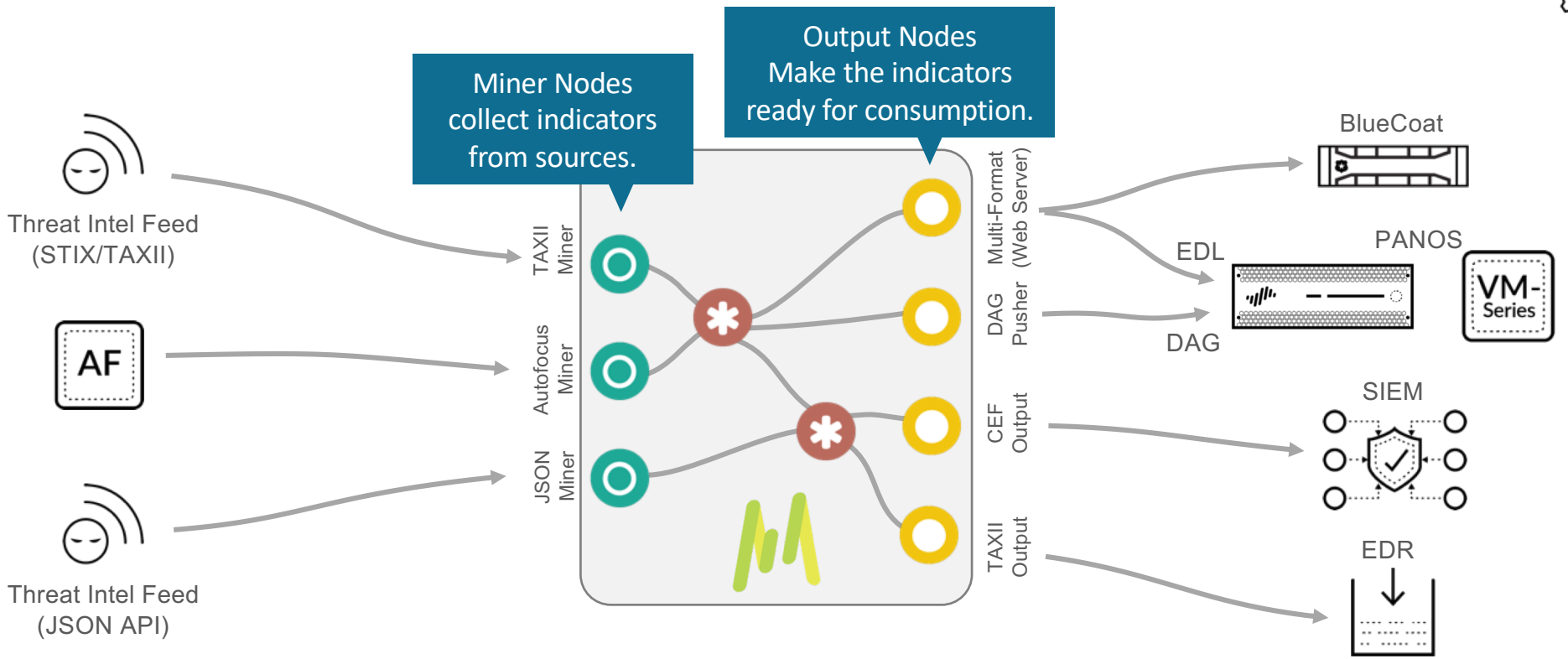
MineMeld Value Proposition

Jesús Díaz

jdiaz@paloaltonetworks.com

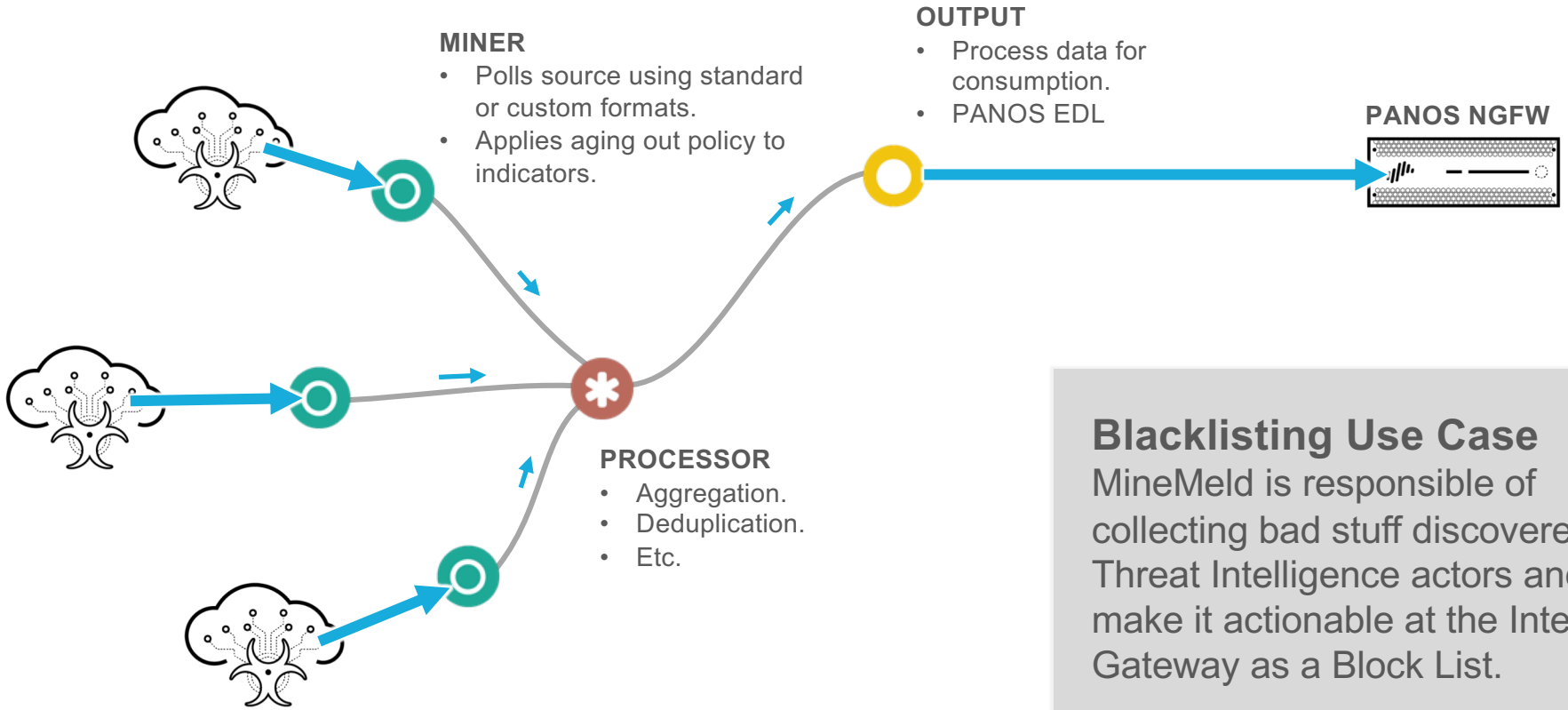
WHAT'S MINEMELD?

What is MineMeld?



MineMeld is an extensible threat intelligence processing framework that collects, aggregates and filters indicators from a variety of sources making them available for consumption in our platform.

