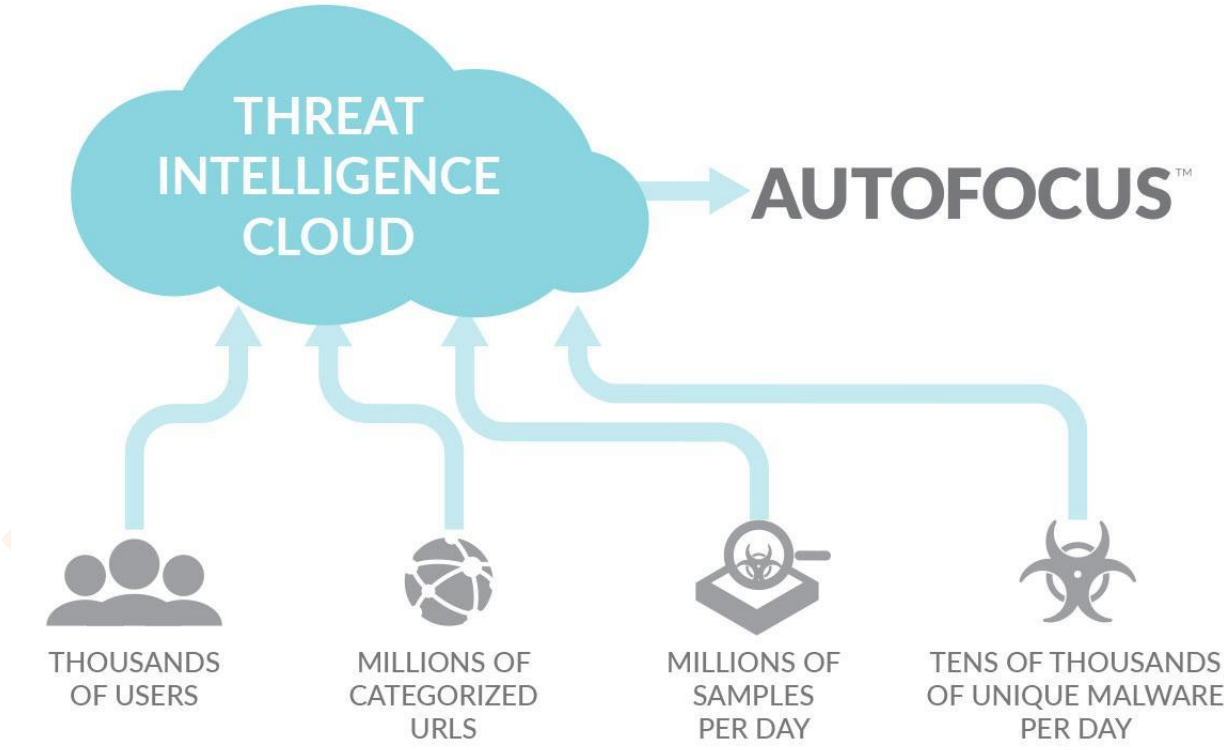
Threat intelligence (AutoFocus)

Highly automated and increasingly sophisticated cyberattacks are occurring in greater volume than ever before. Overburdened security teams, futilely attempting to investigate every threat in the enterprise network, have little time to analyze and understand truly advanced attacks.

Palo Alto Networks AutoFocus enables a proactive, prevention-based approach to network security that puts automation to work for security professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS software and Panorama. AutoFocus speeds the security team's existing workflows, which allows for in-depth investigation into suspicious activity, without additional specialized resources.

AutoFocus is built on a large-scale, distributed computing environment hosted in the Palo Alto Networks Threat Intelligence Cloud. Unlike other solutions, the service makes threat data accessible and actionable at the IoC level and goes beyond simply showing summarized logs from multiple sources in a dashboard. AutoFocus has unprecedented visibility into the threat landscape, with the collective insight of thousands of global enterprises, service providers, and governments feeding the service.

Palo Alto Networks AutoFocus Threat Intelligence Cloud



The service correlates and gains intelligence from:

- WildFire
- URL Filtering with the PAN-DB service
- Palo Alto Networks global passive DNS network
- Palo Alto Networks Unit 42 threat intelligence and research team
- Third-party feeds, including closed- and open-source intelligence

AutoFocus makes over a billion samples and sessions, including billions of artifacts, immediately actionable for security analysis and response efforts. AutoFocus extends the Security Operating Platform with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows. Together, the platform and AutoFocus move security teams away from legacy manual approaches that rely on aggregating a growing number of detection-based alerts and post-event mitigation, to preventing sophisticated attacks and enabling proactive hunting activities.

