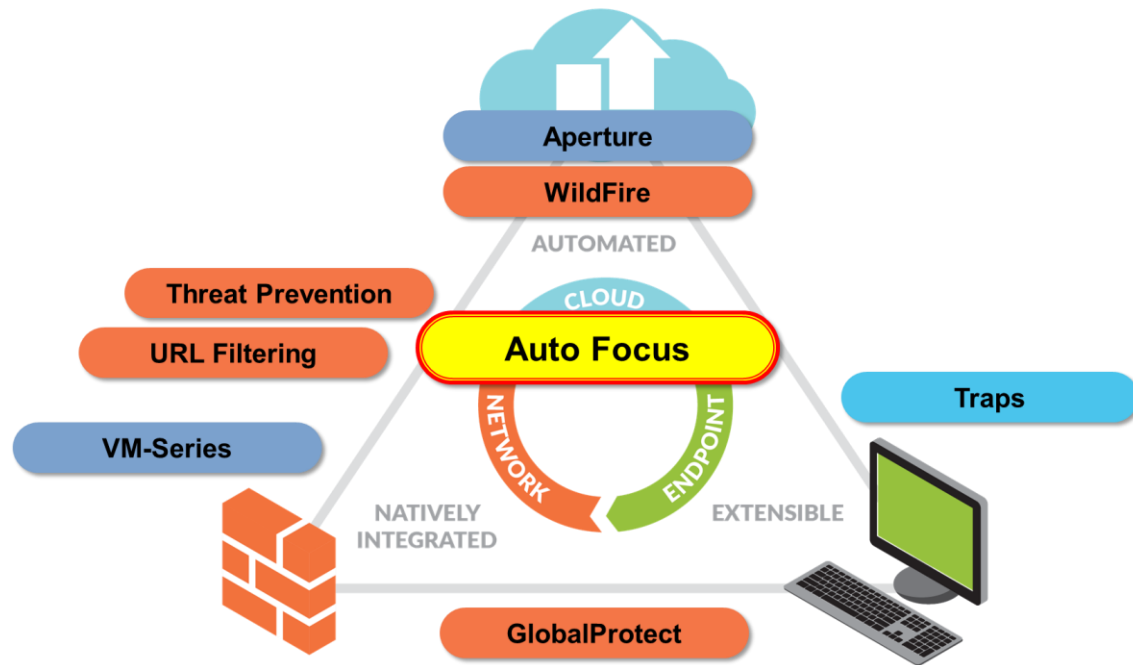


脅威インテリジェンスクラウドサービス  
**Auto Focus**のご紹介



# 次世代 セキュリティ プラットフォーム

脅威インテリジェンスクラウド



次世代ファイアウォール

アドバンスド  
エンドポイント プロテクション



# 脅威インテリジェンスクラウド: Wild Fire

- クラウド上にあるサンドボックス環境でファイルを分析し、未知のマルウェアを発見 & 防御するためのサービス
- 世界中のお客様環境で発見されたマルウェアに対して、シグネチャを自動生成し配信

※WildFire サービスの利用にあたっては、利用する次世代ファイアウォール上で追加のサブスクリプションが必要です



グローバルで10,000社・30,000台以上が利用  
検査されるファイル数:

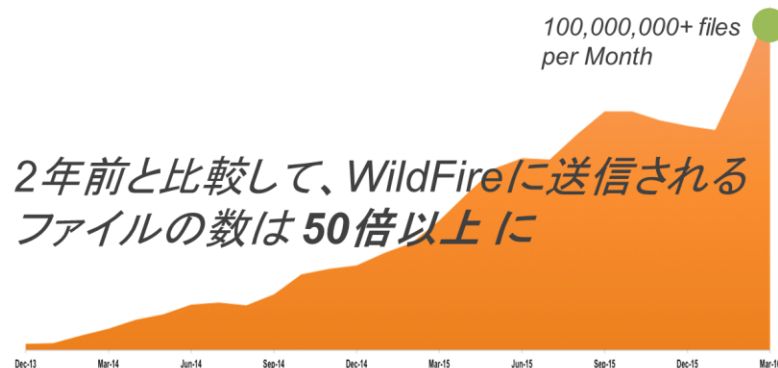
一日当たり 約300万 / DAY

発見されるマルウェア:

