Technical Validation

CleanINTERNET by Centripetal

Operationalizing Advanced Threat Intelligence

By Alex Arcilla, Senior Validation Analyst

June 2022

This ESG Technical Validation was commissioned by Centripetal Networks, Inc. and is distributed under license from TechTarget, Inc.

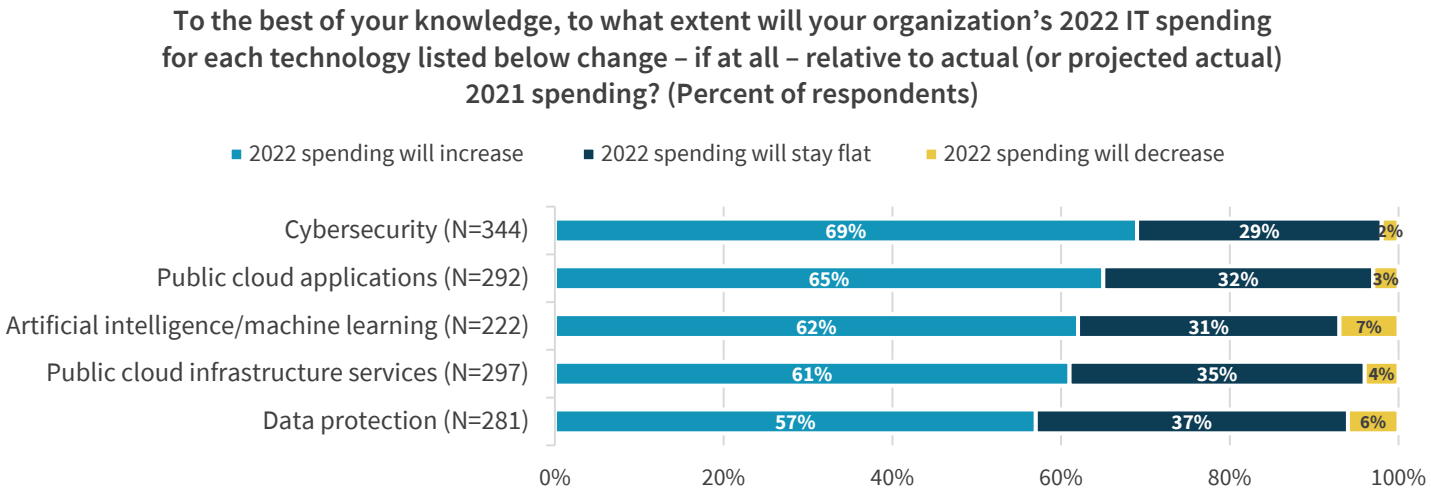
Introduction

This ESG Technical Validation documents our evaluation of CleanINTERNET by Centripetal. We reviewed how the managed security service enables organizations to quickly establish a zero trust security posture (i.e., no network communication is trusted without proper validation) with minimal impact to existing business operations.

Background

ESG research has uncovered that cybersecurity remains a key investment priority, as a recent survey revealed that 69% of respondents will spend more money on strengthening their internal cybersecurity capabilities in 2022 compared to 2021 (see Figure 1).[1] Amongst those areas of cybersecurity, ESG also found that 55% of respondents will increase their spending to bolster their network security capabilities.

Figure 1. Change in 2022 Spending by Technology compared to 2021



Source: ESG, a division of TechTarget, Inc.

Ensuring network security has typically involved using firewalls, router ACLs, IDS, and DPI to allow or block traffic based on a small number of criteria, such as IP address, CIDR, domain name, or signature. However, these technologies have not been designed, either individually or in combination, to deal effectively with today's threats and attack patterns.

Securing network traffic has typically relied on screening traffic based on specific characteristics of known threats and attacks. However, today's cybersecurity events have increased in both volume and complexity. Exacerbating the issue is the fact that organizations are "flying blind" as they deal with unknown threats. Organizations typically rely on a set of indicators of compromise (IOCs) to detect potential threats. While an IOC may initially show that a possible threat may be low risk, the threat posed by that same IOC can evolve and reveal a potential high-risk threat capable of damaging business operations.

Alternatively, an organization can choose to develop a zero trust security posture that would mitigate evolving threats along a risk continuum. However, establishing this posture is no small feat. The time and effort needed to curate and understand IOCs sourced by cyber threat intelligence (CTI) providers, create and update policies continuously using those IOCs, and prioritize those events to be remediated require significant investments in separate tools, integration efforts between multiple platforms, skills development, and cybersecurity professionals.

[1] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021. All ESG research references and charts in this ESG Technical Validation have been taken from this survey results set, unless otherwise noted.