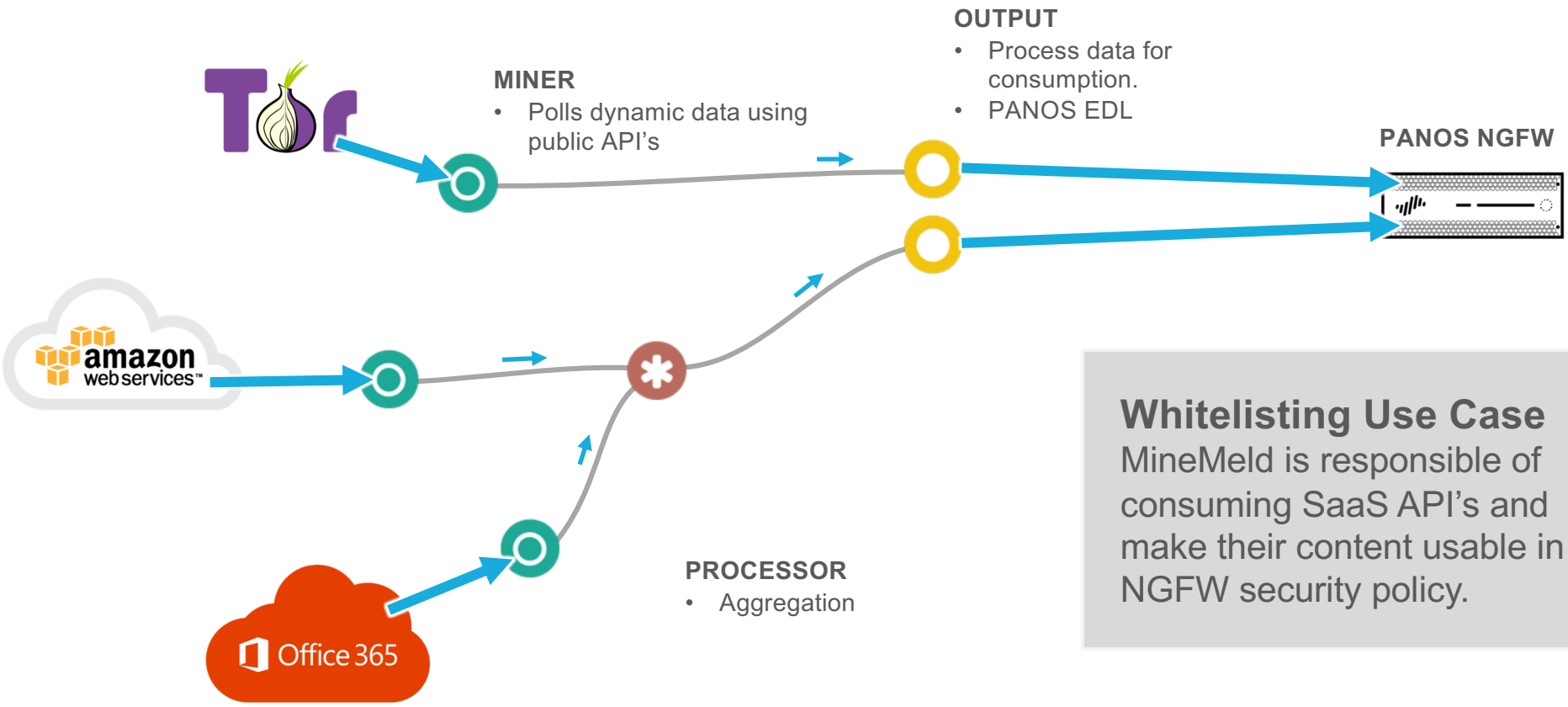
Working with Indicators of Compromise (IoC)



Blacklisting Use Case

MineMeld is responsible of collecting bad stuff discovered by Threat Intelligence actors and make it actionable at the Internet Gateway as a Block List.

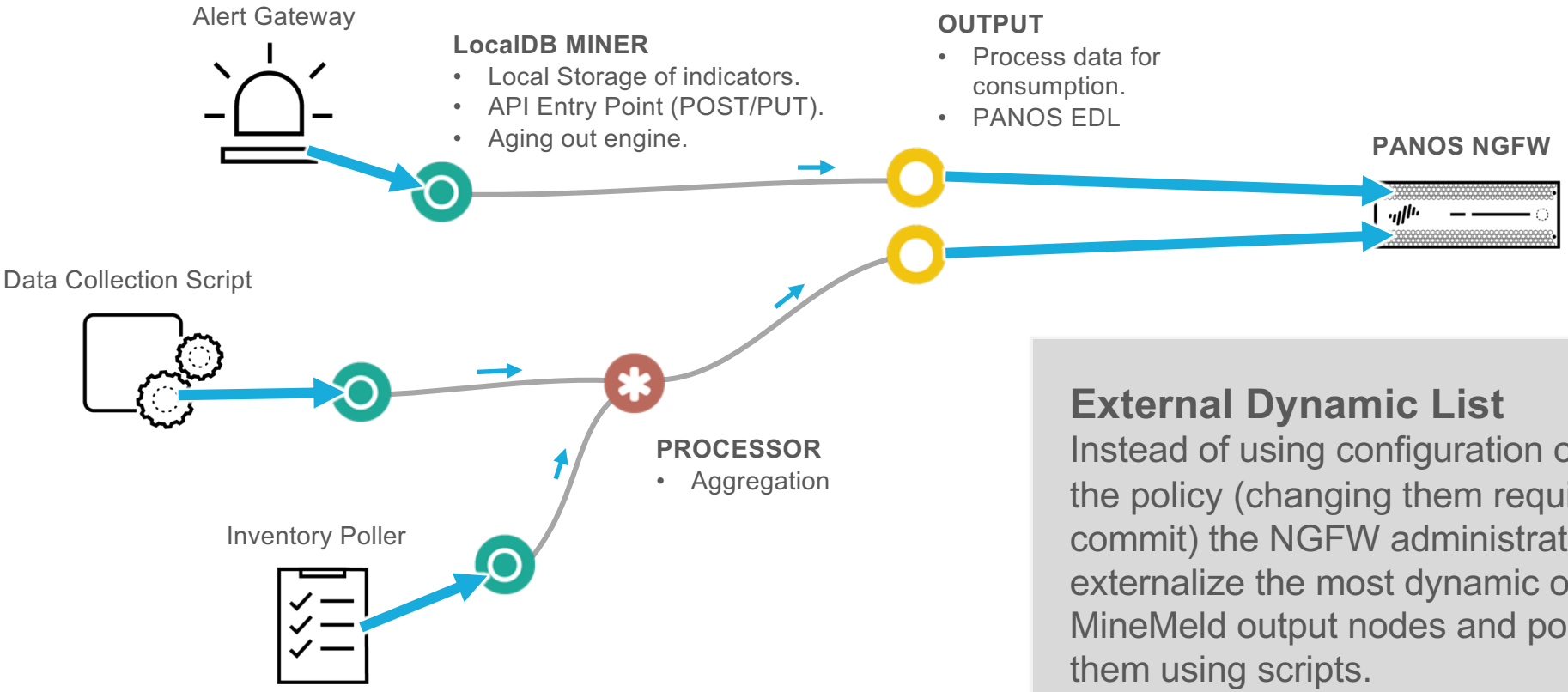
Working with Dynamic Data (IP's, Domains, URL's)



Whitelisting Use Case

MineMeld is responsible of consuming SaaS API's and make their content usable in the NGFW security policy.

