CYBER STASH

Converging Forces

Elevating Cybersecurity with Threat Detection and Hunting

Abstract

The intricate world of enterprise cybersecurity, the differentiation between threat detection and threat hunting is essential to a comprehensive defence strategy. These two concepts are often used interchangeably but entail distinct approaches and objectives. The paramount consideration lies in recognising the synergistic interplay between threat detection's agility in promptly identifying and mitigating threats with established footprints and threat hunting's prowess in unveiling nascent, cryptic, or hitherto uncharted threats. In harmonising these distinct paradigms, an enterprise can hope to fortify its cyber resiliency amidst the ceaseless evolution of the threat landscape.

Threat Detection is predicated upon the utilisation of prior knowledge encompassing known threats and established attack patterns. It operates by subjecting network traffic and digital assets to continuous scrutiny, comparing their attributes against preconfigured threat signatures. Upon detecting some correspondence, an immediate response protocol is set into motion for threat containment. This approach excels in addressing recognised threats but may prove less adept in confronting novel, unforeseen, or highly intricate adversarial tactics. In the realm of threat detection, the emphasis rests on immediate response to known threats. Security systems and tools are primed to recognise patterns and behaviours characteristic of previously identified attacks, enabling swift remediation and containment measures. It operates as the frontline defense, effectively repelling intruders with established battle-tested tactics.

Threat Hunting, in contrast, epitomises a proactive and methodical undertaking. It entails a systematic exploration of the digital terrain, wherein the discerning investigator, deprived of predetermined threat templates, seeks aberrations, atypical behavioural cues, and deviations from baseline norms. It is an approach that thrives in the domain of undiscovered and concealed threats, unshackled by the constraints of predefined threat profiles. It is a more proactive and inquisitive approach. It operates under the assumption that unknown threats may lurk within the digital environment, undetected by traditional security measures. Threat hunting is not confined to the parameters of prior knowledge; it thrives in the ambiguity of the digital abyss. Unlike threat detection, it is not contingent on predefined patterns and signatures. Instead, threat hunting embraces the spirit of exploration and inquiry, utilising diverse data sources, behavioural analytics, and anomaly detection to expose elusive intrusions, emerging threats, or unprecedented attack vectors.

Network Threat Detection and Hunting

Network Threat Detection stands as a multi-pronged strategy that extends beyond the confines of predefined lists encompassing specific IP addresses and domains associated with established adversary activities. It is further characterised by its ability to scrutinise network traffic, carefully evaluating each digital entity for the presence of well-established threat indicators while keenly discerning patterns suggestive of intrusion and exploitation.

This vigilant process operates as a sentry, maintaining continuous surveillance over network activities, and when an alignment with a known threat is identified, it triggers an immediate response. The response may encompass alerting to the presence of a known threat or proactively intervening to prevent its impact. Network Threat Detection exhibits excellence in building a robust defense against familiar attack indicators and indicators of compromise, as well as demonstrating a knack for detecting frequently employed intrusion tactics.

In an enterprise cybersecurity context, Network Threat Detection assumes a pivotal role, affording organisations the means to thwart recognised threats while also providing insights into the common strategies employed by adversaries. This comprehensive approach bolsters the security posture of the enterprise, facilitating timely responses to known threat vectors and intrusion attempts.

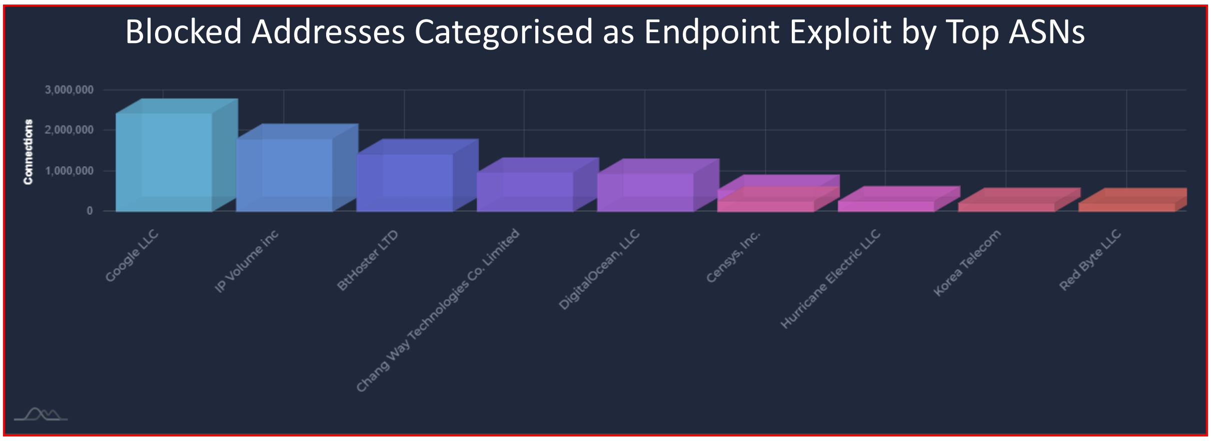
Network Threat Hunting conversely assumes the mantle of a proactive and investigative methodology. It extends its purview to encompass a broader spectrum of network traffic, encompassing data traversing to regions affiliated with high-risk countries and Autonomous System Numbers (ASNs). Additionally, it casts its net wider by scrutinising for anomalous network traffic patterns, such as the detection of unusually elevated volumes of internet traffic within DNS traffic flows.