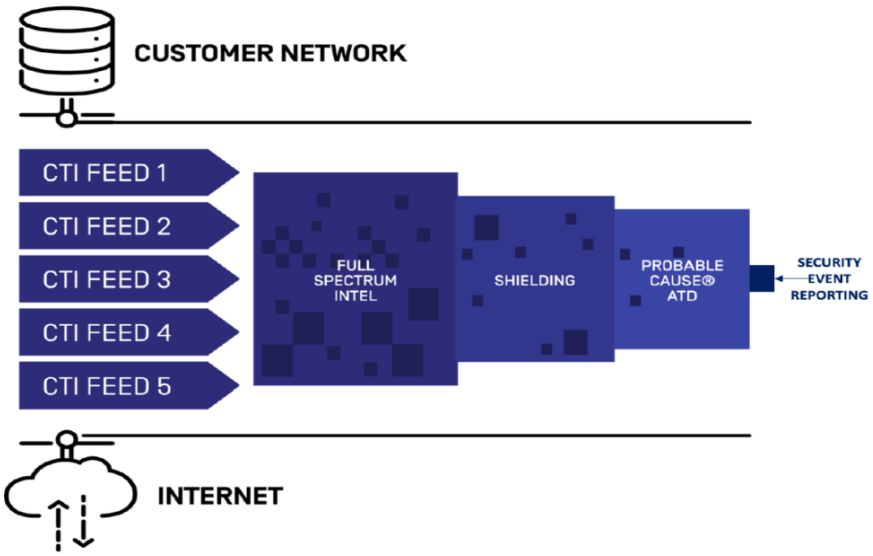
CleanINTERNET by Centripetal

Centripetal has designed the CleanINTERNET solution to provide organizations with continuous threat-intelligence-based defense against known and unknown threats and attacks. CleanINTERNET operates as a network-security-as-a-service (NSaaS) to help organizations enforce dynamically updated rules and policies against incoming and outgoing network traffic from any internet connection.

CleanINTERNET helps organizations' cyber defenses adapt to the dynamic nature of potential threats and attacks, regardless of their security risk level. By enforcing a sequence of dynamic policies that are composed of packet filtering rules derived from dynamic threat intelligence, CleanINTERNET triages an organization's threat events down to those events that need to be addressed proactively before damage occurs. CleanINTERNET can be tailored for any organization and its risk profile, regardless of industry segment or vertical.

Figure 2 illustrates how CleanINTERNET triages network traffic for threats to arrive at a focused set of actionable insights, then enforces a zero trust security posture.

Figure 2. CleanINTERNET by Centripetal



Source: Centripetal Networks, Inc.

The CleanINTERNET managed service:

- Ingests billions of unique threats from thousands of CTI feeds supplied by hundreds of global CTI providers. Working with multiple CTI providers[2] enables Centripetal to capture the unique, malicious IOCs associated with active internet threats.
- Maximizes intel coverage with an open framework for CTI provider integration, as no single provider provides complete coverage.
- Creates and automatically updates zero trust network security policies composed of millions of packet filtering rules. These policies, which are customized for each organization, are applied to network traffic by the RuleGATE platform, a threat intelligence gateway designed to filter and process network packets at line rates up to 100Gb/s. The RuleGATE filters out (i.e., shields against) or monitors all packets that contain IOCs, as such packets may present business- or mission-critical risk. Since Centripetal refreshes its filtering rules with frequently updated CTI data, new policies are

[2] One CTI provider can potentially supply hundreds of CTI feeds.

created and immediately replace existing policies residing on a RuleGATE without degrading network performance, yet still providing zero trust protections.[3]

- **Performs secondary inspection and advanced threat detection (ATD) on suspect network packets with ProbableCause threat-analysis technologies.** ProbableCause technologies couple intelligence risk assessment with intensive inspection (combining IDS, DPI, packet capture (PCAP), and safe decryption of network communications) to correlate network traffic patterns and prioritize and triage risky communications.
- **Prioritizes events that a customer should examine and address immediately to reduce business risk with AI-Analyst**, an artificially intelligent machine cybersecurity analyst.

CleanINTERNET focuses organizations on remediating security events that will most likely cause network security breaches while shielding the organization from possible risk threat communications (e.g., dropping packets). The CleanINTERNET managed service removes the burden of building and managing a zero trust network security posture in-house by seamlessly integrating multiple technologies and CTI feeds. Since this effort requires both investment in disjointed tools, integration efforts, and a staff of cybersecurity analysts, organizations avoid both unnecessary capital and operational expenses.

ESG Technical Validation

ESG evaluated CleanINTERNET via remote demonstrations conducted in Portsmouth, NH, and Atlanta, GA, with the goal of assessing how the solution can help organizations maximize IOC coverage sourced by hundreds of CTI providers, maintain network performance when processing millions of IOCs against network packet traffic, identify and triage most relevant risks to the business, and minimize an organization's security event workload.

Maximizing IOC Coverage

To achieve zero trust, organizations require hundreds of CTI providers but face the challenge of tracking and analyzing millions of IOCS from thousands of CTI feeds that are updated regularly with new intelligence. Such a large number of CTI providers is complex to manage, challenging to consume, and expensive to purchase.

Because Centripetal uses approximately 100 CTI providers to gain maximum coverage of millions of IOCs associated with active internet threats, organizations no longer have to manage and consume CTI from large numbers of providers to begin establishing a zero trust security posture. Centripetal maximizes IOC coverage to enable zero trust security postures for all customers.

ESG Testing

ESG audited data provided by Centripetal to determine how it maximizes IOC coverage. To verify that using a large number of CTI providers is ideal for establishing a zero trust security posture, we reviewed existing reports and estimated the volume and percentage of actionable IOCs by type—IPv4 address, IPv4 address range, domain name, URL—that are provided by the 100+ CTI providers used by Centripetal. Summary data in Table 1 shows the percentage of IOCs (by type) that are unique to one provider, two providers, etc.

