Technical Brief

STAMUS NETWORKS

# Using Predefined Threat Hunting Filters in Clear NDR®

This technical brief describes the guided threat hunting filters that are currently included in the Clear NDR. These filters give security analysts a powerful tool to quickly review the vast evidentiary data store created by Clear NDR to proactively identify suspicious activity, hidden threats, shadow IT, and policy violations that their automated systems might miss.

Clear NDR is a network-based threat detection and response (NDR) system that delivers:

- Response-ready and high-fidelity threat detection from machine learning, behavioral anomaly algorithms, IOC matching, heuristics, and signatures
- Open interfaces for simple integration with SOAR, SIEM, XDR, EDR, IR
- Support for third-party and custom threat intelligence
- Explainable and transparent results with extensive evidence
- Integrated guided threat hunting

Clear NDR automatically detects and identifies threats by monitoring on-prem and cloud-based networks and presents security teams with complete contextual evidence for each threat, detailed incident timelines, and more.

## PROACTIVE THREAT HUNTING

Because many organizations have found proactive threat hunting to be an important part of their defenses, Clear NDR includes many features designed for threat hunters. Using Clear NDR's Hunting and Investigation interface, security analysts can hunt for specific threat types, well-publicized threats, known Declarations of Compromise® (DoCs), anomalous activity, suspicious behaviors, and more.

The Hunting and Investigation interface provides security analysts a powerful set of query tools to easily filter through the vast data store generated by the Clear NDR Network Probes as they monitor network activity.

The Hunting and Investigation interface uses a drill down approach, creating composite filters to uncover interesting events captured by Clear NDR Probes. The analyst applies additional filter criteria based on event metadata by simply clicking on the magnifier icons next to the field value.

The Clear NDR Hunting and Investigation module includes six primary components that help hunters with various tasks:

- Guided threat hunting filter sets
- Context and classification
- Previously unseen communications (Stamus Sightings)
- Metadata search tools
- Host Insights
- Automation

In this tech brief we focus on the **guided threat hunting filter sets**.

## PROACTIVE THREAT HUNTING

Because defenders often need a place to begin their hunt, the Hunting and Investigation interface gives security practitioners over 100 ready-to-use guided threat hunting filter sets, including those which can identify unknown attack surfaces created by policy violations and shadow IT.

Note: we may refer to these "pre-defined filter sets" or "guided threat hunting filter sets" depending upon the context. But rest assured, both terms are describing the same thing.

A filter set is basically a hunting idea or concept – translated into criteria based on the selection, negation, and wild carding of event metadata values – which results in a filtered query of the Clear NDR data. As of the U42 software release, there are over 120 pre-defined filter sets, accessible from the Hunting and Investigation interface, and organized around the following 11 categories:

- Adware
- Anomaly
- Compliance
- Hunt
- Info
- MITRE
- Phishing
- Policy
- Roles
- Services
- Trojan

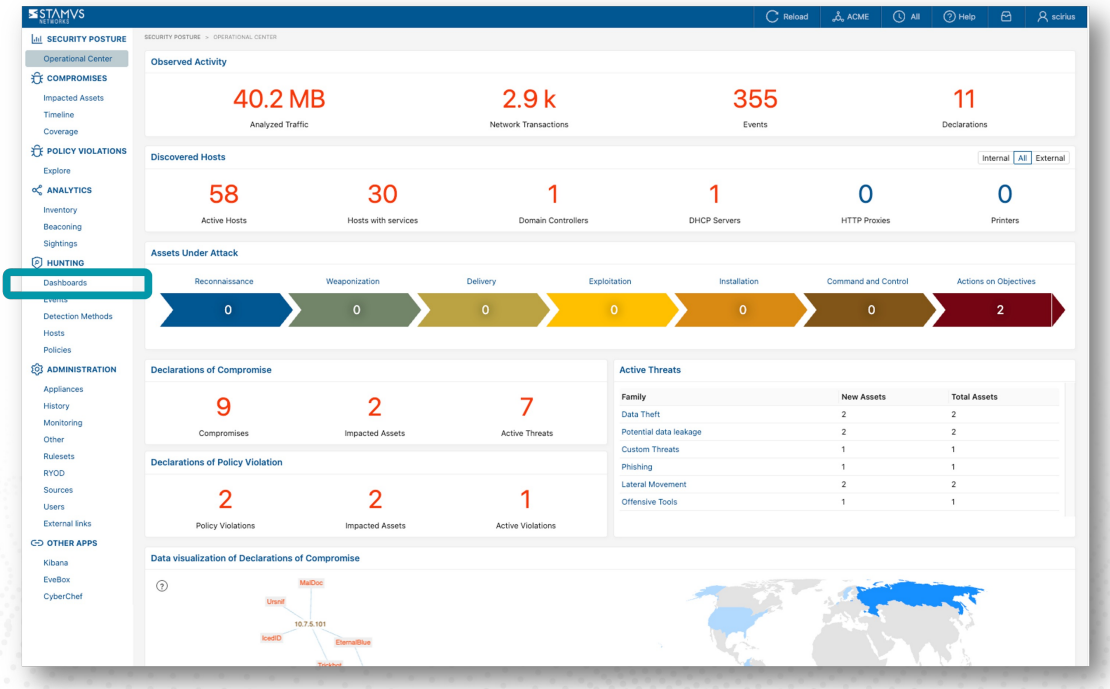
The filter-sets give defenders a very powerful hunting advantage because they can be used to display specific threat activity or policy violation on the network - from a specific detection event to a new proxy, printer, domain controller, or network service in the enterprise. For example, with just a single click, a security analyst can spot a new python-based web server in the marketing department.