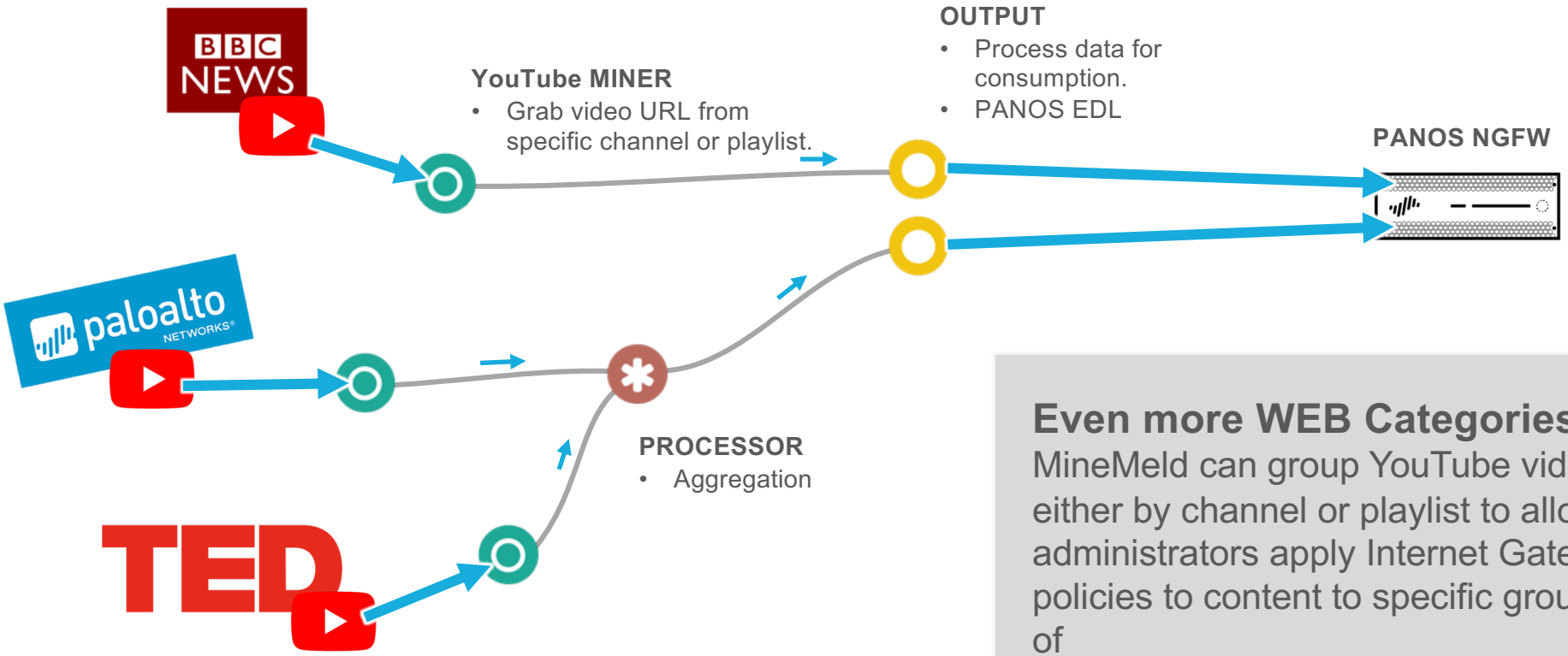
MineMeld as the “last mile” in a Incident Response Chain



External Dynamic List

Instead of using configuration objects in the policy (changing them requires a commit) the NGFW administrator can externalize the most dynamic objects as MineMeld output nodes and populate them using scripts.

Dynamic Custom URL Categories

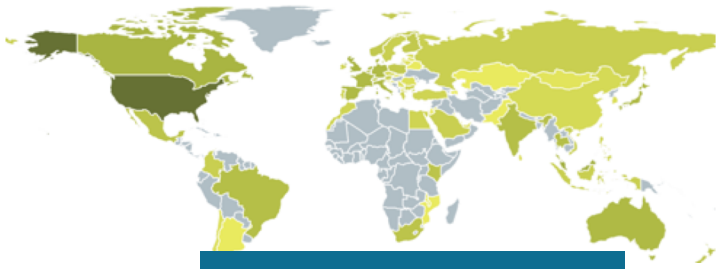


Even more WEB Categories

MineMeld can group YouTube videos either by channel or playlist to allow administrators apply Internet Gateway policies to content to specific groups of

MineMeld Facts

OpenSource
in GitHub



Some 4000s instances running worldwide

Miners for +170 different feeds.

API to interfaces with PANOS HTTP Log Forwarding Feature

+400 containers hosted in AutoFocus

More than 10 different output formats.

Packages ready to consume for Ubuntu, Docker, Azure and AWS

MINEMELD

USE CASES

Part 1: MineMeld for end users

Actionable Third Party Threat Intelligence

MineMeld expands the value proposition of Palo Alto Networks into the the Threat Intelligence space like AutoFocus and other Palo Alto Networks platform components.

Third Party Enforcement

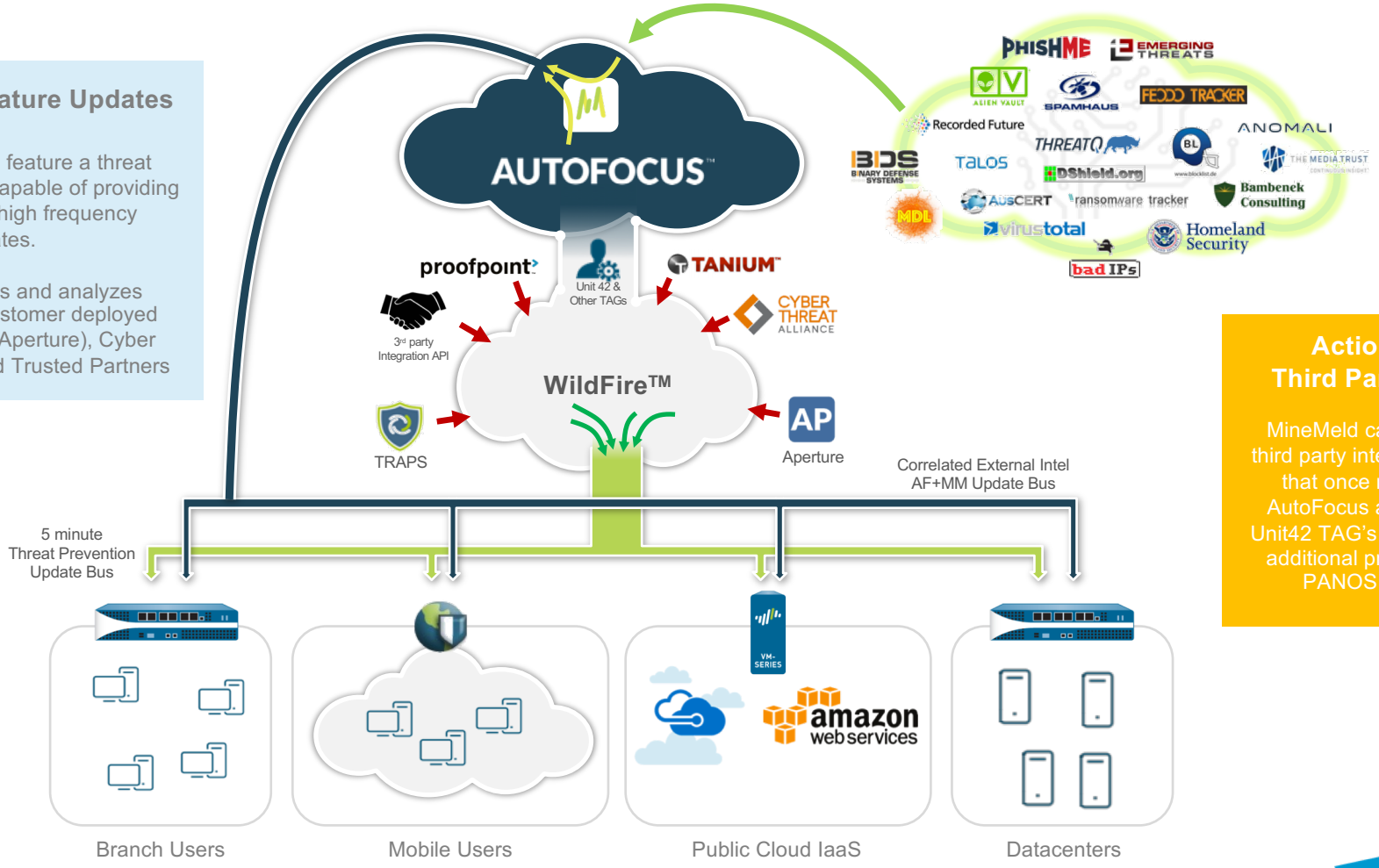
MineMeld can be integrated with security enforcement solutions by third parties.