[3] Centripetal employs its own cybersecurity analysts to refine and curate these rules and policies.

Table 1. Summary Data from over 100 Global CTI Providers included in CleanINTERNET

	IP-Coverage (%)	Domain-Coverage (%)	URL-Coverage (%)
Zero trust coverage IOCs sourced by only one provider	81.75	94.26	99.43
Zero trust coverage IOCs sourced by only two providers	12.35	5.16	0.53
Zero trust coverage IOCs sourced by only three providers	2.96	0.54	0.04
Zero trust coverage IOCs sourced by four providers	1.15	0.03	0
Zero trust coverage IOCs sourced by five providers	0.66	0	0
Zero trust coverage IOCs sourced by six providers	0.47	0	0
Zero trust coverage IOCs sourced by seven providers	0.28	0	0
Zero trust coverage IOCs sourced by eight providers	0.15	0	0
Zero trust coverage IOCs sourced by nine providers	0.09	0	0
Zero trust coverage IOCs sourced by 10+ providers	0.13	0	0

Source: ESG, a division of TechTarget, Inc.

Based on data ESG reviewed, we saw that the 100+ CTI providers used by Centripetal supplied approximately 350 million actionable malicious IOCs, which translated into approximately 750 million unique IOCs. However, based on the data in Table 1, ESG observed that no single CTI provider supplied more than a few (i.e., single digit) percentage points of the total aggregate of IOCs. The data also revealed that minimal overlap of IOCs existed.

By examining this data, ESG saw how each additional CTI provider supplied incremental, yet unique, IOC coverage to support the creation of packet filtering rules for enforcing zero trust policies. ESG could see how using a large number of CTI providers helps to ensure good coverage of the active internet threat surface and capture the latest, up-to-date IOCs to develop appropriate policies supporting zero trust postures.

Why This Matters

A zero trust security posture requires that an organization tracks and mitigates every single IOC associated with an active internet threat. While many CTI providers exist to provide this IOC data, no one provider supplies more than a small percentage of relevant IOCs. Furthermore, little IOC overlap exists between CTI providers. However, organizations do not typically have the time, resources, or budget to purchase services from and manage the necessary number of CTI providers let alone track and analyze large numbers of highly dynamic CTI feeds to establish a zero trust posture.

ESG validated that CleanINTERNET by Centripetal maximizes its IOC coverage by employing approximately 100 CTI providers to identify and track as many unique and up-to-date IOCs as possible. Because no CTI provider supplies more than a small percentage of the IOCs comprising the active internet threat surface, we saw the value of using many CTI providers to achieve a zero trust posture.

Maintaining Network Performance

Processing in-line packet traffic against such large numbers (e.g., tens of millions) of stateless packet filtering rules and swapping the associated policies on a single network firewall can negatively impact network performance, such as by dropping packets and introducing unacceptable latency. If network performance degrades, organizations risk not meeting business-critical needs. CleanINTERNET has been designed to easily scale the number of rules, filter network traffic, and dynamically swap policies without sacrificing network performance, thus maintaining a zero trust security posture.

ESG Testing

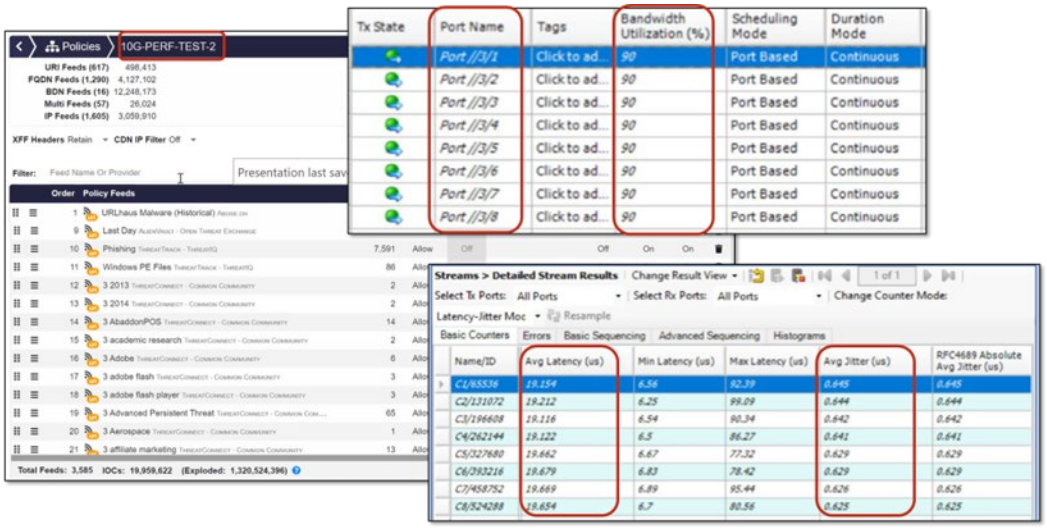
ESG began by observing how the Centripetal RuleGATE maintains network performance when using massively scaled, dynamically swapped policies to filter out network traffic that may pose a security risk. To observe performance, we used a Spirent Test Center to generate bi-directional traffic that continuously ran through all four pairs of 10G ports on a

RuleGATE appliance. Utilization on each port was at 90%. The Global RuleGATE Manager application was used to create zero-trust policies, distribute them to the RuleGATE appliance, and signal the RuleGATE to enforce the policies on the traffic.