## SELECTING AND USING FILTER SETS

The following screenshots illustrate the steps needed to select and use a predefined threat hunting filter set.

To take advantage of the predefined filter sets, the user should navigate to the Hunting and Investigation section on the user interface. See example below.

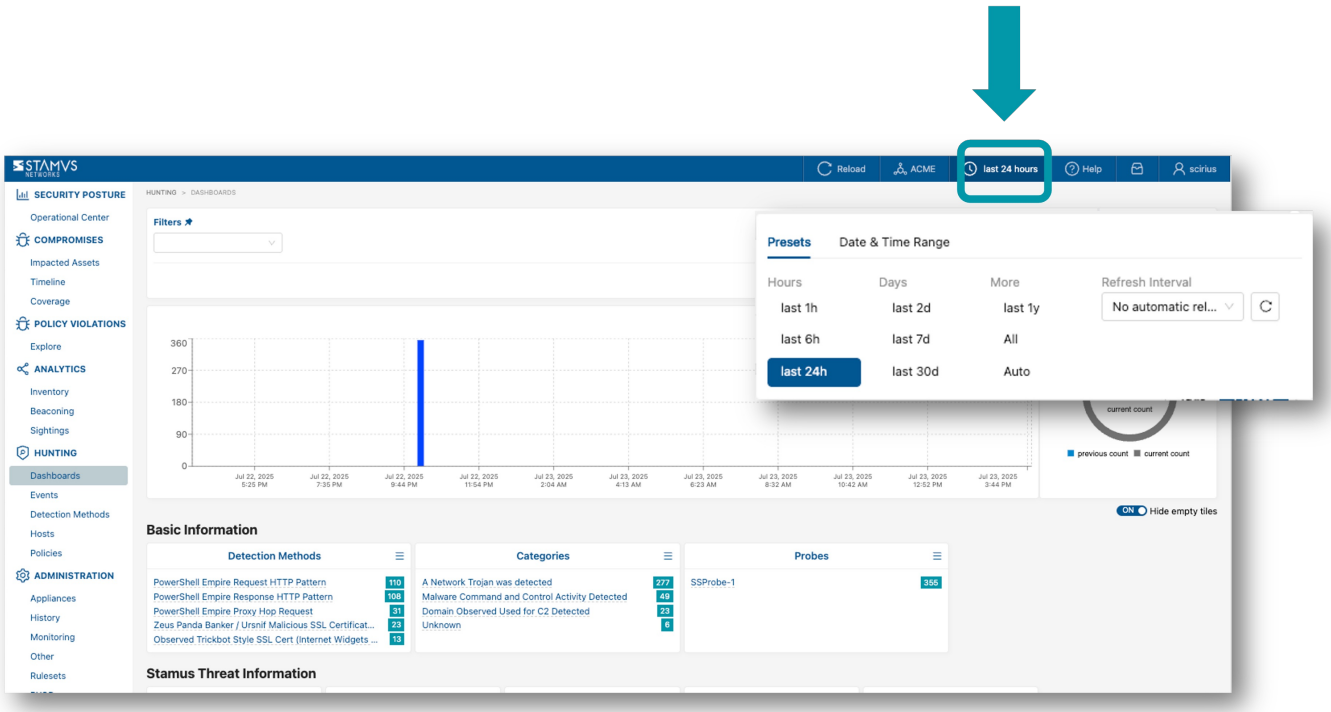
Open the Hunting and Investigation *Dashboards*




The Clear NDR Hunting and Investigation dashboard serves as the main launching point for the threat hunting tool. It includes over 50 elements of event metadata that can be viewed at a quick glance. It also allows the user to pivot and connect to the other hunting tools in the system.