Actionable Third Party Intelligence

5 minute Threat Signature Updates

Both WildFire and PAN-DB feature a threat signature generation engine capable of providing PA/VM-Series FW's with high frequency signature updates.

WildFire constantly collects and analyzes suspicious samples from customer deployed sensors (TRAPS, PANOS, Aperture), Cyber Threat Alliance Members and Trusted Partners



Actionable Third Party IOC's

MineMeld can consume third party intelligence data that once mixed with AutoFocus artifacts and Unit42 TAG's can generate additional protections to PANOS devices

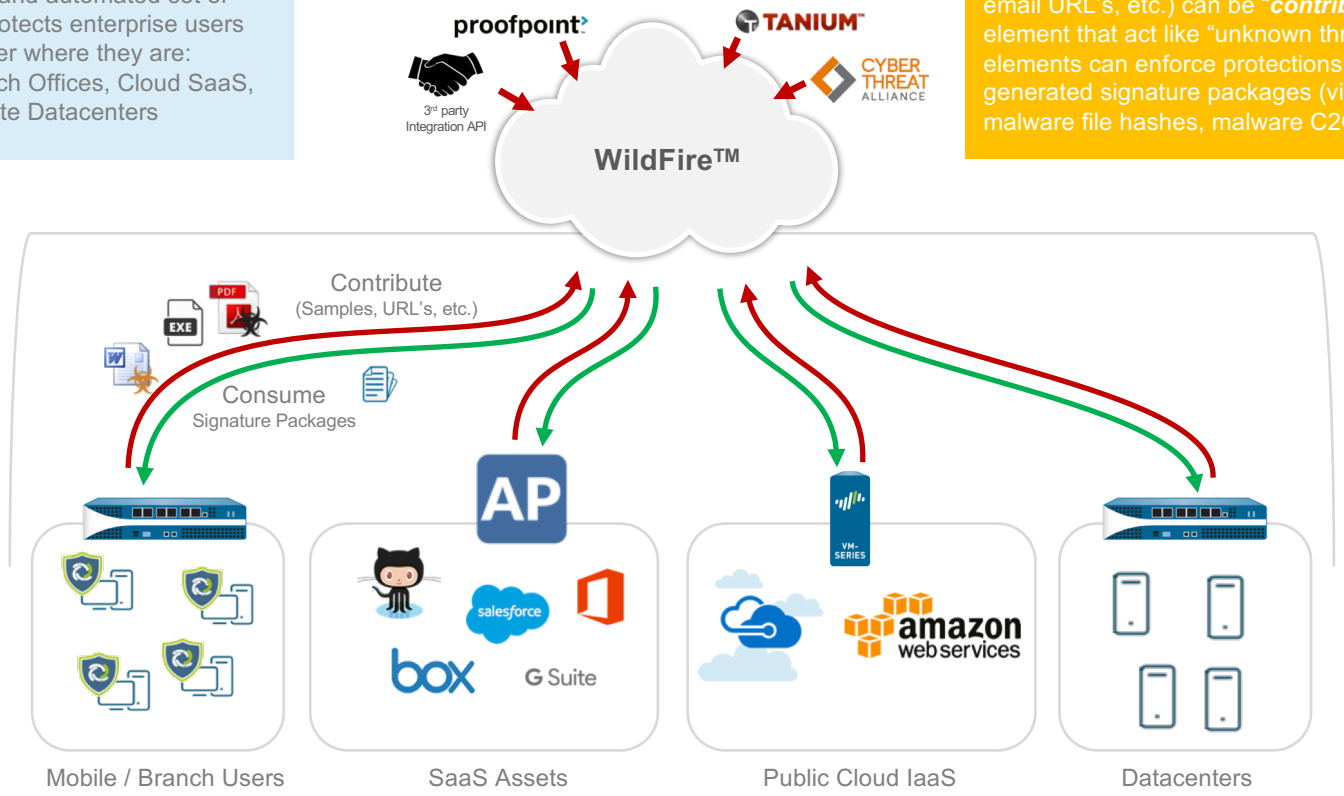
Palo Alto Networks Platform: "Core" Threat Intelligence Ring

The Palo Alto Networks Platform

A highly integrated and automated set of components that protects enterprise users and assets no matter where they are: Mobile Users, Branch Offices, Cloud SaaS, Could IaaS or Private Datacenters

The "Core" Threat Intel Ring

Suspicios samples (binaries, office documents, android packages, email URL's, etc.) can be "***contributed***" to WildFire by any platform element that act like "unknown threat sensors". These same elements can enforce protections by "***consuming***" automatically generated signature packages (virus patterns, malware URL's, malware file hashes, malware C2C patterns, DNS Domains, etc,)