ESG first observed the effects of swapping large numbers of policies on network performance, specifically the average latency, jitter, and packet loss. Using the Global RuleGATE Manager, a first policy named "10G-PERF-TEST-1" was initially enforced. This policy contained 20 million IOCs, which translates to 20 million unique packet filtering rules and over one billion granular IOCs,[4] characterized by details such as IP address, domain name, or URI, from 3,585 cyber-threat intelligence feeds. After 10 minutes, the first policy was swapped out with another policy named "10G-PERF-TEST-2",[5] containing a different set of 20 million unique packet filtering rules from the same feeds (see Figure 3). Traffic was generated for another 10 minutes.

ESG then navigated to the Spirent Test Center and verified that at 90% bandwidth utilization on all eight ports, and an aggregate traffic load of 144Gb/s, the average latency measured on each port was 18-19 microseconds, while the average jitter was approximately 0.6 microseconds (see Figure 3).

Figure 3. Low Latency and Jitter Associated with Swapping Large Policies on RuleGATE

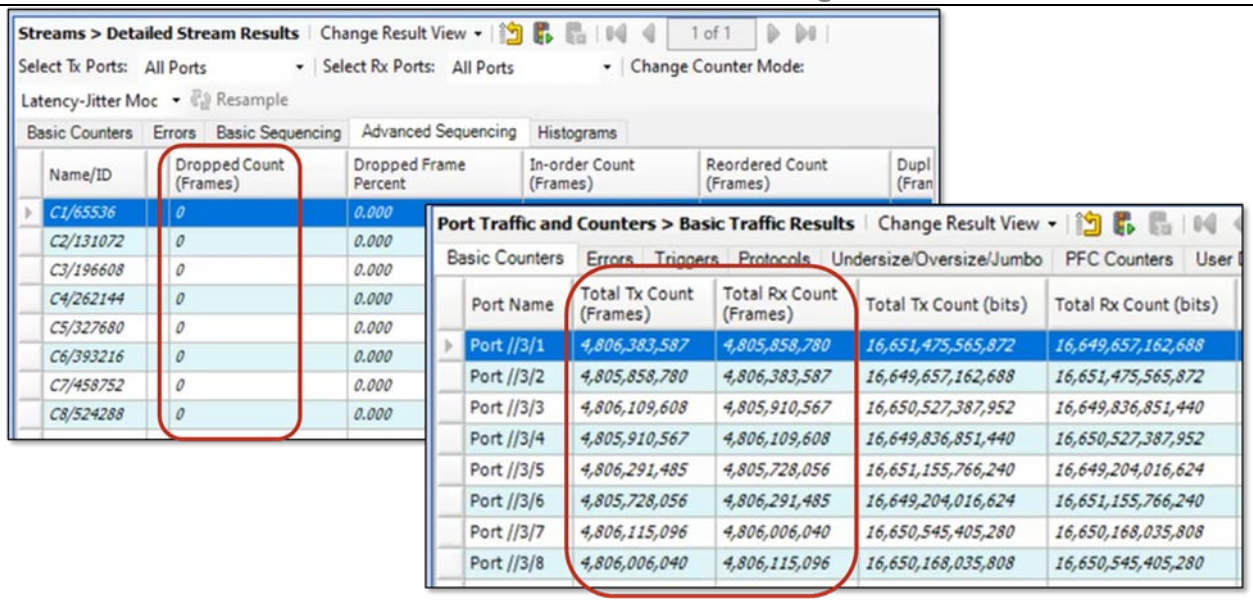


Source: ESG, a division of TechTarget, Inc.

To determine if any packet loss occurred, ESG stopped the Spirent Traffic Center from generating traffic. As shown in Figure 4, we viewed that the number of frames transmitted and received on each port pair was equal. Accordingly, no frames were dropped.

[4] The 10G-PERF-TEST-1 policy set contained approximately 1.3 billion unique IOCs, when considering every IPv4 address represented by CIDRs.
[5] The 10G-PERF-TEST-2 policy set contained approximately 1.3 billion unique IOCs, updated with refreshed data.

Figure 4. No Packet Loss Observed When Traffic Ceased to Run though RuleGATE



Source: ESG, a division of TechTarget, Inc.

What the Numbers Mean

- Because latency and jitter were extremely low, at 90% bandwidth utilization on each 10G port, ESG verified that CleanINTERNET can process and filter traffic against large policies containing millions of IOCs and rules without adversely impacting network performance. (We note that bandwidth utilization in production networks typically averages less than 90%).

- Observing that CleanINTERNET does not drop network packets when swapping out policies, ESG noted that organizations do not risk losing any business-critical traffic. More importantly, since CleanINTERNET is designed to automatically update policies on the RuleGATE, organizations can maintain a zero trust posture without any gaps in coverage.