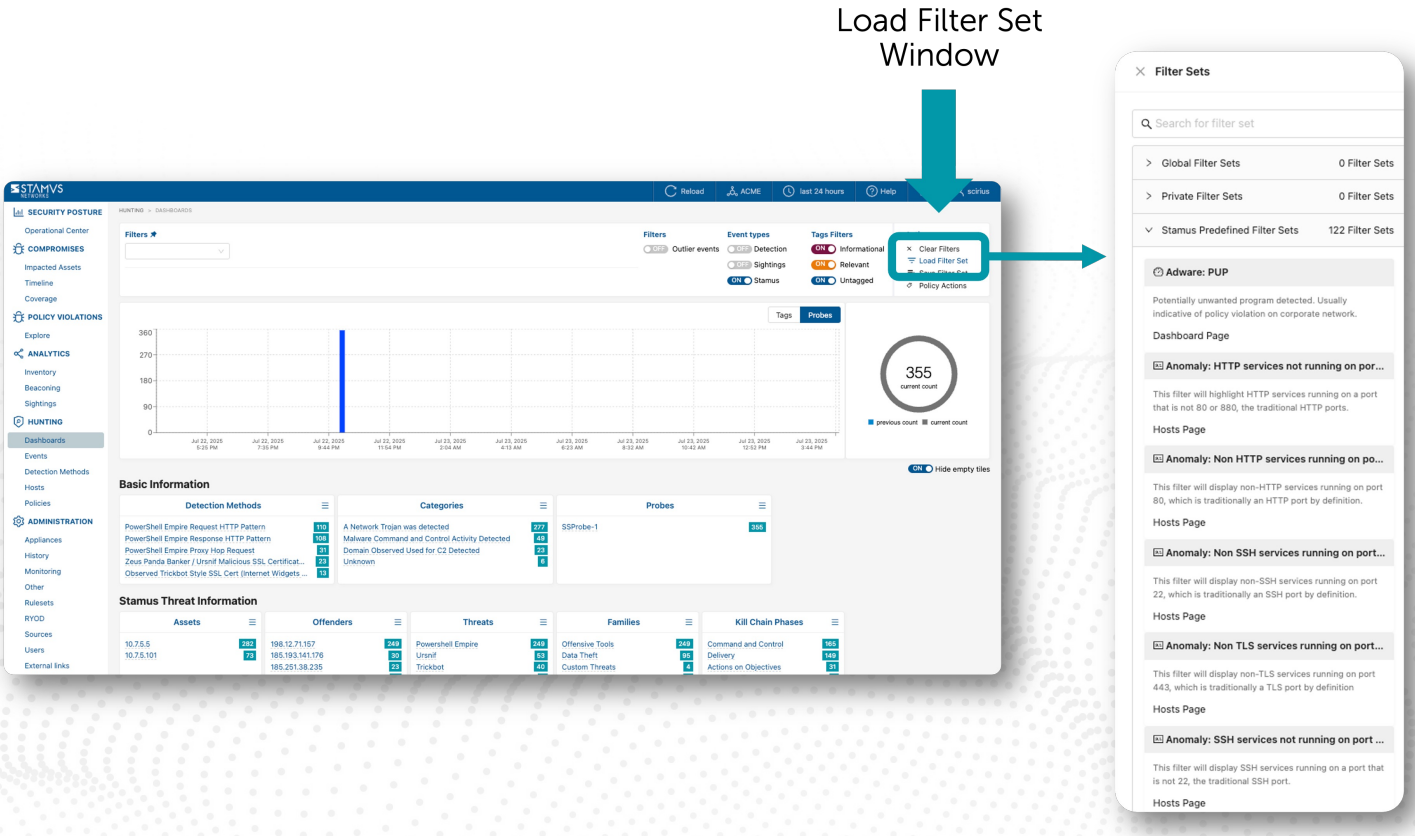
From here you can select the timescale of the data in which you wish to hunt.

