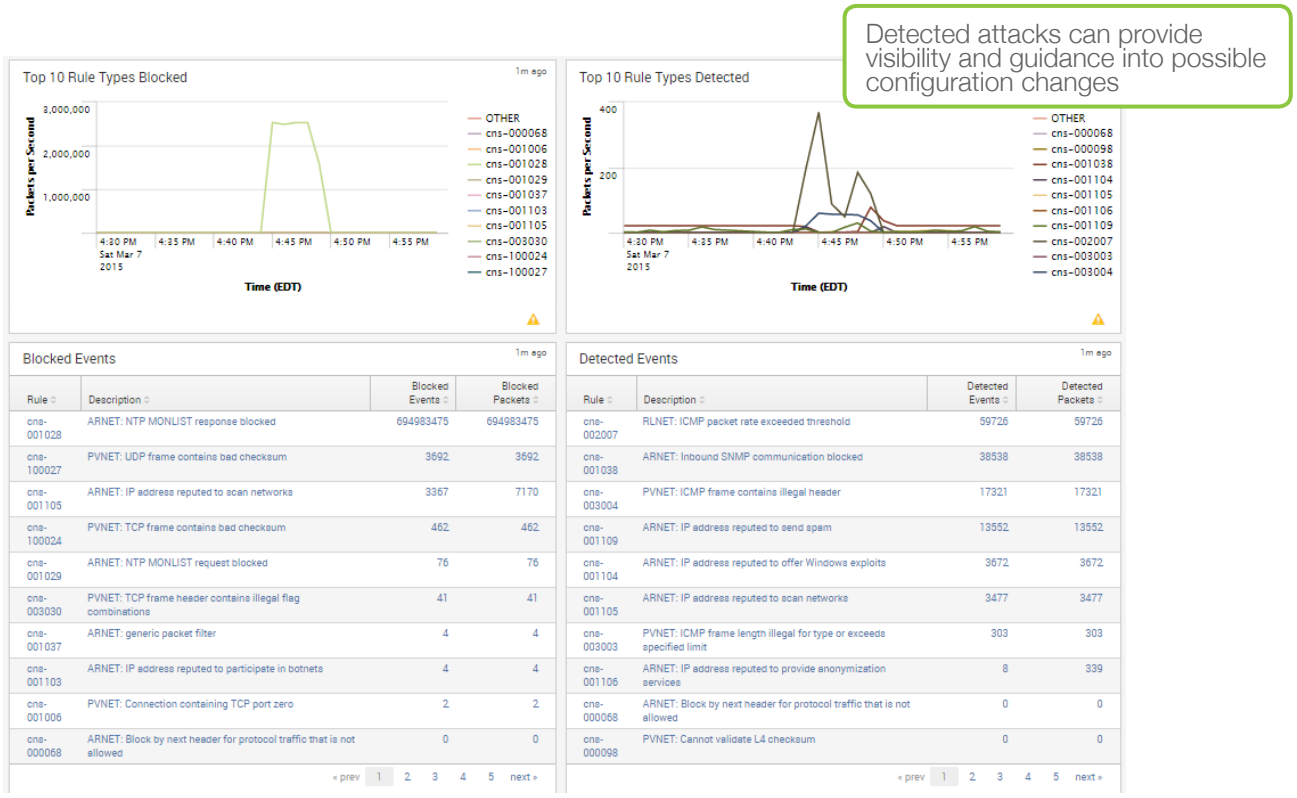


Figure 4 -SecureWatch Analytics provides visibility into both blocked malicious as well as detected suspicious activity

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.