- Alternatively, traditional network firewalls and router access control lists (ACLs) cannot effectively deal with the volume and rate of dynamically changing CTI. Both firewalls and ACLs do not scale to establish a zero trust posture, as they can only enforce a limited number of packet filtering rules, typically up to the tens of thousands range (compared to the billions of unique IOCs required for zero trust). As that limit is reached, network performance degrades.

- Swapping out packet filtering rules on firewalls and ACLs is typically a manual and time-consuming process, which can create a security gap and compromise an organization's security posture. Since CleanINTERNET has been designed to swap out policies automatically, ESG can see how no security gaps are incurred as rules are swapped out.

Why This Matters

Establishing a zero trust network security posture requires that every network packet be scrutinized. However, traditional methods, specifically firewalls and router ACLs, cannot effectively filter and process all network traffic against a continuously growing and evolving zero-trust policy without adversely affecting network performance.

ESG validated that CleanINTERNET by Centripetal can help organizations establish a zero trust network security posture without compromising network performance. We observed how CleanINTERNET can filter and analyze network traffic without incurring excessive latency, jitter, or packet loss. This was especially notable as ESG observed how performance did not degrade as CleanINTERNET swapped out and automatically updated its zero trust policies with refreshed CTI and corresponding packet filtering rules.

Identifying Most Relevant Security Events

In addition to firewalls and router ACLs, organizations have used other technologies, such as IDS, DPI, packet capture (PCAP), and decryption, as additional tools for detecting "bad" internet communications traffic. Yet, the typical amount of network traffic may overwhelm these technologies, leaving organizations unable to prioritize which events truly warrant further investigation. On the other hand, Centripetal's ProbableCause technologies, which are integrated on the RuleGATE, reduce the volume of network traffic to be processed for security events by using CTI to identify and process only those targeted events that are most likely to cause a security breach.

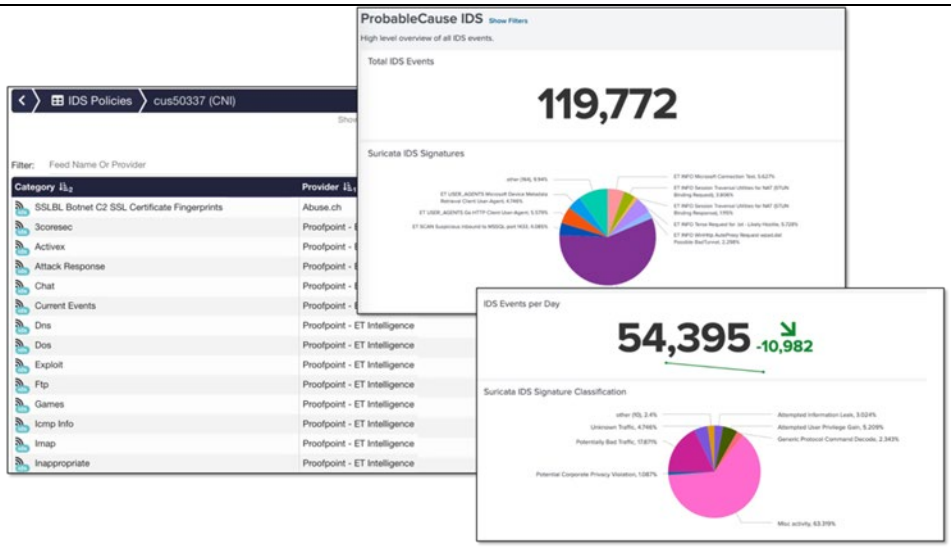
ESG Testing

With the goal of verifying how ProbableCause technology efficiently determines threat events most likely to cause a security breach, ESG first navigated to the ProbableCause IDS module (see Figure 5). We observed that CleanINTERNET can leverage multiple Suricata[6] IDS rules and process network packets quickly. In this example, ProbableCause IDS was working with 50,000+ unique rules. We noted that traditional IDS solutions cannot maintain acceptable levels of network performance when processing traffic against thousands of rules.

Because CleanINTERNET filtered out all traffic that did not match the current threat intelligence, ESG noted the lower average number of events processed by the ProbableCause IDS. Should an organization use its own IDS on all network traffic, the amount of noise (e.g., false positives) could have inflated those numbers displayed in Figure 5.

[6] Suricata is an independent open source threat detection engine.