Select timescale for the data



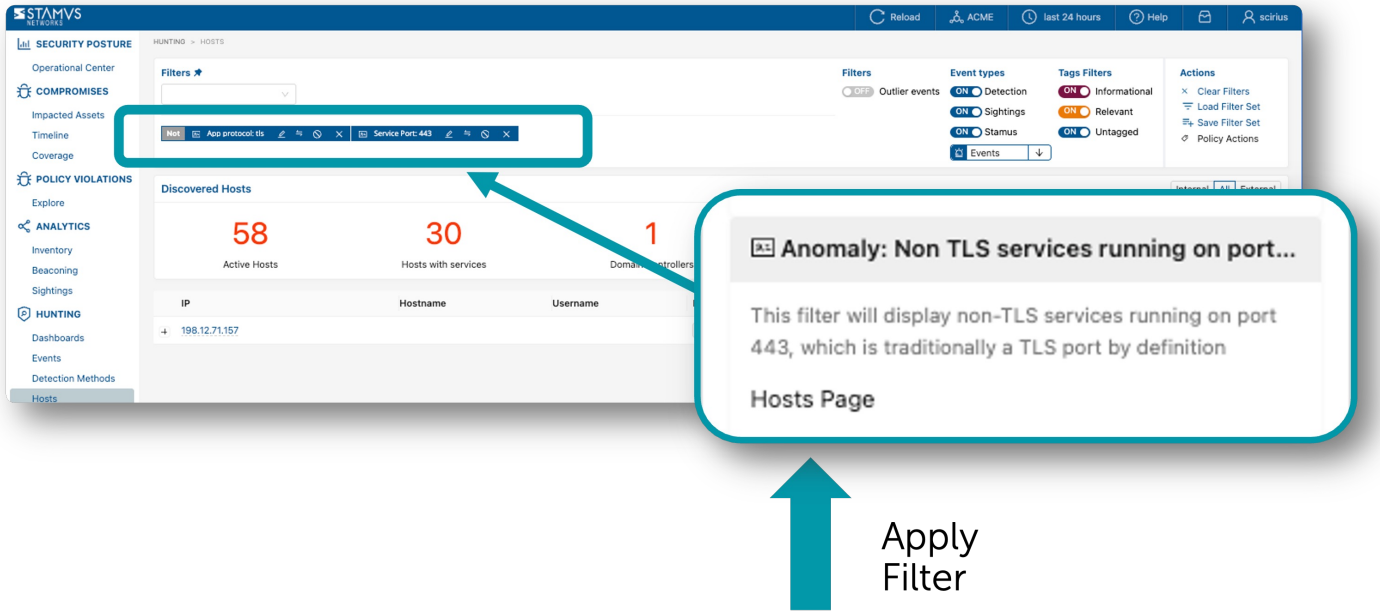

Next, open the Filter Sets window from the filter menu area.

Load Filter Set Window



With the filter set window open, select the filter you wish to apply. You may do this by searching for the filter set in the search bar at the top of the pop-up window or by scrolling until you find the filter you are looking for.

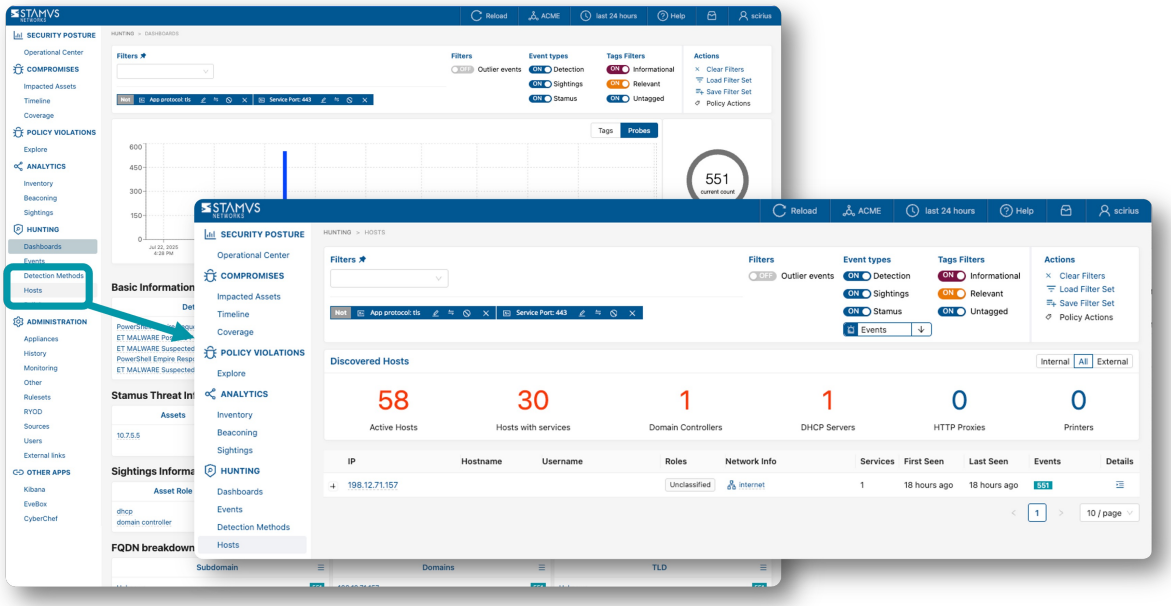
When you click on the filter in the pop-up window, the filter is applied to the data, and the criteria defined by the filter set appear in the Clear NDR Hunt and Investigation dashboard's "active filters" bar.