一日当たり 約4万 / DAY

100,000,000+ files  
per Month

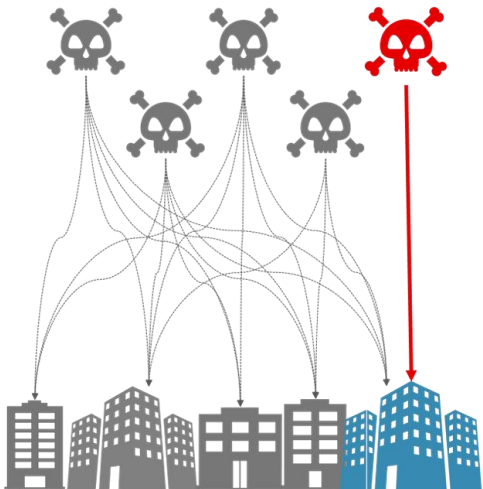
2年前と比較して、WildFireに送信される  
ファイルの数は50倍以上に



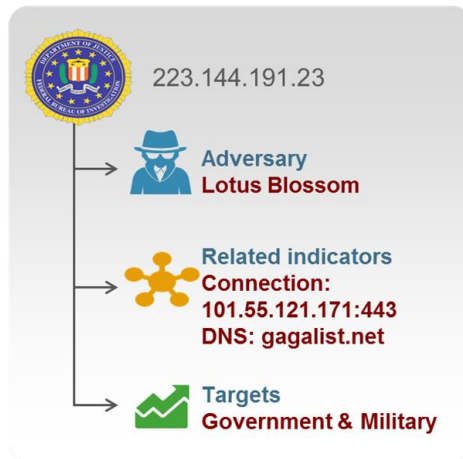
WildFire 上で検査されるファイル数の推移

# 脅威インテリジェンスを活用したセキュリティ対策

## 重要なイベントの優先度の設定



## 兆候とインシデントに コンテキストを付与



## 即時 または プロアクティブな対応



# Auto Focus の提供するメリット



重要なイベントを発見

クリティカルなイベントを  
タグ付けし、統計的に分析



攻撃の背後に誰がいるのか




攻撃者と攻撃手法を特定






インシデントへの対応

関連するインジケータをブロック

 unit42

 CryptoWall  
 Blackpos  
 ShellCrew



 sty\_fake\_google\_update  
 IL\_Veronika\_Carbanak  
 IL\_slevin\_DoubleFantasy

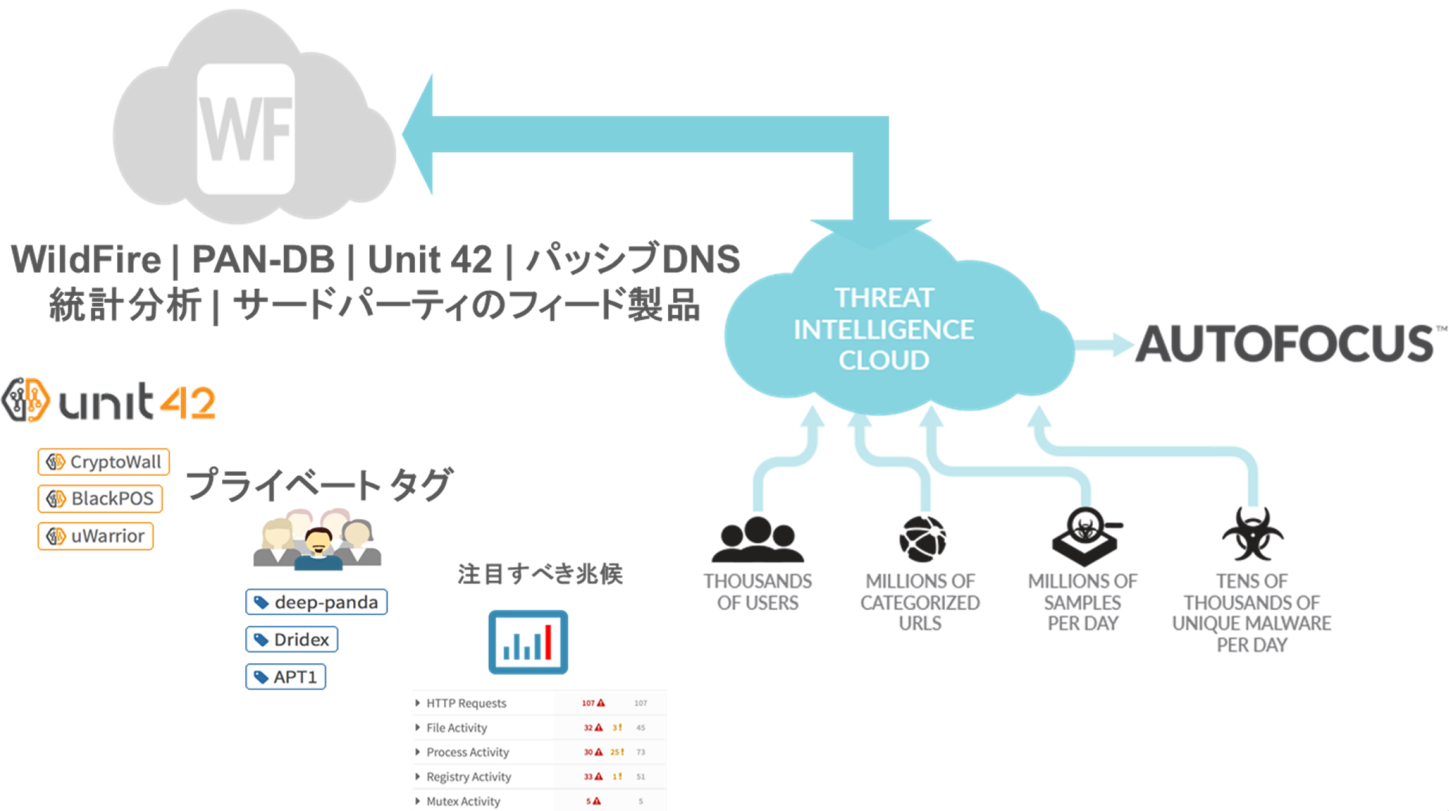


pDNS



- 10,000社 Wild Fire利用
- 10億のサンプル
- 毎日300 - 500万増加
- 数十億の痕跡
- UNIT 42 インテリジェンス
- 広範囲な関連付け

# Auto Focusに蓄積される脅威データ



# 統合ログ / Auto Focus & Panorama連携 (PAN-OS7.1~)



ワークフローの  
シンプル化

統合ログ / Auto Focus &  
NGFW & Panorama連携

[統合ログ表示機能]