- MANDATORY FOR TARGETED ATTACKS
- HIGH CAPACITY
- AUTOMATED
- EFFICIENT
- SCALABLE

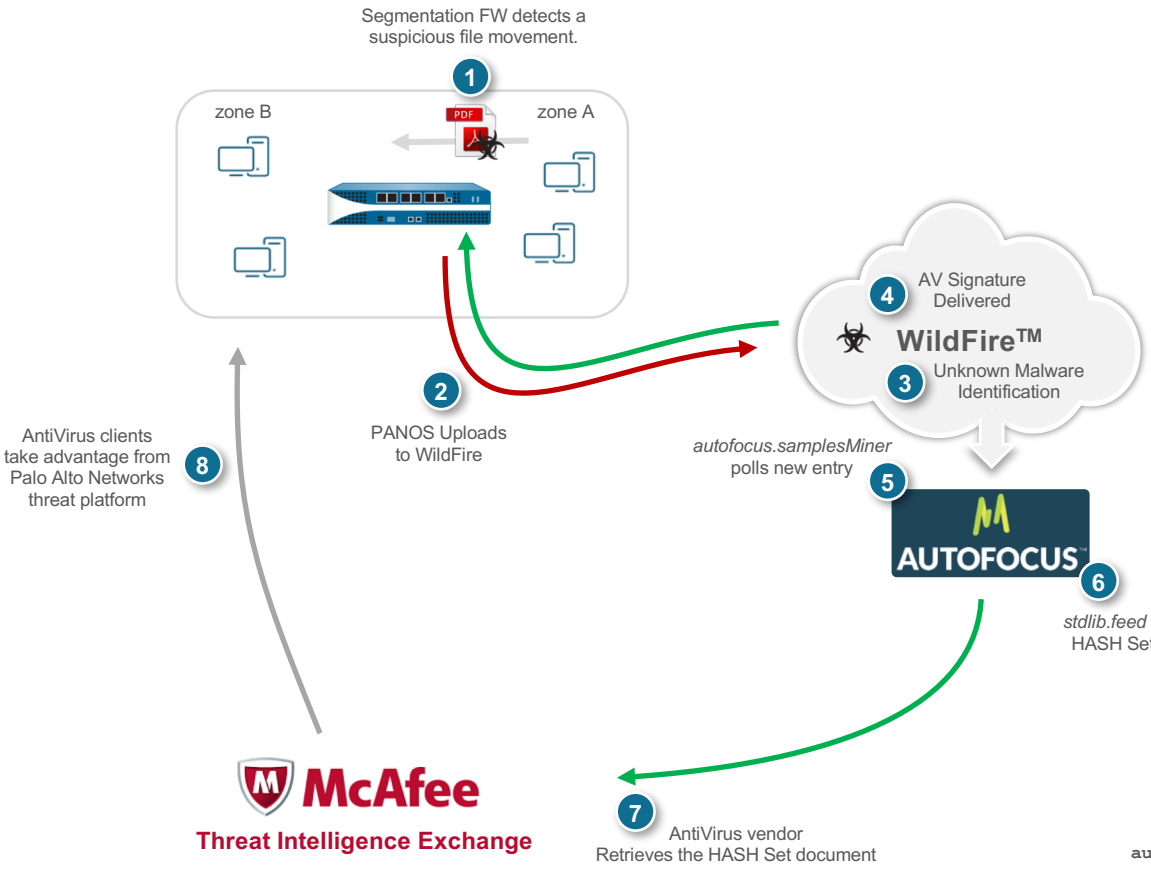
AutoFocus + MineMeld: "Extended" Threat Intelligence Ring

The "Extended" Threat Intel Ring

All WildFire generated artifacts are processed and correlated by AutoFocus using intelligence provided by Palo Alto Networks' Unit42 and other sources.

Identified IOC can be aggregated by MineMeld and converted into actionable documents ready to be consumed by third party enforcers or SIEM's

Extended Ring Use Case 1: Malware HASH sharing

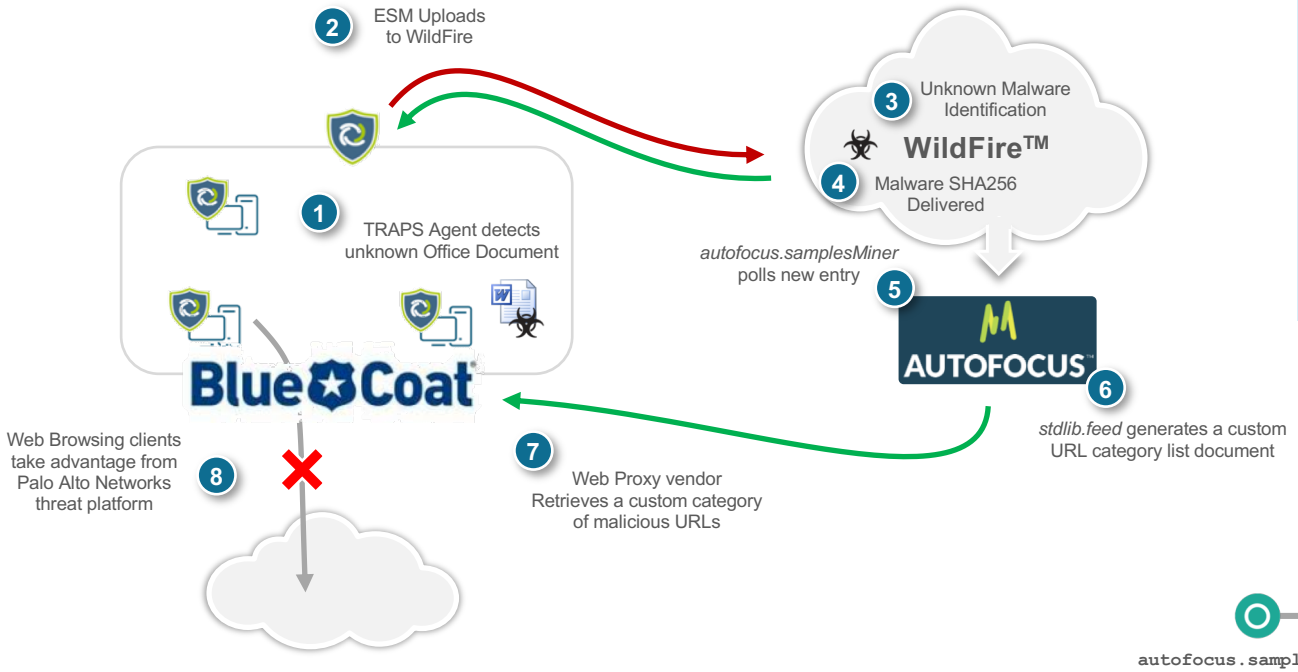


Competitive Advantage
Network Segmentation Deals

Attaching WildFire and AutoFocus to your Enterprise-Class Network Segmentation opportunities gives you differentiation arguments against other FW vendors.

In this case the Palo Alto Networks platform will end up filling the reputation database of the incumbent AV product.

Extended Ring Use Case 2: Malware URL Enforcement



Competitive Advantage
End Point Protection Deals

Attaching AutoFocus to your Enterprise-Class TRAPS opportunities gives you differentiation arguments against other EPP vendors.

In this case the Palo Alto Networks platform will end up filling a custom URL category with malicious URL's in the customer's incumbent Web Proxy product.


DEMO TIME!!!