Once the filter set is applied, the security analyst may click on the magnifying glass icons beside the various data elements to further filter the data or they may click on the various data elements directly to pivot into a different view altogether.

Often, the next step for the analyst is to review the various hosts identified by the filter to gain additional context. In the example below, the user has clicked on the "Hosts" item on the left-hand navigation pane to pull up the listing of all hosts involved in this filtered activity.

Pivot to the *Hosts* Module




# COMPLETE LIST OF PRE-DEFINED HUNTING FILTERS

## Adware Filter Sets (1)

This group of filter sets provide guided hunting to identify various potentially unwanted programs operating on the network.

**Potentially Unwanted Program** - Potentially unwanted program (PUP) detected. Usually indicative of policy violation on the network.

## Anomaly Filter Sets (6)

This group of filter sets provide guided hunting to identify hosts using traditional services (such as TLS, SSH, HTTP, etc) on non-traditional ports.

**HTTP services not running on port 80/8080** - This filter will highlight HTTP services running on a port that is not 80 or 880, the traditional HTTP ports.

**Non-HTTP services running on port 80** - This filter will display non-HTTP services running on port 80, which is traditionally an HTTP port by definition.

**Non SSH services running on port 22** - This filter will display non-SSH services running on port 22, which is traditionally an SSH port by definition.

**Non-TLS services running on port 443** - This filter will display non-TLS services running on port 443, which is traditionally a TLS port by definition.

**SSH services not running on port 22** - This filter will display SSH services running on a port that is not 22, the traditional SSH port.

**TLS services not running on port 443** - This filter will display TLS services running on a port that is not 443, the traditional TLS port.

## Compliance Filter Sets (1)

This group of filter sets provide guided hunting to identify hosts with unusual encryption certificate usage operating on the network.

**Not common SSL certificate issuers** - This filter displays results of network traffic analysis that have TLS services using uncommon SSL certificate issuers. Can be used to rapidly identify hosts using self-signed certificates on the network.

## Hunt Filter Sets (71)

This group of filter sets provide guided hunting a broad array of hunting ideas based on metadata associated with events. These include obfuscated executables, suspicious zipped files transfers, suspicious payloads, successful scans, backdoors, exploits, crypto miners, base64 functions detected in events, and others.

**HTTP obfuscated executable as Image content** - This filter set can be used to uncover malware posing as images in HTTP content. In this case, the HTTP content presents itself as an image (with a png, gif, jpeg extension, for example), but the actual downloaded or transferred file is an executable.

**Phishing events** - This filter identified suspicious, likely, or successful phishing communication.

**Suspicious DNS requests** - This filter highlights DNS requests to suspicious or non-traditional domains.

**Likely hostile domain events** - This filter highlights DNS requests to likely hostile domains.

**Malware family present in events** - This filter highlights the events in which malware family is identified.

**Exploit kit present** - This filter highlights the events that use exploit kits.

**Executable code present** - This filter highlights the events that detect any executable code.

**C2 domains detected** - This filter highlights the events that C2/CnC domains detected.

**Command and Control activity present (CnC)** - This filter highlights the events associated with command and control activity (CnC).

**Admin payload search** - This filter highlights the events that include "Admin" or "Administrator" in their alert payload.

**Backdoors and exploits for public facing web servers** - This filter set returns a very potent information set of events that indicate either an ongoing backdoor or an exploit for public facing web servers or php based applications.