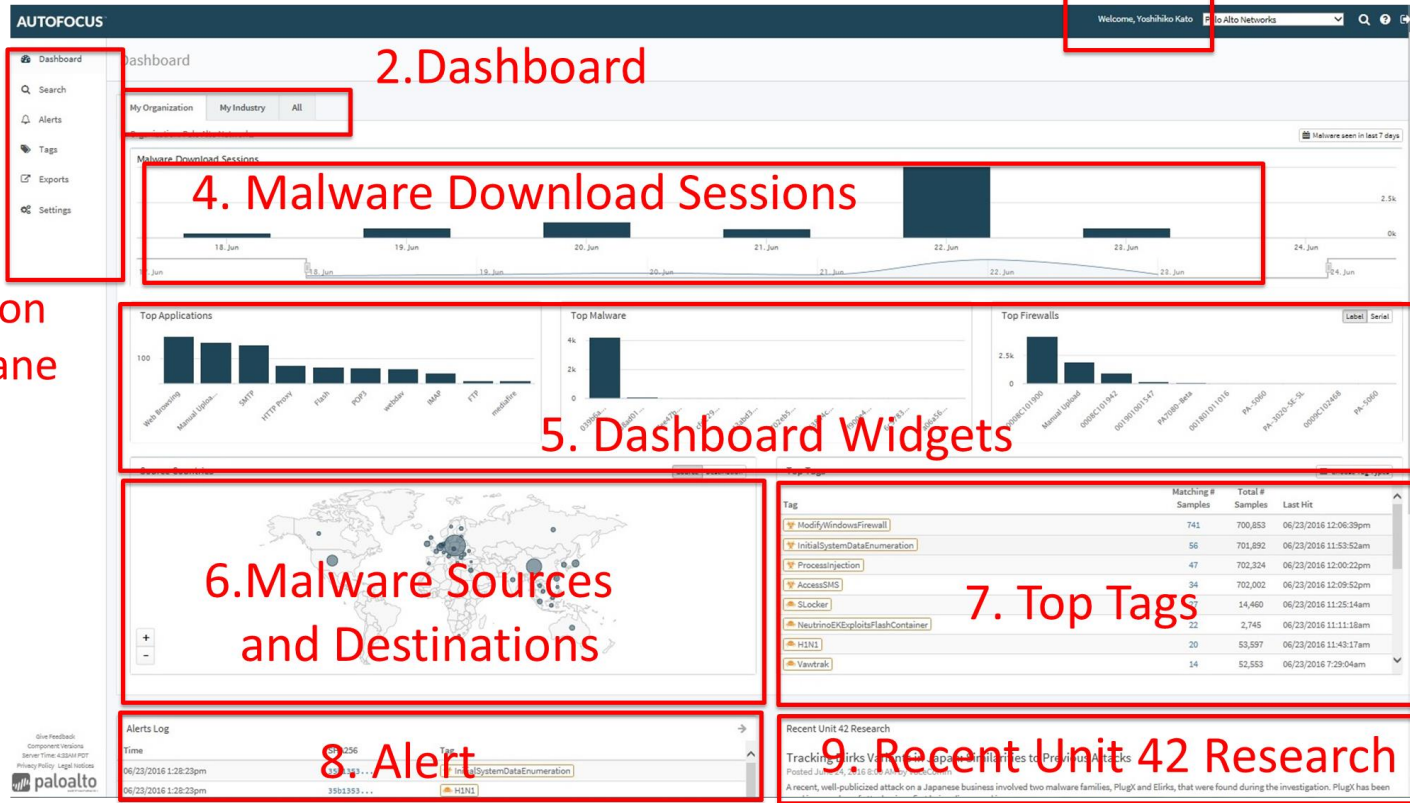
各種ログの調査を容易に行うため各種ログを統合表示

- トラフィックログ
- 脅威防御ログ
- URLログ
- Data Filteringログ
- WildFireログ

A screenshot of the Palo Alto Networks Panorama log viewer interface. The interface shows a sidebar on the left with various log categories like Traffic, Threat, and Security. The main area displays a table of logs with columns for Log Type, Receive Time, Log Subtype, Source Zone, Destination Zone, Source User, Destination Address, Dest. Port, Application, Action, and Log. The table contains multiple rows of log entries, all with a status of 'allow'.

# Auto FocusのDashboard画面

1. Support Account



3. Navigation Pane

4. Malware Download Sessions

2. Dashboard

5. Dashboard Widgets

6. Malware Sources and Destinations

7. Top Tags

8. Alert

9. Recent Unit 42 Research



# Auto FocusのDashboard画面

<b>1.Support Account</b>	ログインしているアカウントを表示します
<b>2.Dashboard</b>	<p>表示するデータのコンテキストを "My Organization", "My Industry", "ALL" の 3 つのタブから選択します。</p> <p>Dashboard 上に表示される脅威情報とアクティビティは、選択したコンテキストの情報を表示します。