SecureWatch® ANALYTICS DASHBOARD

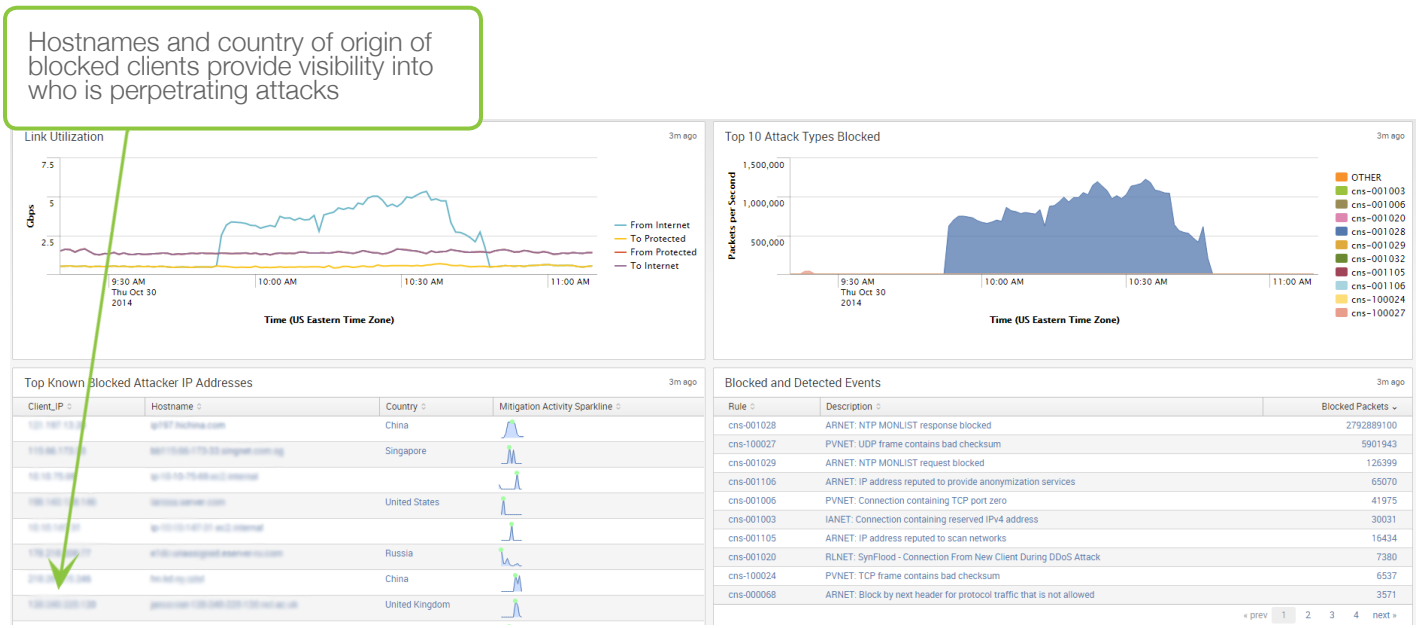


Figure 5 - Attacker visibility

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

Figure 6 - Post level visibility

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