**Coinminers** - This filter highlights the events that are related to coin miners.

**Crypto miners or Ransomware** - This general wildcard filter highlights events of cryptominers or ransomware malware variants.

**Current events** - This filter highlights the events that trigger based on the CURRENT_EVENTS ET rules.

**DNS over HTTPS** - This filter returns all the events related to DNS over HTTPS usage transactions. It is important here to review providers that are highlighted. In many organizations, this may also be a policy violation.

**DNS related events** - This filter highlights all the events with DNS-related metadata.

**DOS or Windows executable** - This filter highlights all the events that are related to DOS or Windows executable HTTP transfers.

**Executable related events** - This filter highlights all the events related to executable files, including downloads, posts, and others. This usually provides interesting data that warrants further investigation.

**Executable downloads from PowerShell** - This filter highlights all the events that include executable-related transfers from PowerShell HTTP user agents.

**Executable downloads from programmable software** - This filter highlights all the events that include executable-related transfers from HTTP user agents that are common scripting languages.

**HTTP Executable related events** - This filter highlights all the events that take place via HTTP and are either posting or downloading executables.

**HTTP POSTs** - This filter highlights all the events that include HTTP POST requests. This type of request can hide malicious activity.

**HTTP direct requests and replies to private IP** - This filter highlights all the events that include HTTP requests and responses directly to an internal IP address - not a domain name. This activity may be suspicious because a domain name is typically part of the transaction when communicating with servers inside the network. While common in some development environments, it could also indicate lateral movement.

**HTTP likely direct IPv6 communications** - This filter highlights all the events detecting direct IPv6 communication and communication events likely using directly IPv6 HTTP hosts.

**HTTP non-internal direct IP requests and replies** - This filter highlights all the events that indicate HTTP requests and responses directly by IP - not using a domain name. This activity may be suspicious because a domain name is typically part of the transaction when communicating with servers outside the network (non private/internal IPs).

**HTTP payloads containing admin** - This filter highlights all the events that indicate HTTP payloads containing “admin”.

**HTTP payloads containing root** - This filter highlights all the events that indicate HTTP payloads containing "root".

**Hunting related events** - This filter highlights all the events that are generated from rules with the "hunting" designation.

**Hosts with more than one user** - This filter highlights all the hosts that have more than one user. This typically generates a list of good candidates for investigation.

**Hosts with suspicious http user agents** - This filter highlights all hosts that have been seen using suspicious and non-traditional user agent strings. This typically generates a list of good candidates for investigation.

**Low noise recently-created signatures** - This filter returns very interesting low noise events created from signatures from 2020 onward.

**Longer domain DNS requests** - This filter highlights all the DNS-related events with domains equal to or greater than 70 characters. The results can further be narrowed if needed by selecting or negating different TLDs from the interface. That gives a good first Hunting angle.

**Low noise signature events** - This filter highlights the events which have rarely triggered. These low noise alerts can sometimes hide valuable artifacts and discoveries.

**Malicious filenames in payloads** - This filter highlights the events whose payloads contain known malicious files or filenames.

**Malware-related events** - This filter highlights the malware-related events.

**New executables seen** - This filter highlights the events that are related to executables downloaded from new previously unseen locations.

**Non common TLDs** - This filter highlights the events which do NOT involve the most common top level domains. The resulting set can help focus the hunting activity related to http, dns, and uncommon events.

**Non lib/open SSH clients** - This filter highlights the SSH-related events that have no libssh or openssh client version.

**One word HTTP user agents** - This filter highlights one-word HTTP user agents.

**Potential Bot HTTP user agents** - This filter highlights user agents that may be potential bot crawlers.

**Punycode domains present in DNS, TLS or HTTP** - This filter highlights the events that have punycode names present in DNS, TLS, HTTP requests.

**Recent malware or trojan** - This filter highlights the malware- or trojan- related events.

**Remote Administration Console OpenLocalMachine** - This filter highlights the events that are related to remote administration console being accessed.

**Remote Administration Registry HKEY_CLASSES_ROOT** - This filter highlights the events that are related to remote administration registry being accessed.

**Root payload search** - This filter highlights the events containing "root" in the payloads.

**Severity 1 events** - This filter highlights the events classified as "Severity 1" by one of the rulesets.

**Shell content http transfer** - This filter highlights the events that identify HTTP shell files or script transfer.

**Shorter domain DNS requests** - This filter highlights the DNS-related events associated with shorter domain name lengths - 10 characters and below. The results may further be filtered if needed by selecting or negating specific TLDs from the interface.