</p> <ul style="list-style-type: none"><li>・ My Organization – お客様のデバイスで検知された情報</li><li>・ MY Industry – お客様が所属する業種の他のお客様デバイスで検知された情報</li><li>・ All – すべてのお客様</li></ul> <p>Dashboardは、表示するデータを以下の期間で定義することが可能です。</p> <p>Last 7日(デフォルト)、30日、90日、Last 6ヶ月、All time(検知開始以降すべて)</p>
<b>3.Navigation Pane</b>	<p>3.ナビゲーションペインは、グローバル及び過去の脅威情報の検索、マルウェアタグやアラートを管理するための項目で、以下の項目で構成されています。</p> <ul style="list-style-type: none"><li>・ Search – 検索エディタでは、ブーリアン理論(真と偽)を使用して、“My Samples”、“Public Samples”、“All Samples” のカテゴリ毎に自由形式の検索を実行することができます。</li><li>・ Alert – タグをベースにアラートを設定します。Private、Public サンプルと一致した際にUnit 42タグ、Publicタグ、Private タグのアラート等を生成します。</li><li>・ Tags – タグは、過去や新しいサンプルデータに対して比較される条件です。お客様自身のタグを作成することが可能です。また、Unit42も既知の脅威の検出を助けるためにAutofocus 上でタグを公開しています。Tagのページでは、“Private タグ”、他のAutofocus ユーザによって共有された”public タグ”、Unit 42 タグを参照することが可能です。</li><li>・ Export List – IPアドレスやURL、ドメイン情報をCSVファイルに出力することが可能です。</li><li>・ Settings – Autofocus ポータルの設定を更新します</li></ul>
<b>4. Malware Download Sessions</b>	<p>マルウェアダウンロードセッションヒストグラムは、マルウェア最初に検知した時間から選択した時間のレンジで、マルウェアセッションを表示します。</p> <p>既知のマルウェアセッションは反映されません。</p>