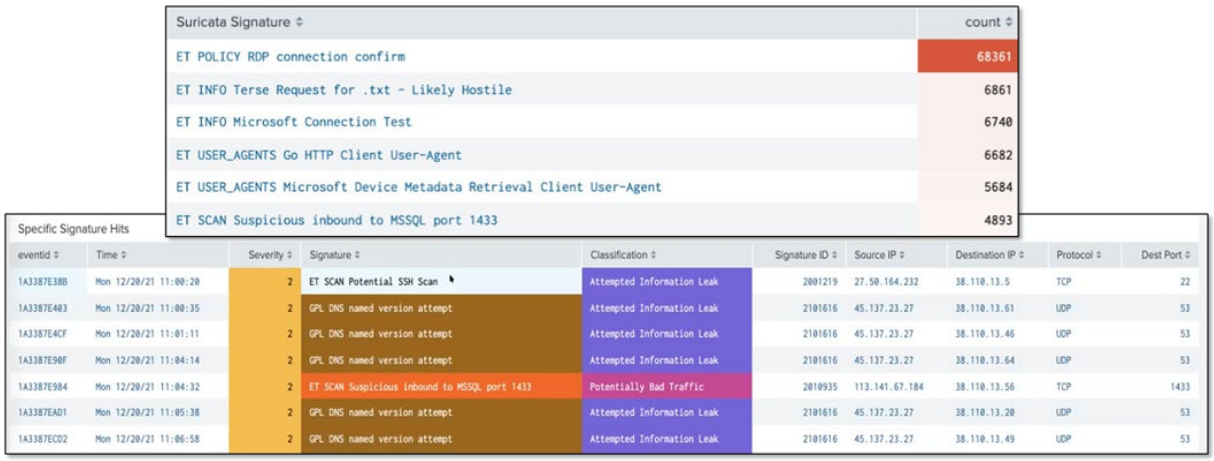
Figure 5. ProbableCause – IDS: Use of Suricata Rules and IDS Dashboard



Source: ESG, a division of TechTarget, Inc.

ESG also observed that ProbableCause provides detailed information about recent IDS scans. Details included the number of times an IDS rule was invoked and specific signature hits (see Figure 6). With this additional detail, we noted that CleanINTERNET analysts could guide customers, specifically those involved with incident response (IR), on those scans representing suspicious activity. For example, an RDP-focused signature could indicate that either a legitimate user or bad actor is attempting to access networks. Given the number of times that rule was invoked, this specific event may warrant extra attention. Additional detail to examine could include the specific signature hits (bottom of Figure 6) to add additional context to the signature counts, such as SSH scans, severity score, and source and destination IP addresses.

Figure 6. Details about Most Recent IDS Scan



Suricata Signature	count
ET POLICY RDP connection confirm	68361
ET INFO Terse Request for .txt - Likely Hostile	6861
ET INFO Microsoft Connection Test	6740
ET USER_AGENTS Go HTTP Client User-Agent	6682
ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	5684
ET SCAN Suspicious inbound to MSSQL port 1433	4893

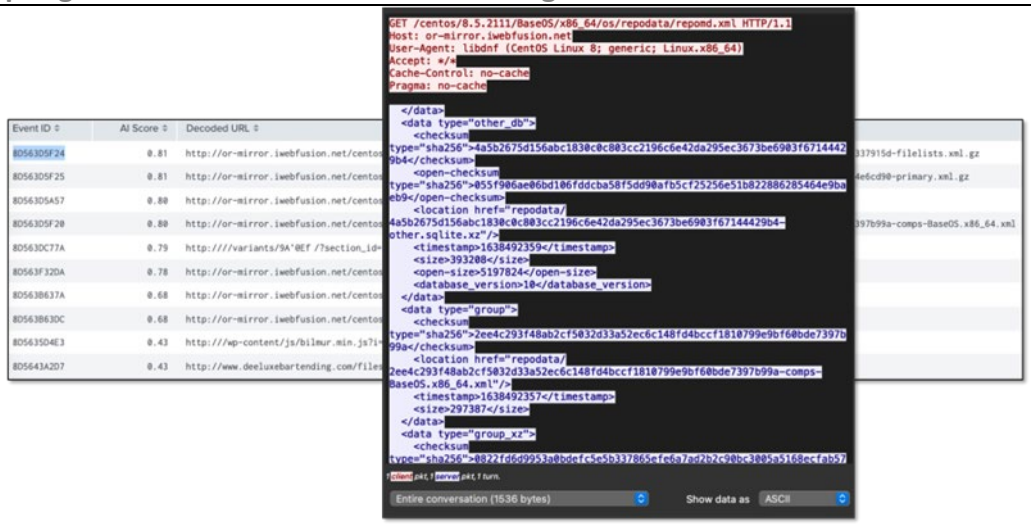
Specific Signature Hits

eventid	Time	Severity	Signature	Classification	Signature ID	Source IP	Destination IP	Protocol	Dest Port
1A3387E38B	Mon 12/20/21 11:00:20	2	ET SCAN Potential SSH Scan	Attempted Information Leak	2001219	27.50.164.232	38.110.13.5	TCP	22
1A3387E403	Mon 12/20/21 11:00:35	2	GPL DNS named version attempt	Attempted Information Leak	2101616	45.137.23.27	38.110.13.61	UDP	53
1A3387E4CF	Mon 12/20/21 11:01:11	2	GPL DNS named version attempt	Attempted Information Leak	2101616	45.137.23.27	38.110.13.46	UDP	53
1A3387E90F	Mon 12/20/21 11:04:14	2	GPL DNS named version attempt	Attempted Information Leak	2101616	45.137.23.27	38.110.13.64	UDP	53
1A3387E984	Mon 12/20/21 11:04:32	2	ET SCAN Suspicious inbound to MSSQL port 1433	Potentially Bad Traffic	2010935	113.141.67.184	38.110.13.56	TCP	1433
1A3387EAD1	Mon 12/20/21 11:05:38	2	GPL DNS named version attempt	Attempted Information Leak	2101616	45.137.23.27	38.110.13.20	UDP	53
1A3387ECD2	Mon 12/20/21 11:06:58	2	GPL DNS named version attempt	Attempted Information Leak	2101616	45.137.23.27	38.110.13.49	UDP	53

Source: ESG, a division of TechTarget, Inc.