**Stamus flowbits metadata tags** - This filter highlights the events flagged with any stamus flowbit(s).

**Stamus critical lateral SMB, DCERPC** - This filter highlights SMB critical changes events - deletion/additions/changes/resets/configurations/installations.

**Stamus lateral SMB, DCERPC** - This filter highlights SMB informational events.

**Successful HTTP Scans** - This filter highlights successful HTTP scans, potentially revealing the use of default passwords and credential logging.

**Successful trojan/downloaders HTTP requests** - This filter highlights the events containing trojan or downloader HTTP requests.

**Suspicious HTTP User Agents - 1** - This filter highlights events that are using HTTP application layer protocol but with an user agent that includes specific characters not common to user agents.

**Suspicious HTTP User Agents -2** -This filter highlights events that are using HTTP application layer protocol but with an user agent that is not common - aka not mozilla/firefox/opera/edge/wget and similar.

**Suspicious filenames in payloads** - This filer highlights events that identify suspicious filenames that are commonly used in malware. These may include variations of powershell/zip/post/get requests/cached browser data and many more.

**TLS payloads containing root or admin** - This filter highlights the events identifying "root" or "admin" in the TLS payload.

**Trojan related events** - This filter highlights the trojan-related events.

**Unusual in length http user agents** - This filter highlights the events containing HTTP user agents which contain fewer than 55 characters.

**Windows binary executable** - This filter highlights the events that identify transfers or downloads of Windows binary dll, com or bat files.

**Zipped files in transfer** - This filter highlights the HTTP-related events that identify zipped file name transfers.

**Base64 decoding functions in payloads** - This filter highlights the events that contain base64 decoding functions.

**Base64 encoding functions** - This filter highlights the events that contain base64 encoding functions.

**Exploit signatures for encoded strings** - This filter highlights the exploit signature-based events that have encoded execution strings values in the payload.

**Hunting signatures for encoded strings** - This filter highlights the hunting signature-based events that contain encoded strings values in the payloads.

**URL Shortener services** - This filter highlights events that are related to online URL shortening services.

**Web client encoded values** - This filter highlights the events that have encoded values in the client-side HTTP URLs or payload.

**Web server encoded values** - This filter highlights the events that have encoded values in the server-side HTTP URLs or payload.

## Info Filter Sets (6)

This group of filter sets provide guided hunting to identify user agents operating on the network.

**Curl HTTP User Agents** - This informational filter highlights the HTTP-based events that contain Curl HTTP User Agents.

**Java HTTP User Agents** - This informational filter highlights the HTTP-based events that contain Curl Java User Agents.

**Perl HTTP User Agents** - This informational filter highlights the HTTP-based events that contain Perl HTTP User Agents.

**Python HTTP User Agents** - This informational filter highlights the HTTP-based events that contain Python HTTP User Agents.

**Shockwave Flash HTTP User Agents** - This informational filter highlights the HTTP-based events that contain Shockwave Flash HTTP User Agents.

**Wget HTTP User Agents** - This informational filter highlights the HTTP-based events that contain Wget HTTP User Agents.

## MITRE Filter Sets (7)

This group of filter sets provide guided hunting to identify events for which the MITRE technique is identified.

**Technique - Data Encrypted for Impact** - This filter highlights the events for which the MITRE technique is identified as "Data Encrypted for Impact."

**Technique - Data Obfuscation** - This filter highlights the events for which the MITRE technique is identified as "Data Obfuscation."

Technique - Develop **Capabilities - This filter highlights the events for which the MITRE** technique is identified as "Develop Capabilities."

**Technique - Encrypted Channel** - This filter highlights the events for which the MITRE technique is identified as "Encrypted Channel."

**Technique - Exfiltration Over C2 Channel** - This filter highlights the DS events for which the MITRE technique is identified as "Exfiltration Over C2 Channel."

**Technique - Phishing** - This filter highlights the events for which the MITRE technique is identified as "Phishing."

**Technique - Resource Hijacking** - This filter highlights the events for which the MITRE technique is identified as "Resource Hijacking"

## Phishing Filter Sets (2)

This group of filter sets provide guided hunting to identify potential successful phishing attempts taking place on the network.

**HTTP status code 200 detection** - This filter highlights successful (status code 200) HTTP related events that may be identified with possible attempts of phishing and policy violations.

**Phishing general detection** - This filter highlights events that contain the keyword "phishing," identifying all activity that may be considered possible phishing attempts.