# Auto FocusのDashboard画面

<b>5. Dashboard Widgets</b>	<p>Dashboard ウィジェットは、選択されたコンテキスト毎("My Organization", "My Industry", "ALL")と選択した時間帯に応じて、Top10の情報を表示します。</p> <ul style="list-style-type: none"><li>• Top Applications – 最も使用された10のアプリケーションを表示</li><li>• Top Malware – 検知数が高い10のマルウェアサンプルを表示</li><li>• Top Firewalls – マルウェアサンプルを検知したセッション数が最も多い10のFirewallを表示(My organization タブ選択時のみ)</li><li>• Target Industries – マルウェアを最も検知した10のインダストリーを表示(Allタブを選択した場合のみ)</li></ul> <p>ドリルダウン&amp;ダッシュボードウィジェットをクリックすると、"Search"画面に移動し、対象の情報を検索することが可能です。</p>
<b>6. Malware Sources and Destinations</b>	<p>地理的にマルウェアのホットスポットを表示します。Source(送信元)、Destination(宛先)が選択可能です。</p> <p>Source(送信元)は、オリジナルのマルウェアセッションレートが高い国を表示します。</p> <p>Destination(宛先)は、攻撃を受けているレートが高い国を表示します。</p> <p>表示した円の大きさはアクティビティが高いことを意味します。該当のマップは拡大することが可能で、マルウェアセッション数を調べることが可能です。</p>
<b>7. Top Tags</b>	<p>Autofocus Tag にマッチしたサンプル数が多いタグを表示します。以下のタグカテゴリ毎、又は組み合わせて表示することも可能です。</p> <p>このTop Tagsリストは、マルウェアセッションヒストグラムで選択した期間で、指定したカテゴリのタグにマッチしたサンプル数を降順に表示します。</p>
<b>8. Alert</b>	<p>Unit 42 Autofocus タグ、有効にしたPublic、Private タグにマッチした最新の50件のマルウェアのアラート等を表示します。</p>
<b>9. Recent Unit 42 Research</b>	<p>パロアルトネットワークスの脅威インテリジェンスチームのUnit42 が配信する最新の研究、ニュースのクイックリンクを表示します。</p>

# Auto FocusのSearch画面

The screenshot shows the Auto Focus Search interface. The top navigation bar includes the 'AUTOFOCUS' logo, a user greeting 'Welcome, Yoshihiko Kato', and a dropdown menu for 'Palo Alto Networks'. The left sidebar contains navigation items: Dashboard, Search, Alerts, Tags, Exports, and Settings. The main content area is titled 'Search' and includes a search input field, a 'Search' button, and a 'Remote Search' button. Below the search bar are tabs for 'Samples', 'Sessions', 'Statistics', and 'Domain, URL & IP Address Information'. A table below these tabs provides a summary of each category. At the bottom, a search filter configuration area is shown with a dropdown menu for categories and a text input for search conditions.

**⑤ 検索条件入力後 Searchボタンをクリック**

**① 検索条件の追加・削除**

Category	Description
Samples	Wildfireのサンプルの解析結果概要。「My Samples」、「Public Samples」、「All Samples」から対象を選択
Sessions	対象のサンプルに関連するセッション情報の概要
Statistics	検索結果に表示対象を絞り込んだ「Dashboard」情報
Domain, URL & IP Address Information	指定条件を含むサンプルに関連する接続先情報 (Passive DNSやPAN-DBなどの評価情報を表示)