ESG then reviewed the decryption capabilities within ProbableCause for decrypting, filtering, and packet-capturing TLS-secured communications (e.g., HTTPS sessions). We saw the list of decrypted HTTPS threat events already identified by the RuleGATE. To examine the decrypted information associated with a specific event (downloading an .XML file via HTTPS) we simply noted the EventID and accessed the Global RuleGATE Manager to download and view the PCAP file almost immediately (see Figure 7).

Figure 7. Decrypting HTTPS Threat Events and Examining PCAP



Source: ESG, a division of TechTarget, Inc.

We should note that obtaining PCAP information in organizations not using CleanINTERNET does not occur as quickly and seamlessly as we observed. Instead, incident responders would have to access multiple tools and consult with other internal groups to obtain the PCAP. The brief time that CleanINTERNET analysts spend on retrieving such information helps minimize the overall time to assess the potential threat and remediate, if required.

Why This Matters

While technologies such as IDS, DPI, PCAP, and decryption can pinpoint potential threat events within an organization's network traffic, they do not scale easily when processing large volumes of traffic. Moreover, using these separate technologies does not guarantee that events most likely to breach security will be identified, resulting in undetected security gaps.

ESG validated that CleanINTERNET helps to identify those events most likely to breach an organization's security using an integrated and orchestrated combination of CTI, IDS, DPI, PCAP, and decryption. Because CleanINTERNET has already supplied a set of security events without the "noise," the solution can process more traffic for threat events in less time, decreasing the time and effort of identifying such events.

Minimizing Customer's Security Event Workload

Security analysts face daily lists of flagged security events that require attention. Yet, these lists are typically too long to be managed by both CleanINTERNET security analysts and CleanINTERNET customers. While such lists may contain events considered "high severity," a fraction of those events may require further investigation by Centripetal and reported to customers. Without automated tools for triaging high-severity events into likely reportable or non-reportable events, the risk of spending time on analyzing non-reportable events increases.

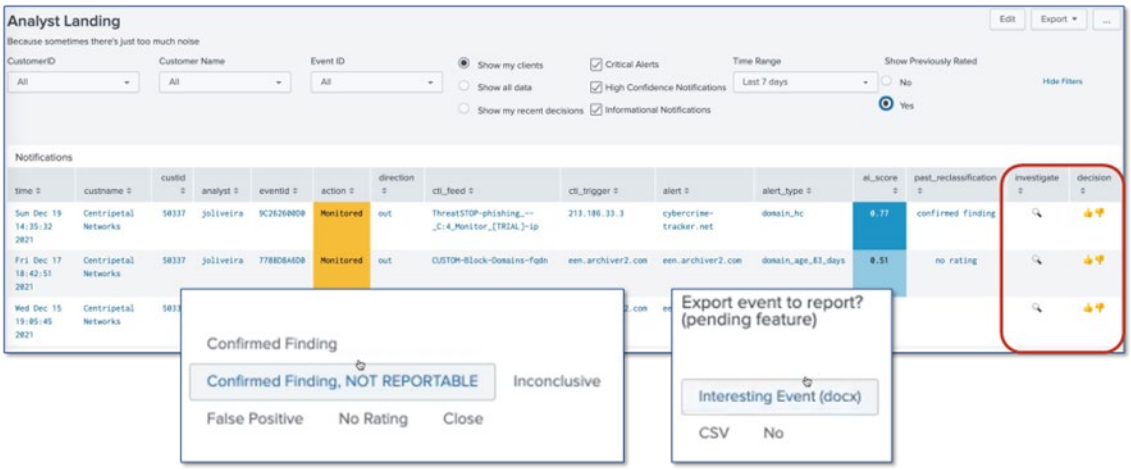
CleanINTERNET's AI-Analyst further curates the set of security events, by reportability likelihood, which have been generated by the RuleGATE and analyzed by ProbableCause. The result is a relatively small subset of critical security events that should be reported to CleanINTERNET's customers.

ESG Testing

ESG navigated to the AI-Analyst module to see how it determines those security events that are most relevant (or reportable) to customers. In Figure 8, we saw the security events that CleanINTERNET determined required further

investigation. On the right side of the ***Analyst Landing*** page, we noted the "Decision" column. By clicking on the "thumbs up" or "thumbs down" emoji, we observed that an analyst can submit security events into the training data for CleanINTERNET's machine learning system for recognizing reportable or non-reportable security events. Simultaneously, the analyst can also submit events for automated report generation. Feedback options (shown at the bottom of Figure 8) could indicate an analyst's assessment of its reportability. That feedback would then affect the AI score (or reportability likelihood) assigned by CleanINTERNET to future security events.