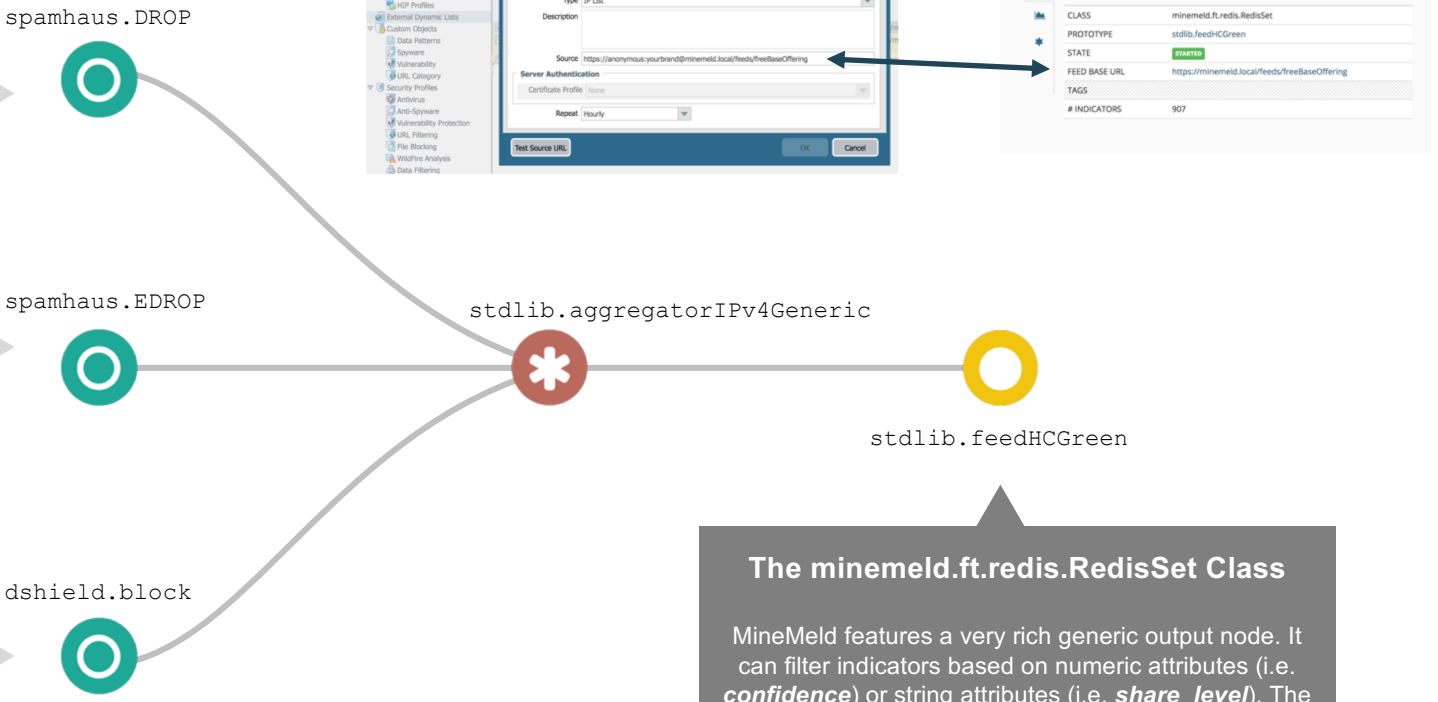
Basic value added feed example

Spamhaus

The Spamhaus Project is an international nonprofit organization whose mission is to track the Internet's spam operations and sources, to provide dependable realtime anti-spam protection for Internet networks, to work with Law Enforcement Agencies to identify and pursue spam and malware gangs worldwide, and to lobby governments for effective anti-spam legislation

Dshield

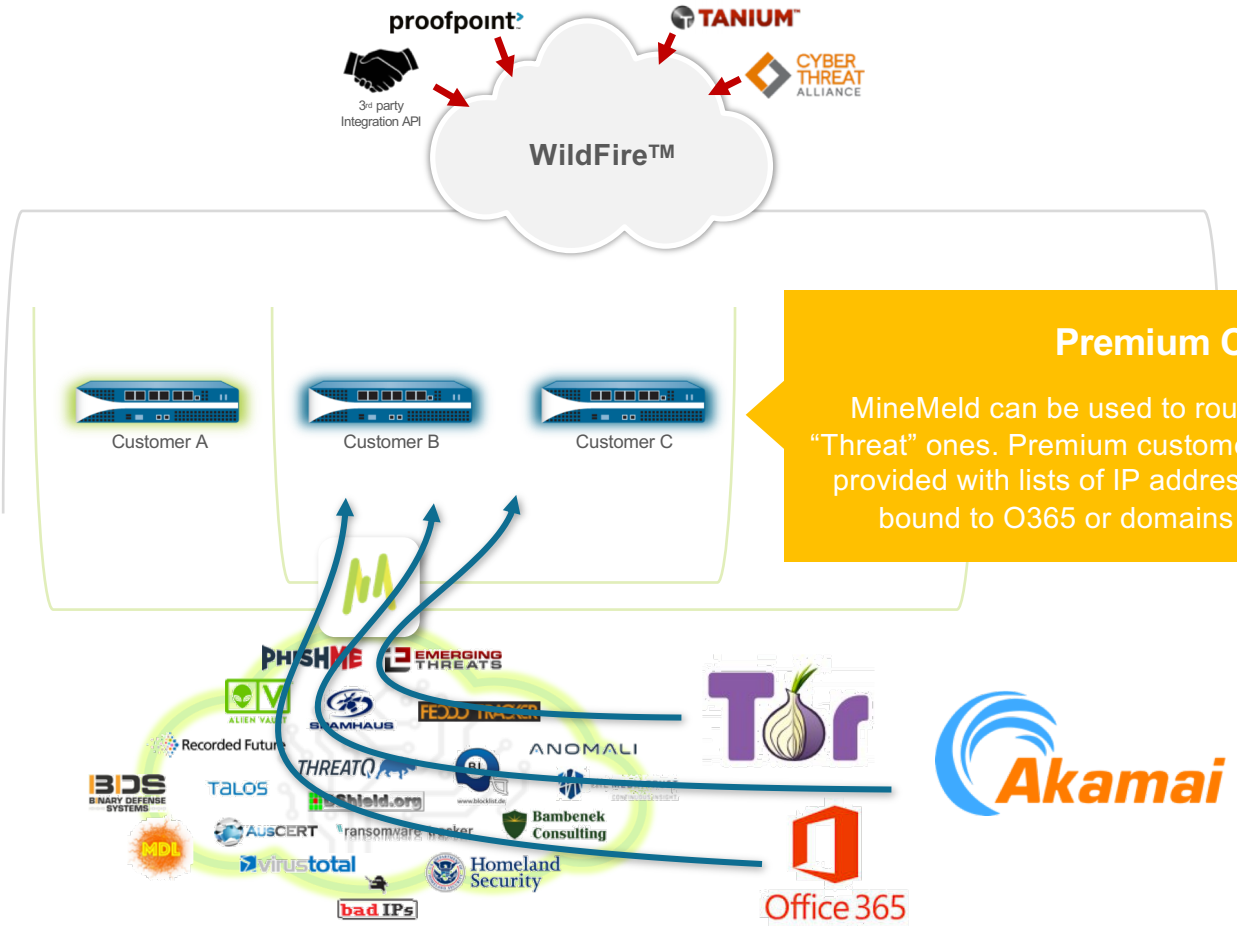
The ISC uses the DShield distributed intrusion detection system for data collection and analysis. DShield collects data about malicious activity from across the Internet. This data is cataloged and summarized and can be used to discover trends in activity, confirm widespread attacks, or assist in preparing better firewall rules.



The minemeld.ft.redis.RedisSet Class

MineMeld features a very rich generic output node. It can filter indicators based on numeric attributes (i.e. ***confidence***) or string attributes (i.e. ***share_level***). The list is provided through basic authentication and,by default, the format is ready to be consumed by PANOS External Dynamic List feature.