**② カテゴリ ③ 検索条件 ④ 検索対象の数値を入力**

**※ 検索条件のカテゴリを指定**

# Search例: タグ検索例 (Petya\*/ランサムウェア)

※2016年3月に発生、HDDのMFTを書き換えるランサムウェア。MBRを書き換えることで起動時にメッセージを表示。

Search

Match the following condition:

Tag is in the list Petya x

Search Remote Search

Samples Sessions Statistics Domain, URL & IP Address Information

My Samples Public Samples All Samples Found 28 samples in 7 seconds

Sort by: First Seen

First Seen	WildFire Verdict	SHA256	File Size (Bytes)	File Type	Tags
06/15/2016 9:46:11pm	Malware	8dfff25a3787389a95bfc3ed7b993430b5513ded63535df914a7ff89e6e945d	1,011,712	PE	Petya
06/13/2016 9:40:23am	Malware	108e17d98c3ef17d5d377487fb1.....e2a571f8acd4b41f7ef23a9da0	230,921	PE	Petya
			120,832	PE	Petya
			424,960	PE	Petya
			248,288	PE	Petya
			794,692	PE	Petya
			797,892	PE	Petya
			797,892	PE	Petya
			534,528	PE	Petya
			237,568	PE	Petya
			230,923	PE	Petya
			498,176	PE	Petya
			733,184	PE	Petya
			230,912	PE	Petya

Samplesタブ

Search

Match the following condition:

Tag is in the list Petya x

Search Remote Search

Private Public

Sample 9812d29... Petya Add Tag

File Analysis Network Sessions Coverage

WildFire AV Signature

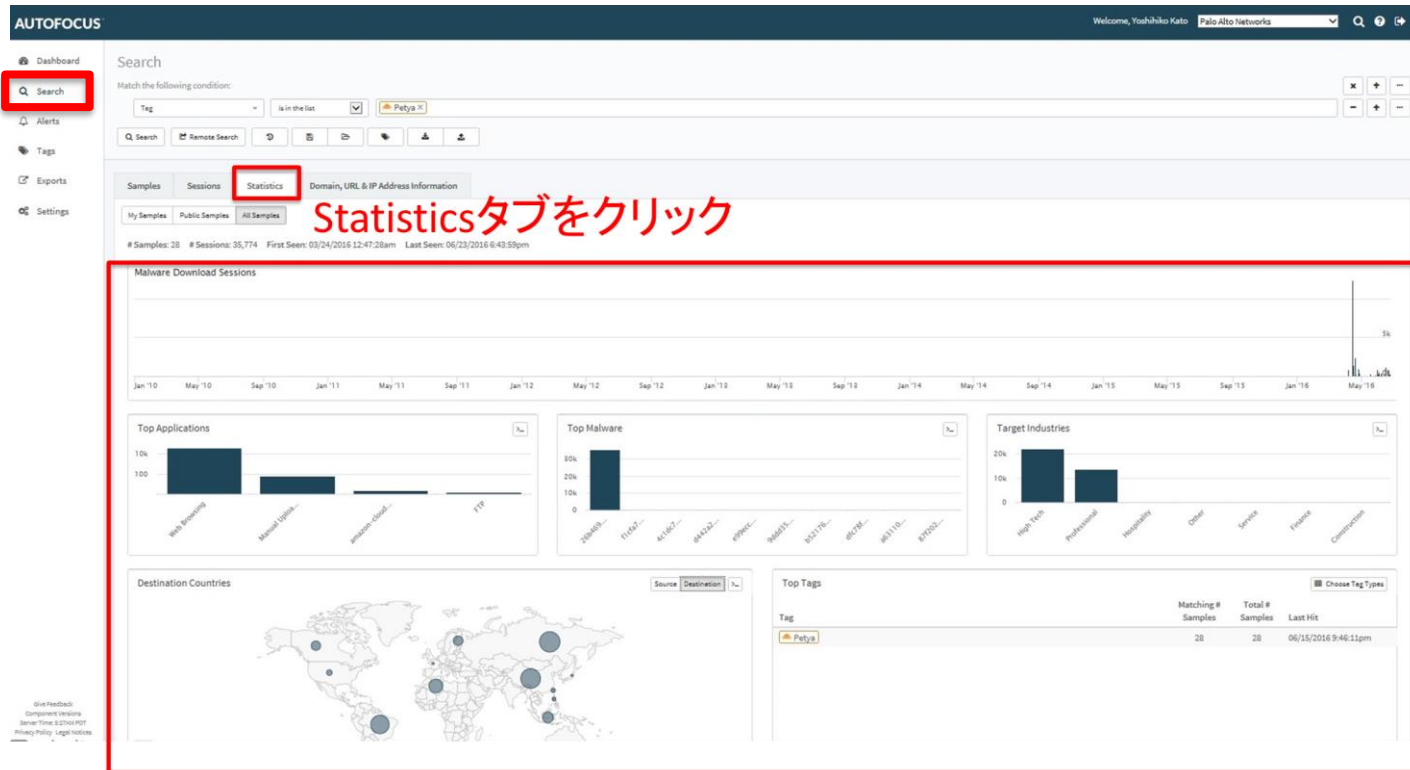
Signature Name	Create Date	Content Versions	daily
		First Last Current?	
Virus/W32.WGeneric.genf	05/31/2016 4:51:14am	1895 1895	Yes