Priority alerts and tags

AutoFocus enables you to distinguish the most important threats from everyday commodity attacks, contextualizing events on your network with tags. Unique to AutoFocus, tags enrich your visibility into the most critical threats, with contextual intelligence that lets you know which malware families, campaigns, threat actors, malicious behaviors, and exploits are being used against you.

When a tag matches an event on your network, a priority alert is sent via email, within the AutoFocus dashboard or via HTTP post, with the full tag context included. Alerts are highly customizable, which enhances your existing security workflow with prioritization and context for the most critical threats.

Tags can be created for any host or network-based indicator in AutoFocus to alert you when a specific threat has been observed in your organization or industry. All tags are searchable so that you can quickly identify associated malicious samples or indicators.

As new threats are identified, Palo Alto Networks Unit 42, your own organization, and the global community of AutoFocus experts add new tags to the service. AutoFocus is the primary analysis tool used by Unit 42 to identify new threats, correlate global data, identify connections between malicious samples, and build adversary or campaign profiles.

With AutoFocus and the Security Operating Platform, security teams can:

- Determine how targeted or unique a threat seen on their network is
- Investigate related malicious samples
- Identify suspicious DNS queries with domain resolution history

Threat correlation

When security teams conduct threat analysis, they must quickly identify which IoCs represent the best path to remediation. For an active or ongoing compromise, the speed of investigation and the ability to meaningfully correlate data is critical. Each file has hundreds, potentially thousands, of artifacts, with only a small number of unique IoCs than can be correlated to the larger profile of an adversary or related attacks.

AutoFocus uses an innovative statistical analysis engine to correlate billions of artifacts across a global dataset and bring forward unique IoCs likely associated with targeted attacks. The service automatically applies a unique visual weighting system to identify unique and critical IoCs, which guides analysis and incident response efforts down the most relevant path.

AutoFocus allows you to build sophisticated multilayer searches at the host and network-based artifact levels, and target your search within industry, time period, and other filters. These searches allow you to make previously unknown connections between attacks and plan your incident response actions accordingly.

When further analysis is required, security teams can switch between AutoFocus and PAN-OS software or Panorama, with pre-populated searches for both systems. AutoFocus provides the entirety of Palo Alto Networks threat intelligence, which dramatically reduces the time it takes to conduct analysis, forensics, and hunting tasks.

Actionable intelligence

Security teams require more than a way to prioritize, analyze, and correlate threat intelligence – they need a way to convert it into actionable controls to prevent future attacks. AutoFocus enables you to create new protections for the Security Operating Platform by exporting high-value IoCs from the service into PAN-OS software external dynamic lists to instantly block malicious URLs, domains, and IP addresses. AutoFocus can also export IoCs to third-party security devices via a standard CSV format. Security teams can use AutoFocus to identify unique, targeted attacks against their organization and take direct action to mitigate and prevent them.

Threat analysis, forensics, and incident response teams often rely on a broad range of scripts, open-source tools, security devices, and services to investigate potential security incidents. AutoFocus can dramatically reduce the time required to investigate by enriching third-party services through:

- **Open API support.** The AutoFocus API is built on an easy-to-use *representational state transfer* (RESTful) framework and allows for integrations into hundreds of use cases, such as sending threat intelligence data to existing SIEM tools. This framework makes data available for additional threat analysis or custom threat-blocking automations.
- **Remote sweeping capability.** Security teams can move from indicators in the service to internal and third-party external systems directly from AutoFocus. Teams can define up to 10 external systems, which lets them continue their analysis seamlessly across their entire infrastructure, such as correlating logs from next-generation firewalls or triggering searches in SIEM tools.

- **Support for STIX data format.** AutoFocus provides out-of-the-box integration with *Structured Threat Information Expression* (STIX) infrastructure and makes data available for export in the STIX data format.

Key Terms

Representational state transfer (REST) is an architectural programming style that typically runs over HTTP. It is commonly used for mobile apps, social networking websites, and mashup tools.