Value added feeds for “premium customers”



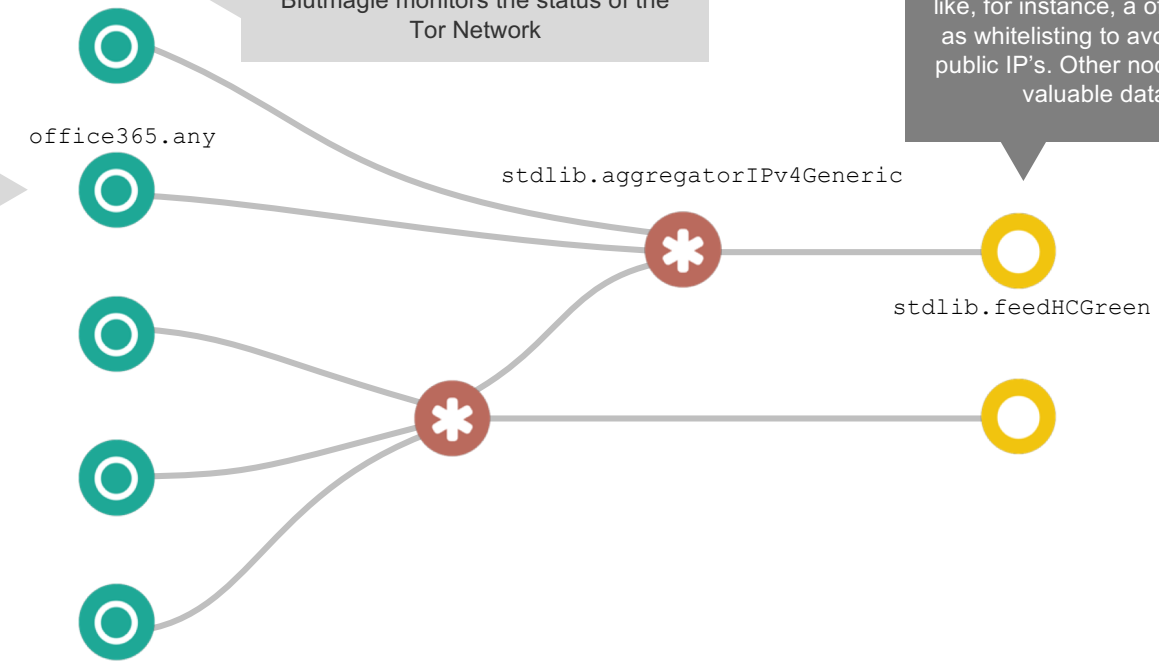
Premium Customers

MineMeld can be used to route any indicator and not only “Threat” ones. Premium customers might be interested in being provided with lists of IP addresses of TOR exit nodes, URLs bound to O365 or domains for a given CDN Provider.

Premium feed example

office365.any (whitelist)

This reference article lists every endpoints used by Office 365. If your organization restricts computers on your network from connecting to the Internet, this article lists the endpoints (FQDNs, Ports, URLs, IPv4, and IPv6 address ranges) that you should include in your outbound allow lists to ensure your computers can successfully use Office 365.



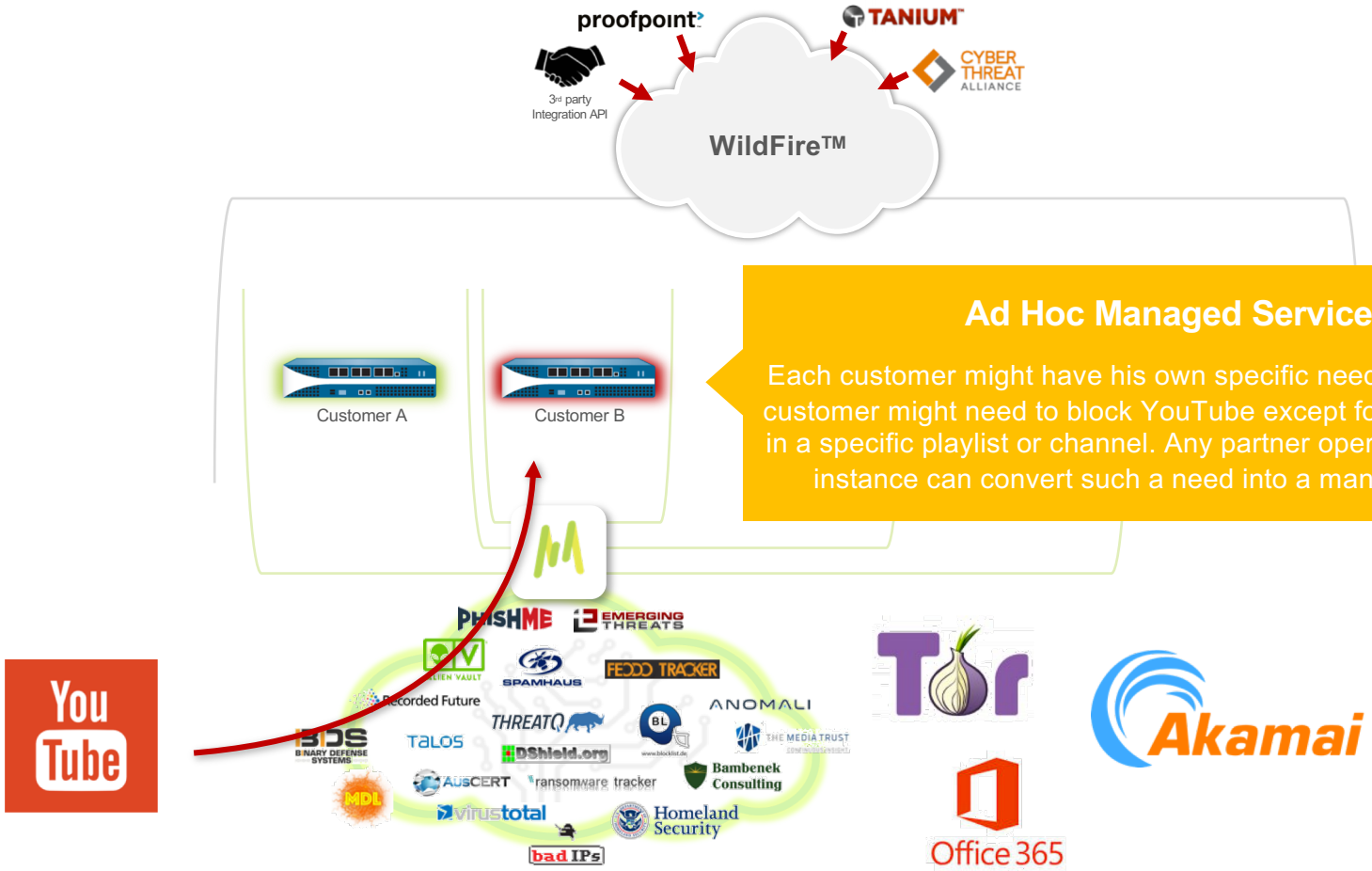
blutmagie.tor_exit_nodes

Blutmagie monitors the status of the Tor Network

Premium Customer Feed

Premium Customers are provided with extra features like, for instance, a office365.any miner node configured as whitelisting to avoid accidental blocking of Microsoft public IP's. Other nodes like tor_exit_nodes can provide valuable data for concerned customers.