## Policy Filter Sets (17)

This group of filter sets provide guided hunting to identify potential organizational policy violations such as the use of older or vulnerable TLS encryption, Dynamic DNS, TOR traffic, clear text passwords and more operating on the network.

**Abused file sharing hosting** - This filter highlights the use of commonly abused file sharing services and providers.

**CVE Detection - 2020 onward** - This filter highlights events associated with more recently identified vulnerabilities (CVE issued from 2020 onward).

**CVE global detection** - This filter highlights events associated with publicly-identified vulnerabilities (CVE issued).

**Clear text password - 1** - This filter highlights events associated with clear text passwords.

**Clear text password - 2** - This filter highlights events associated with unencrypted passwords.

**Dynamic DNS requests - 1** - This filter highlights DNS-related events associated with communication to and from Dynamic DNS providers (Group 1).

**Dynamic DNS requests - 2** - This filter highlights DNS-related events associated with communication to and from Dynamic DNS providers (Group 2).

**External IP checking** - This filter highlights events associated with IP check or lookup.

**FTP application used** - This filter highlights hosts having deployed FTP applications and usage.

**FTP clear text alerts and sightings** - This filter highlights FTP events.

**FTP network services** - This filter highlights hosts with deployed network service of FTP as a service to other hosts.

**Old TLS versions** - This filter highlights events that identify the use of TLS encryption versions prior to version 1.2.

**Outdated software** - This filter highlights outdated or old software that should be upgraded or patched.

**Possible TOR traffic** - This filter highlights TOR traffic-specific events that may constitute an organizational policy violation.

**Public DNS queries** - This filter highlights queries to public DNS infrastructure.

**SMTP clear text events** - This filter highlights unencrypted SMTP events.

**Vulnerable software** - This filter highlights known-vulnerable software that should be upgraded or patched.

## Roles Filter Sets (4)

This group of filter sets provide guided hunting to identify hosts functioning in critical roles, such as domain controllers, DHCP servers, proxies, printers, and more on the network.

**Detected printers and printer services** - This filter highlights printers and printer services detected in the network.

**Detected DHCP servers and services** - This filter highlights DHCP servers and services detected in the network.

**Detected Domain Controllers and DC services** - This filter highlights domain controllers and DC services detected in the network.

**Detected HTTP(S) Proxies and HTTP(S) proxy services** - This filter highlights HTTP(S) Proxies and HTTP(S) proxy services detected in the network.

## Services Filter Sets (7)

This group of filter sets provide guided hunting to identify specific network services observed in communications between network assets. These include Apache, Microsoft IIS, Nginx servers, HTTP(S) proxies, and others operating on the network.

**Apache HTTP servers** - This filter highlights Apache HTTP servers found in the network.

**COMODO issued certificates** - This filter highlights COMODO-issued certificates in use in the network.

**Let's Encrypt issued certificates** - This filter highlights Lets Encrypt-issued certificates used in the network.

**Microsoft IIS HTTP servers** - This filter highlights Microsoft IIS HTTP servers found on the network.

**Nginx HTTP servers** - This filter highlights Nginx HTTP servers found on the network.

**HTTP proxies in the environment** - This filter highlights non-signature events that identify HTTP proxies operating in the network.

**HTTPS proxies in the environment** - This filter highlights non-signature events that identify HTTPS proxies operating in the network.

## Trojan Filter Sets (1)

This group of filter sets provide guided hunting to identify trojans and PUPs operating on the network.

**PUP resulting in Trojan activity** - This filter highlights potentially unwanted programs (PUP) or adware that results in Trojan activity.

## ADDING FILTER CRITERIA

A security analyst may apply additional criteria to any of the predefined filters to advance their hunt. These criteria include IP address, specific network probe, message, not-in-message, port, signature ID, ES filter, protocol, organization-specific network names, and more.

By simply clicking on the magnifier icons next to the metadata field value, a user may apply additional filter criteria to the data using various metadata fields in the events.

## AFTER THE INITIAL HUNT

The guided hunting filters are designed to help an analyst identify unwanted activity or potentially dangerous threats on their organization's network. Locating the suspicious activity is just the first step.

Once a potential threat has been identified, the user may apply other automations and escalations that can help streamline an organization's threat detection. . To learn more about what to do after the hunt, read our article on automation and escalation with the Clear NDR hunting and investigation interface. The article may be found here: https://www.stamus-networks.com/blog/after-the-hunt



229 rue Saint-Honoré
75001Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com