Structured Threat Information Expression (STIX) is an *Extensible Markup Language* (XML) format for conveying data about cybersecurity threats in a standardized format.

Extensible Markup Language (XML) is a programming language specification that defines a set of rules for encoding documents in a human-readable and machine-readable format.

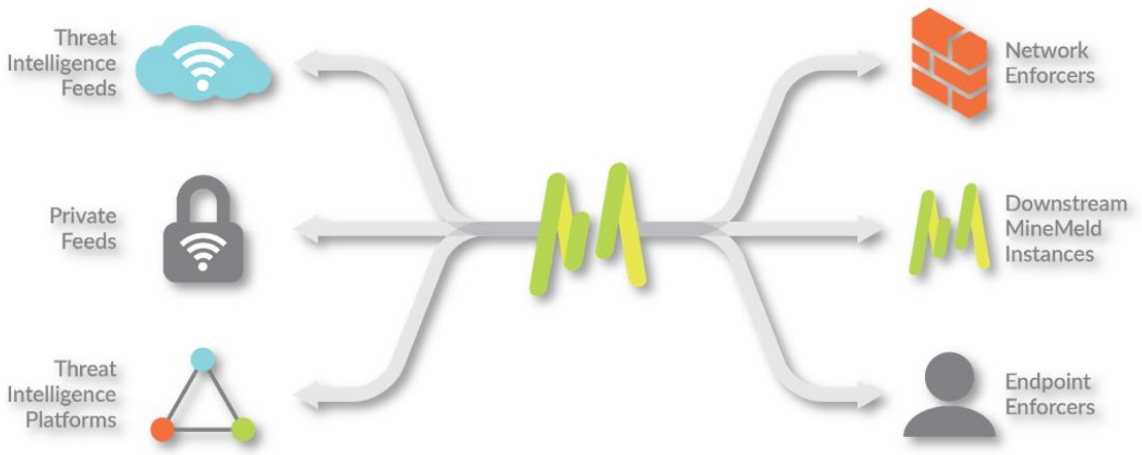
Threat indicator sharing (MineMeld)

To prevent successful cyberattacks, many organizations collect indicators of compromise (IoCs) from various threat intelligence providers with the intent of creating new controls for their security devices. Unfortunately, legacy approaches to aggregation and enforcement are highly manual in nature, often creating complex workflows and extending the time needed to identify and validate which IoCs should be blocked.

MineMeld is an open-source application that streamlines the aggregation, enforcement, and sharing of threat intelligence. MineMeld is available directly on GitHub and on prebuilt virtual machines (VMs) for easy deployment. With an extensible modular architecture, anyone can add to the MineMeld functionality by contributing code to the open-source repository.

MineMeld supports a variety of use cases, with more being added each day by the community, including:

- Aggregating and correlating threat intelligence feeds
- Enforcing new prevention controls, including IP address blacklists
- Evaluating the value of a specific threat intelligence feed for your environment
- Extracting indicators from Palo Alto Networks device logs and sharing them with other security tools
- Sharing indicators with trusted peers
- Identifying incoming sessions from Tor exit nodes for blocking or strict inspection
- Tracking Office365 URLs and IP addresses



MineMeld aggregates and correlates threat intelligence feeds.

MineMeld allows you to aggregate threat intelligence across public, private, and commercial intelligence sources, including between government and commercial organizations.

MineMeld simplifies the collection and correlation of intelligence across:

- Commercial threat intelligence feeds
- Open-source intelligence (OSINT) providers
- Threat intelligence platforms
- Information sharing and analysis centers (ISACs)
- Computer emergency response teams (CERTs)
- Other MineMeld users

After indicators are collected, MineMeld can filter, deduplicate, and consolidate metadata across all sources, which allows security teams to analyze a more actionable set of data, enriched from multiple sources, for easier enforcement.

MineMeld natively integrates with the Palo Alto Networks Security Operating Platform to automatically create new prevention-based controls for URLs, IP addresses, and domain intelligence derived from all sources feeding into the tool. Organizations can simplify their workflows for blocking IoCs with external dynamic lists and dynamic address groups (DAGs), without spending additional resources to manage block lists, including the automated timeout of expired indicators. MineMeld also integrates with the AutoFocus contextual threat intelligence service to allow organizations to identify high-value, targeted indicators – in AutoFocus – and block them on their next-generation firewalls with export lists and MineMeld.