When these unusual patterns materialise, the skilled hands of threat hunters pivot to scrutinise and dissect these enigmatic anomalies. Their focus is centred on unearthing the true essence of this traffic, discerning whether it benignly meanders or conceals a malevolent threat. This process mirrors a thorough exploration into the unknown, unshackled from predefined lists and instead fuelled by an unwavering sense of curiosity and the ardent quest to unearth hidden anomalies.

In the intricate milieu of enterprise cybersecurity, Network Threat Hunting plays a decisive role. It empowers organisations to delve deeper into the intricacies of network traffic, identifying potential threats that might otherwise elude conventional security measures. This method not only detects but also unravels the enigmatic patterns and concealed dangers, enriching an enterprise's cybersecurity posture with a comprehensive understanding of potential anomalies.

Leveraging Operational Threat Intelligence for Risk Mitigation through Tactical Threat Intelligence Policies

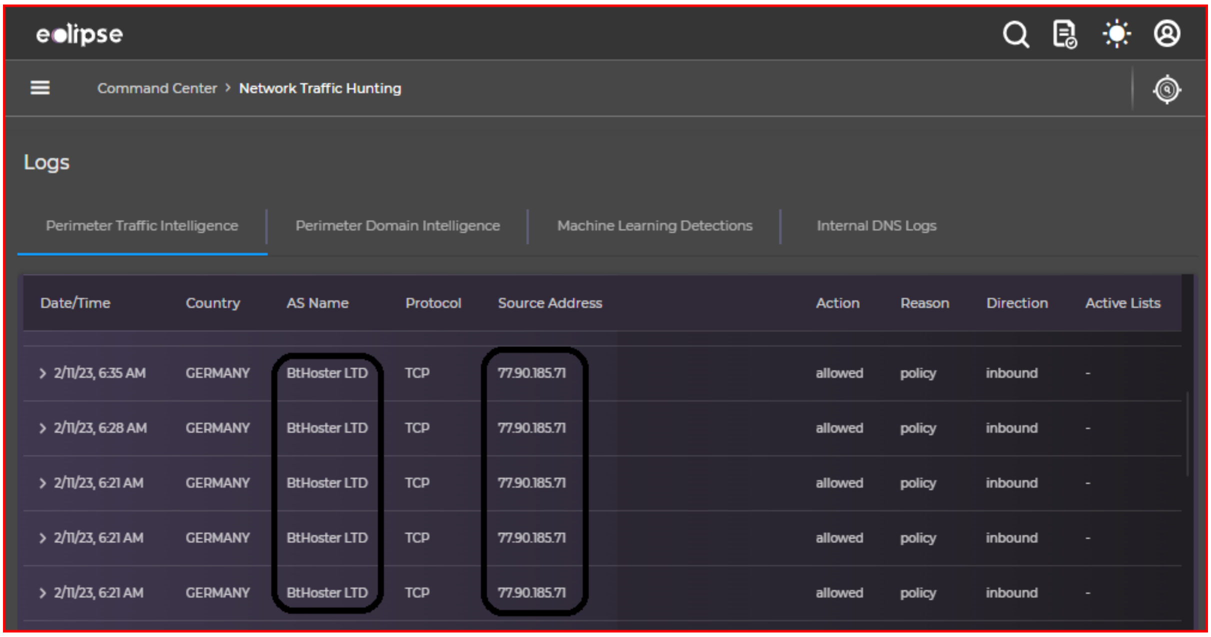
In the graph below, we illustrate the noteworthy inbound denied traffic linked to Autonomous System Numbers (ASNs), which has been blocked because it originates from known malicious IP addresses known to carry out endpoint exploitation.



Blocked Addresses Categorised as Endpoint Exploit by Top ASNs

We can enhance our cybersecurity strategy by identifying the ASNs with the highest concentration of IP-based threat intelligence indicators. With this insight, we can proactively investigate all incoming traffic from these ASNs, regardless of whether there's a known prior correlation with an IP-based threat indicator. To bolster our efforts, we can further validate the discovered IP addresses by cross-referencing them with external sources like VirusTotal. This validation step increases our confidence that the traffic indeed originates from a potential attacker, especially if other cybersecurity vendors have also flagged this IP as a threat.