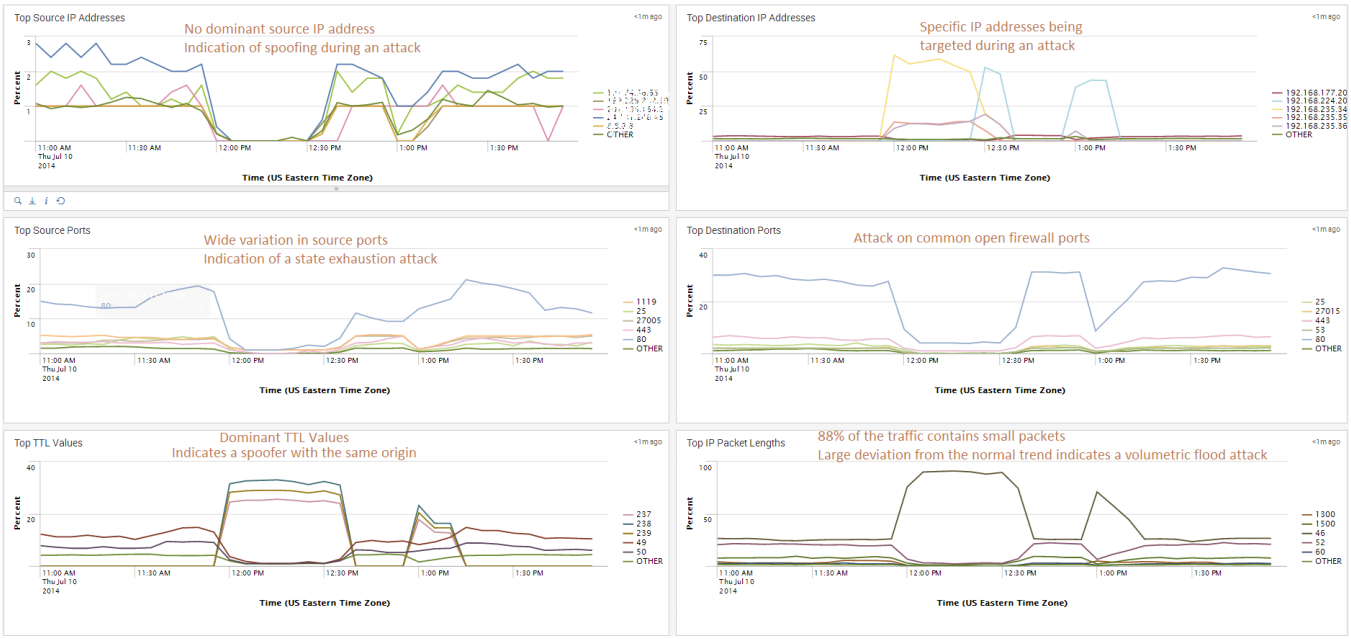


Figure 7 - sFlow statistics provide insight into deviations from normal baseline behavior

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.

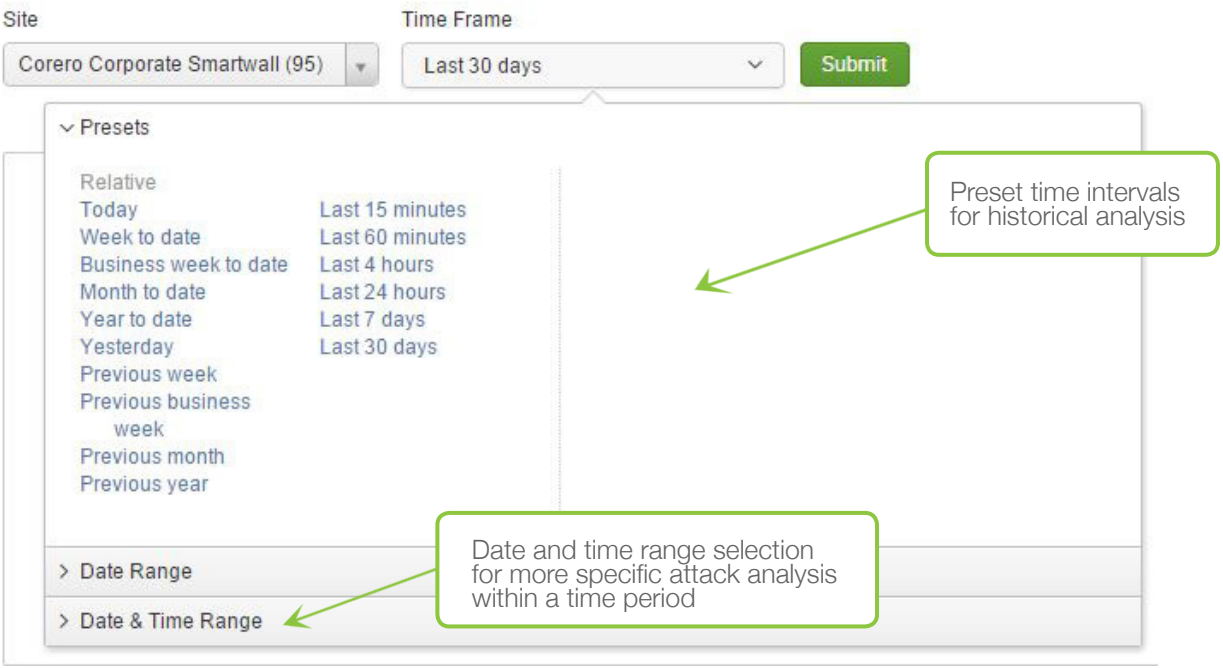
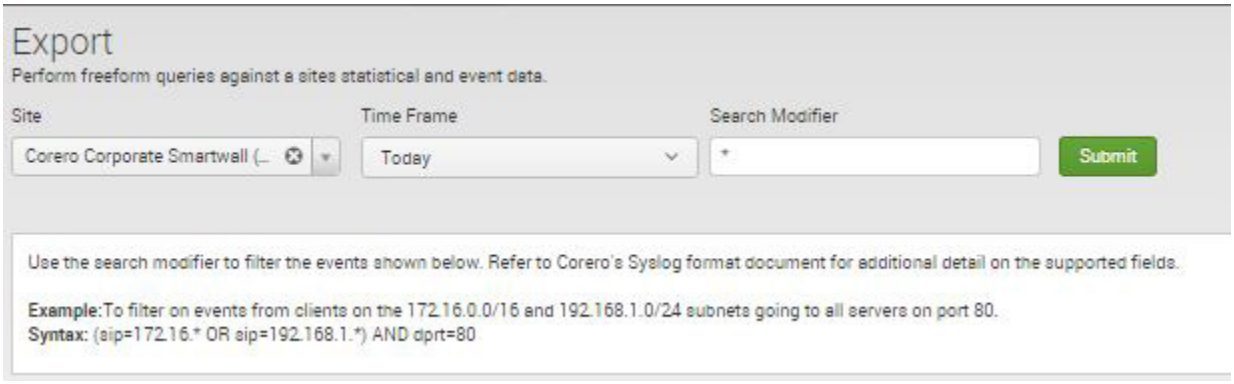