Ad Hoc Managed Services



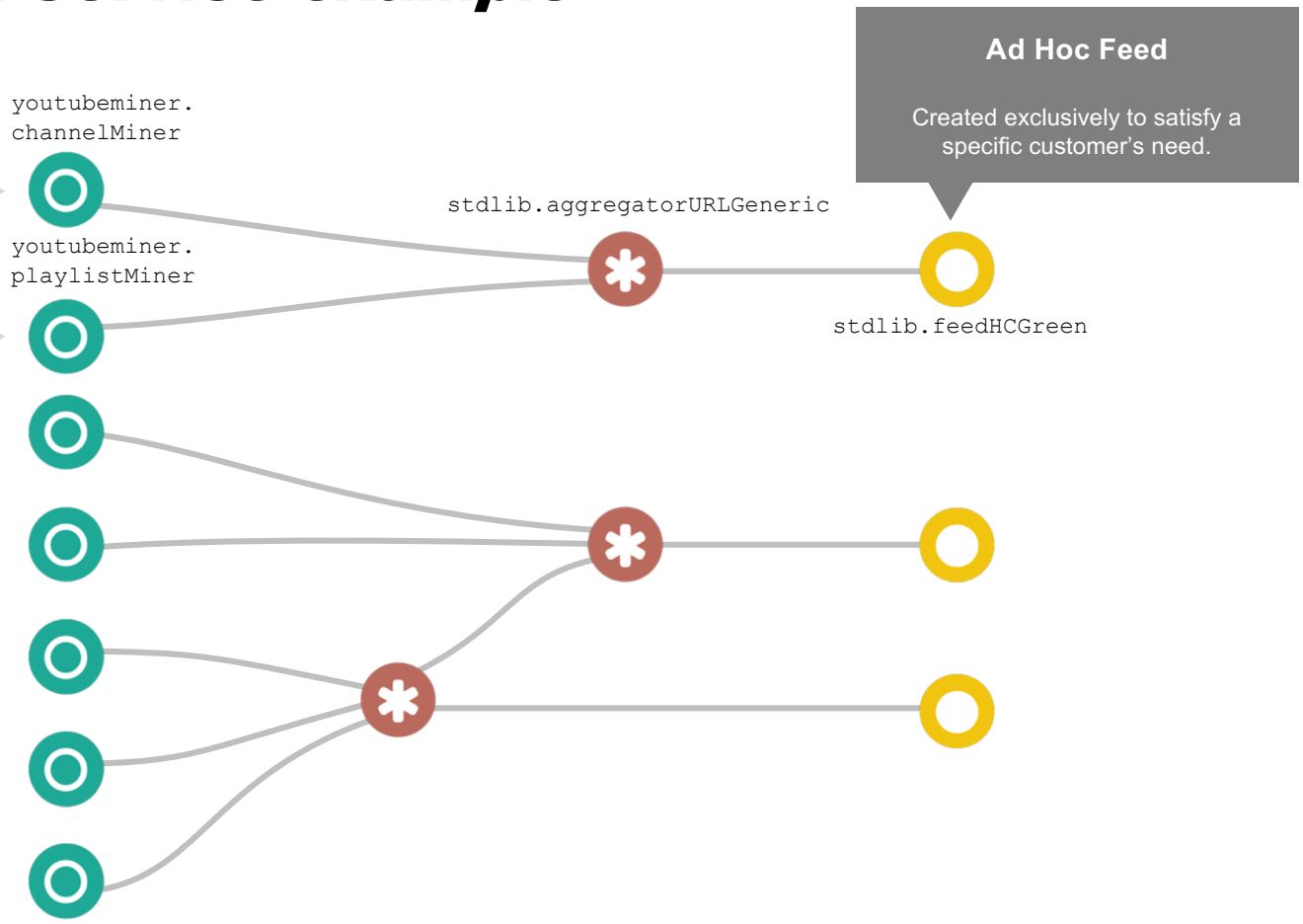
Ad Hoc Managed Services

Each customer might have his own specific needs. For instance a customer might need to block YouTube except for videos provided in a specific playlist or channel. Any partner operating a MineMeld instance can convert such a need into a managed service.

Ad Hoc Managed Service example

youtubeminer.*

YouTube nodes allow you grab list of videos either by channel-id or by playlist-id. A PANOS configuration would provide end customers with a way to block YouTube except for videos collected by these MineMeld nodes.



https://live.paloaltonetworks.com/t5/MineMeld-Articles/Filtering-YouTube-videos-to-only-approved-playlists/ta-p/164928

What if I need to mine CSV?

New prototype:
dshield.block

url https://test.minemeld.com/csv
confidence level to 100
fieldnames
- indicator
- country
- region
- city
- temperature

Ignore_regex pattern as "^(?!https)" (to discard all lines except the ones starting with "https")
Describe the source_name as uclm-csv-temperaturas

Customized Prototype

First New Prototype and then Clone Working Node

https://live.paloaltonetworks.com/t5/MineMeld-Articles/Using-MineMeld-to-extract-indicators-from-a-generic-API/ta-p/218757

What if I need to mine HTML?

New prototype: dshield.block

```
confidence level to 100
fieldnames
fields:
   country:
      regex: '(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code
class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)'
      transform: \4
   region:
      regex: '(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code
class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)'
      transform: \6
   city:
      regex: '(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code
class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)'
      transform: \8
   temperature:
      regex: '(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code
class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)'
      transform: \10
ignore_regex: ^(?!<tr><td>)
indicator:
   regex: '(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code
class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)(<td><code class="small">([^<]+)<\/code><\/td>)'
   transform: \2
Describe the source_name as uclm-html-temperaturas
url with https://test.minemeld.com/html
```

https://live.paloaltonetworks.com/t5/MineMeld-Articles/Using-MineMeld-to-extract-indicators-from-a-generic-API/ta-p/218757

What if I need to mine JSON?

New prototype:
aws.AMAZON

No prefix
extractor: result
fields:
- country
- region
- city
- temperature
indicator: url
url https://test.minemeld.com/json

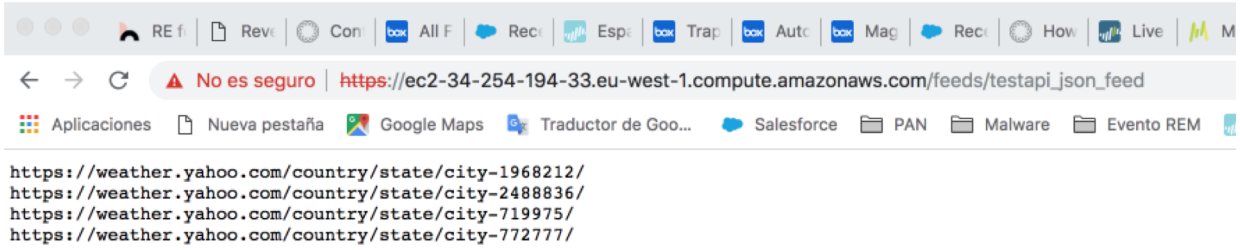
Customized Prototype

First New Prototype and then Clone Working Node

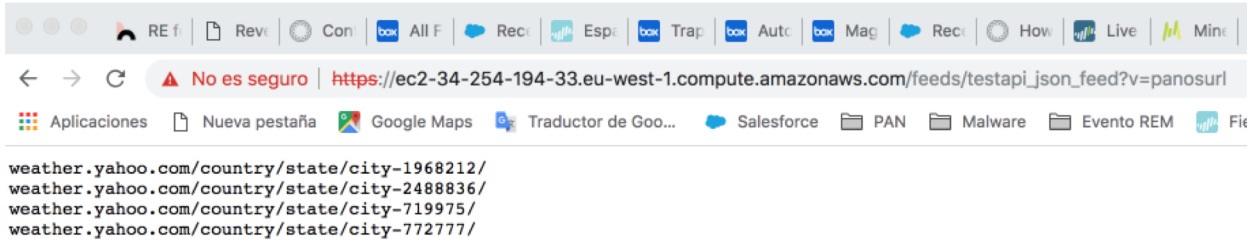
https://live.paloaltonetworks.com/t5/MineMeld-Articles/Using-MineMeld-to-extract-indicators-from-a-generic-API/ta-p/218757

Parameters for the output feeds

https://ec2-34-254-194-33.eu-west-1.compute.amazonaws.com/feeds/testapi_json_feed



https://ec2-34-254-194-33.eu-west-1.compute.amazonaws.com/feeds/testapi_json_feed **?v=panosurl**



https://ec2-34-254-194-33.eu-west-1.compute.amazonaws.com/feeds/testapi_json_feed **?v=json**

https://live.paloaltonetworks.com/t5/Mir


¡GRACIAS!
Red IRIS