To illustrate, we've generated a report for inbound traffic originating from ASN BtHoster LTD, in cases where the source IP address did not match any entries in our threat intelligence database.



eclipse

Command Center > Network Traffic Hunting

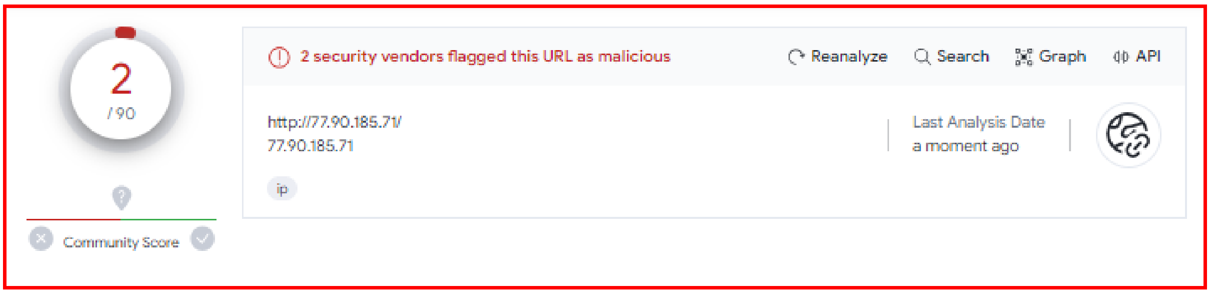
Logs

Perimeter Traffic Intelligence
Perimeter Domain Intelligence
Machine Learning Detections
Internal DNS Logs

Date/Time	Country	AS Name	Protocol	Source Address	Action	Reason	Direction	Active Lists
2/11/23, 6:35 AM	GERMANY	BtHoster LTD	TCP	77.90.185.71	allowed	policy	inbound	-
2/11/23, 6:28 AM	GERMANY	BtHoster LTD	TCP	77.90.185.71	allowed	policy	inbound	-
2/11/23, 6:21 AM	GERMANY	BtHoster LTD	TCP	77.90.185.71	allowed	policy	inbound	-
2/11/23, 6:21 AM	GERMANY	BtHoster LTD	TCP	77.90.185.71	allowed	policy	inbound	-
2/11/23, 6:21 AM	GERMANY	BtHoster LTD	TCP	77.90.185.71	allowed	policy	inbound	-

What we have discovered is the IP address 77.90.185(.)71, which originates from ASN BtHoster LTD. This IP address was previously unknown to both the vendor-agnostic threat intelligence providers our client depends on for blocking malicious traffic and to almost all other security vendors listed on VirusTotal.

However, when we cross-referenced this IP with VirusTotal, we found that two security vendors had identified it as malicious. Further investigation uncovered that this IP address is also listed in various other block lists not associated with any vendors on the VirusTotal list.



2 security vendors flagged this URL as malicious

http://77.90.185.71/
77.90.185.71

ip

Last Analysis Date
a moment ago

Based on this comprehensive information, we can reasonably conclude that this IP address is indeed associated with malicious network activities, specifically, involving port scanning and endpoint exploitation. With this information in hand, we have the flexibility to enhance our defenses by either adding the specific IP address or the entire ASN to our blocking policy. This Network Hunting methodology empowers us to unearth previously undiscovered indicators of attacks, providing valuable insights. We can then utilise this information to make informed proactive blocking decisions, either to block the newly identified malicious IPs or even the entire ASN. This is especially valuable when the organisation has no requirement to make its applications accessible to users originating from within that ASN.

Closing Remarks

The CyberStash cyber defense paradigm adeptly complements elements from both threat detection and threat hunting methodologies. While conventional threat detection relies heavily on recognising established threat indicators, our strategy aligns more closely with the proactive ethos that characterises threat hunting. Through the adept use of operational threat intelligence, we identify Autonomous System Numbers (ASNs) exhibiting a significant concentration of IP-based threat indicators, spanning both familiar and hitherto unseen threats.

By embracing this approach, we elevate the robustness of our security defenses, effectively unveiling potential threats that might otherwise remain shrouded. Our threat assessment is further fortified by cross-referencing findings with external sources. This multifaceted strategy empowers us to make well-informed decisions pertaining to proactive blocking, thus bolstering the overarching strength of our cybersecurity defenses. Importantly, this strategic framework extends its utility to organisations seeking to restrict their exposure to specific ASNs. It not only mitigates risks but also reinforces the resilience of our security posture, effectively marrying the complementary capabilities of both threat detection and threat hunting.

Furthermore, the CyberStash eclipse.xdr Cyber Defense Platform cleverly employs its XDR Gateway to proactively intercept potential sources of cyber-attacks, leveraging insights derived from vendor-agnostic threat intelligence data. Concurrently, we employ Network Analytics to diligently seek out indicators of compromise and impending attacks. These insights form the cornerstone of our decision-making processes, enabling us to further enhance the cyber defenses for our esteemed clients.

Request a Demonstration

CyberStash is your strategic partner in significantly reducing your business's vulnerability to cyberattacks. We not only prevent breaches but also respond swiftly to detected threats before they can cause irreparable harm to your operations.

To gain a profound understanding of how our Eclipse.XDR solution can fortify your business against the dynamic realm of cyber threats, we extend a cordial invitation to get in touch with CyberStash. Our team is delighted to offer you a complimentary presentation and demonstration, providing you with a thorough and informed perspective on the full breadth of our capabilities.

https://www.cyberstash.com