SOLUTION BRIEF

The Key To Reducing SIEM Alerts and Lost Productivity

DEPLOYMENT SCENARIO: SECURITY ARCHITECTURE

Even with firewalls, intrusion prevention systems (IPS), and a wide array of security tools in place, businesses still miss attacks and suffer major breaches every day. Why? One reason is that the sheer volume of security alerts being generated places a huge processing strain on the security team and the infrastructure itself. According to a Ponemon Institute report[1], security teams at large enterprises waste more than 20,000 hours per year chasing false-positive alerts. In addition, 44% of security alerts are never investigated.[2] This translates into wasted time and money along with an increased risk of falling victim to an attack.

By pre-filtering known bad IP addresses and traffic from untrusted countries, you can stop unwanted traffic from ever reaching the firewall. This prevents your security team from being overwhelmed with attacks as well as security information and event management (SIEM) alerts. By deploying this solution, it is possible to see an up to 80% reduction in SIEM alerts within 24 hours which eliminates countless hours spent investigating each alert to ensure you are not being breached or accidentally blocking legitimate traffic.

SOLUTION COMPONENTS:

- ThreatARMOR
- BreakingPoint
- SIEM
- Firewall

BENEFITS

- Reduce the volume of unnecessary SIEM alerts by up to 80%
- Inspect more potential security threats
- Increase internal productivity and reduce costs

[1] The Cost of Malware Containment. Ponnemon Institute. January 2015.
[2] Cisco 2017 Annual Cybersecurity Report. Cisco, 2017.

ixia
A Keysight Business

915-8191-01-8071 Rev A

SOLUTION OVERVIEW

This solution allows you to:

- Validate firewall performance
- Validate the total number of SIEM alerts received without ThreatARMOR
- Validate a reduction in SIEM alerts after deploying ThreatARMOR

Pre-filtering known bad IP addresses and traffic from untrusted countries can stop unwanted traffic from ever reaching the firewall.

WHAT ARE THREAT INTELLIGENCE GATEWAYS

Threat intelligence gateways are devices that screen incoming and outgoing traffic based upon IP address. By pre-filtering known bad IP addresses and traffic from untrusted countries, you can stop unwanted traffic from ever reaching the firewall. This includes detecting infected systems to thwart outbound connections from botnets, phishing scams, and malware exploits. Blocking large volumes of traffic based on IP address, location, and bad behavior enhances your security architecture performance, and reduces your team's "alert fatigue." You can use threat intelligence gateways for either blacklisting or whitelisting security architectures.

VALIDATION OF SIEM ALERT REDUCTION & OPTIMIZATION

To validate the efficacy of this solution, Ixia's ThreatARMOR product is deployed with a firewall, SIEM, and BreakingPoint.

Here is the basic process to validate that your network is protected:

1. Install the Ixia ThreatARMOR product, firewall, SIEM and BreakingPoint in a lab
2. Place ThreatARMOR into the Bypass mode and generate malware traffic using BreakingPoint to attack the firewall
3. Examine results from the firewall, SIEM, and BreakingPoint combination to see how many threats were sent, how many the firewall blocked, and how many the SIEM still observed
4. Place ThreatARMOR in Blocking mode and rerun the test
5. Compare results again from the ThreatARMOR, firewall, SIEM, and BreakingPoint combination to see how many threats were sent, how many the firewall blocked, and how many the SIEM observed now

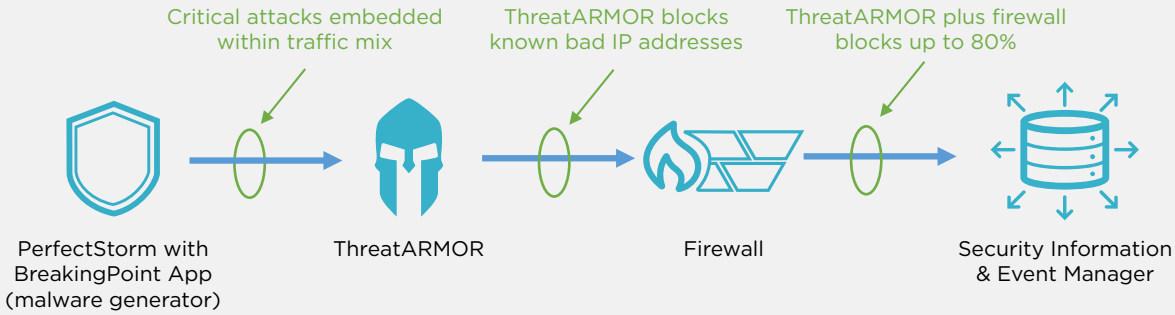
The ThreatARMOR dashboard will provide the aggregate number of communications to bad IP addresses and what was stopped. In addition, details of the IP addresses that were blocked by the system are presented along with the reason why the address was blocked.

While results will vary depending upon the firewall and SIEM combinations deployed, Ixia has seen that a combination of ThreatARMOR with a firewall can reduce SIEM alerts and missed attacks by over 80%.

Pre-filtering known bad IP addresses and traffic from untrusted countries can stop unwanted traffic from ever reaching the firewall.

Figure 1

Configuration Set-Up



SUMMARY

Pre-filtering known bad IP addresses and traffic from untrusted countries is a powerful tool in the war against malware. This pre-filtering creates a first line of defense that stops a huge amount of traffic from ever reaching your firewall. This has the trickle-down effect of dramatically reducing the amount of SIEM alerts that are generated. Once the SIEM alerts are reduced to a manageable number, the IT department has more time to spend investigating each alert to eliminate threats and increase their alert resolution metrics.

Unlike most firewalls, the ThreatARMOR product is continually updated with known bad IP addresses automatically. This saves the IT department a significant amount of time as they don't have to manually update access control lists in the firewall as bad actors hop from one new IP address to another.

SECURITY SOLUTIONS FROM IXIA

Ixia provides various network security solutions including BreakingPoint, ThreatARMOR, PerfectStorm, and Inline and Out-of-Band Network Packet Brokers.

IXIA WORLDWIDE

26601 W. Agoura Road
Calabasas, CA 91302

(Toll Free North America)
1.877.367.4942

(Outside North America)
+1.818.871.1800

(Fax) 1.818.871.1805

www.ixiacom.com

IXIA EUROPE

Clarion House, Norreys Drive
Maidenhead SL64FL
United Kingdom

Sales +44.1628.408750
(Fax) +44.1628.639916

IXIA ASIA PACIFIC

101 Thomson Road,
#29-04/05 United Square,
Singapore 307591

Sales +65.6332.0125
(Fax) +65.6332.0127