Figure 8. Providing Feedback to AI-Analyst on Specific Security Events

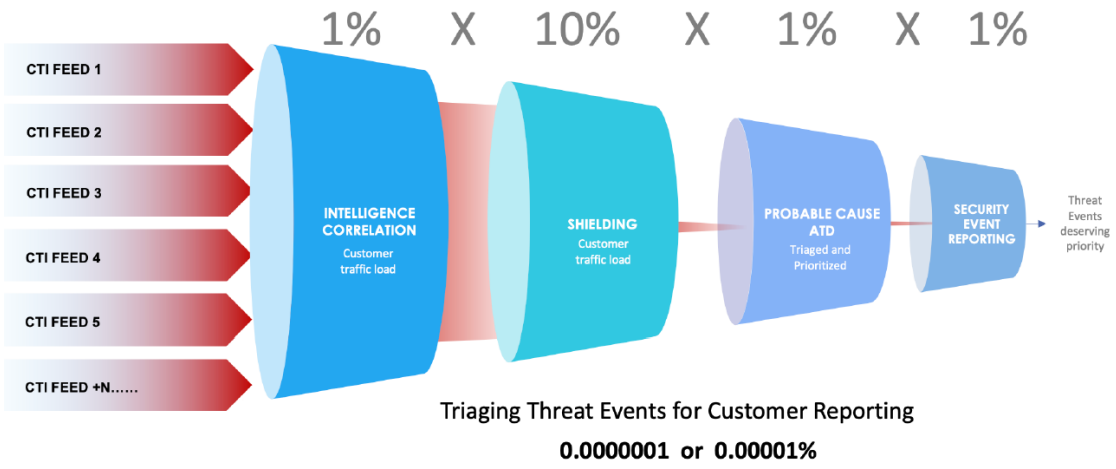


Source: ESG, a division of TechTarget, Inc.

Should the analyst choose the "Confirmed Finding" option, we saw how a report could be automatically generated and sent to affected customers.

ESG then proceeded to estimate how CleanINTERNET effectively reduces the number of security events requiring attention. We reviewed data representing the number of security events that were present as CleanINTERNET processed network traffic for a select number of (anonymized) organizations through the RuleGATE. We considered how the set of security events decreased, as illustrated in Figure 9. The following estimates approximate the percentage of security events remaining as they are processed by CleanINTERNET.

Figure 9. How CleanINTERNET Reduces Network Security Event Workload



Source: Centripetal Networks, Inc.

What the Numbers Mean

- After CleanINTERNET filters traffic to identify security events that should be reported to a customer, this set represents approximately 0.00001% of the original set after CleanINTERNET matched relevant IOCs present in an organization's network traffic.
- To illustrate, if CleanINTERNET filters a billion internet communications events with a zero trust policy derived from a billion IOCs, then the number of security events that are most relevant for a customer to address is 100.
- ESG notes the significant reduction in the security workload for a customer to address. This also reduces the time for a customer to remediate the security events reported by CleanINTERNET, subsequently reducing business risk.

Why This Matters

Security analysts typically manage a never-ending list of alerts every day. There is always the risk of chasing down a potential threat and finding that it does not pose any security risk for a given customer. Imagine an analyst repeatedly facing the same situation. Valuable time and effort have been wasted, and the business remains at risk from other potential threats yet to be remediated.

ESG validated that AI-Analyst helps organizations to focus on only those events that should be addressed and remediated. We saw how AI-Analyst enables CleanINTERNET analysts to provide feedback on events so that CleanINTERNET's machine learning system can determine security events' reportability over time. We also reviewed how AI-Analyst helps CleanINTERNET to significantly reduce a customer's potential event workload. Customers can then use their time efficiently on remediating events that pose legitimate security risks.

The Bigger Truth

The rise of security breaches has prompted organizations to invest heavily in many point solutions. Organizations also continue to struggle with a lack of in-house cybersecurity skills, as ESG research shows that 48% of respondents cite a problematic shortage. When it comes to network security, organizations have typically relied on conventional methods and devices to allow or block traffic of known threats. Yet, the approach does not consider the dynamic nature, let alone the sheer volume, of security events yet to be identified. Simply put, organizations still lack the skills and proper resources to effectively manage such potential threats and attacks.

With CleanINTERNET by Centripetal, organizations can leverage network-security-as-a-service to mount a threat-intelligence-based defense to deal with the nature of today's security events. The solution is designed to identify the most relevant security events that will cause the most harm to an organization's security. Organizations can establish a zero trust network security posture without investing both time and resources to stitch together disjointed technologies and CTI feeds to process and filter huge volumes of network traffic or recruiting cybersecurity analysts.

During our evaluation, ESG validated that CleanINTERNET can help organizations to:

- Maximize IOC coverage to ensure that all relevant and up-to-date IOCs are captured and translated into policies.
- Establish a zero trust network security posture without degrading network performance, thus not disrupting business operations.
- Curate identified security events for a specific business and narrow its risk profile down to those events that are most likely to breach network security, thus helping CleanINTERNET to focus attention on those events and not have to

contend with “noise” such as false positives, security events that have already been remediated by CleanINTERNET, and non-business critical events.

- Determine those events that should be communicated to customers, enabling an organization’s security team to focus time and effort efficiently on “real” issues, reducing a customer’s workload.

If your organization is looking to establish a zero trust network security posture, in light of the dynamic nature and increasing volume of potential threats and attacks, while significantly reducing security event workloads without increasing cybersecurity staff, ESG believes that you should look more closely at CleanINTERNET by Centripetal.

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

www.esg-global.com contact@esg-global.com 508.482.0188