Figure 8 - Historical Report Generation

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.



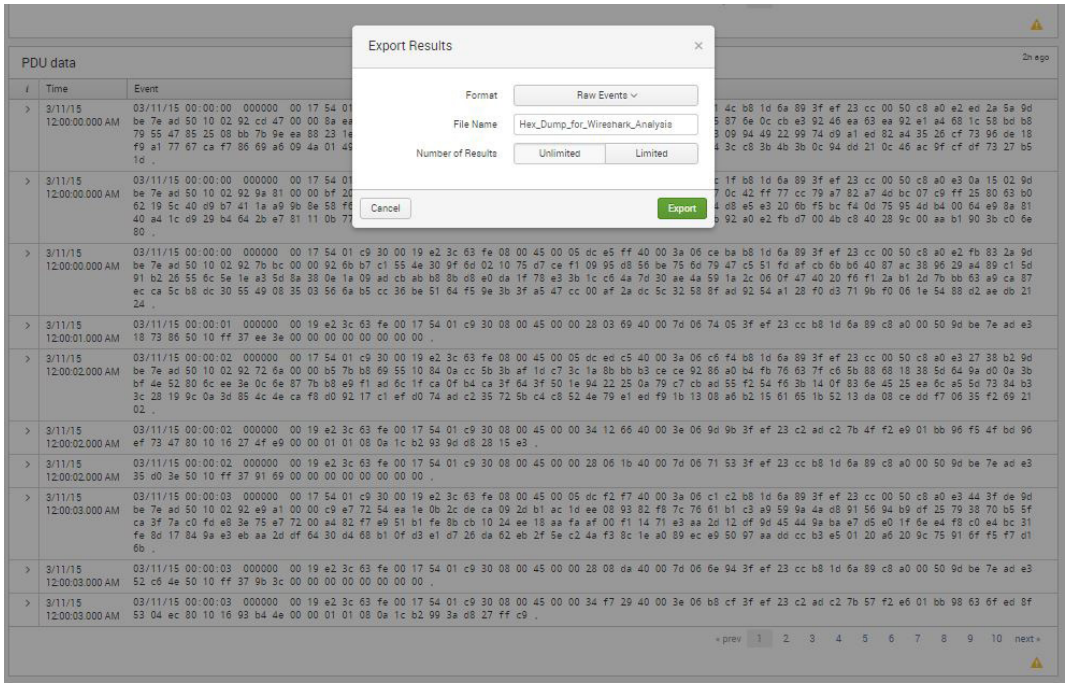


Figure 9 - PCAP Export for Forensic Analysis

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