URLs

URL	Category
time.windows.com	Computer and Internet Info
a1-128.akadns.net	Content Delivery Networks
#11-128.akadns.net	Content Delivery Networks
akadns.net	Content Delivery Networks

# Search Statistics Search View例(Petya/ランサムウェア)

- ・検索結果のStatisticsタブを選択することで統計情報を確認可能。
- ・各グラフを選択することで、その項目に限定した情報を表示可能。



# Alerts (アラート設定) 画面

- ・優先度を持って対応すべき内容(危険度が高いマルウェア等)の情報通知が可能
- ・通知対象のタグタイプ(Unit42tag,public tag,private tag)に対し自分にメールや Http messageを送信可能

The screenshot shows the 'Alerts' settings page in the Palo Alto Networks management interface. The 'Alerts' and 'Settings' tabs are highlighted with red boxes. The page is divided into two main sections: 'Alert On Tag Type' and 'Alert Actions'.

**Alert On Tag Type Configuration:**

Alert On Tag Type	Action	My Samples	Public Samples	
Unit 42	Mail_me	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Add Exception
Except on tag	none	Yes	Yes	<input type="checkbox"/> <input type="checkbox"/>
Public	AAA_email_action	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Add Exception
Private	none	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Add Exception

**Alert Actions List:**

Alert Actions	Type	Endpoint	Actions
none	None		
AAA_email_action	Email	sbradshaw@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
ahayashi	Email	ahayashi@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
Alywin_Alert	Email	aong@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
Anand	Email	anand@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
asano	Email	tasano@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
avisar_xgii	Email	xgii@extomos.com	<input type="checkbox"/> <input type="checkbox"/>
claire-test-alert	Email	cnolan@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
cwoo	Email	cwoo@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
Darren_koh	Email	dkoh@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
dfuertes	Email	dfuertes@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
D_dodat	Email	kfletcher@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
Etchen	Email	etchen@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
fpinheiro	Email	fpinheiro@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>
kato	Email	ykato@paloaltonetworks.com	<input type="checkbox"/> <input type="checkbox"/>

Footer information: Give Feedback, Component Versions, Server Time: 11:58AM PDT, Release Path: 1.4.41-1000000000, paloalto

# Tags画面

- 既知や潜在的な脅威を示す複数の検索条件を各Tagに紐付けることで、Wild Fireで分析された未知のファイルがどのような脅威であるかを瞬時に判別可能。

The screenshot displays the 'Tags' page in the AUTOFOCUS interface. The left sidebar contains navigation options: Dashboard, Search, Alerts, Tags (highlighted with a red box), Exports, and Settings. The main content area shows a table of 780 tags. The table has the following columns: Tag, Company, Source, Status, # Samples, Last Hit, and Votes. The tags listed include 360Root, 4H, 7ev3n, 7ev3nHONEST, 7ev3nHONEST, 9002, a, AbaddonPOS, AccesMembre, AccessDigitalCurrency, AccessLocalAdminSAM, AccessSMS, AccStealer, AccuTrack, AddBHO, AdLoad, Adposhel, Adsms, Adware, Adwind, AgentTSI, AgentTesla, and AirAdminstaller. The 'Tags' menu item in the left sidebar is highlighted with a red box.

Tag	Company	Source	Status	# Samples	Last Hit	Votes
360Root	Palo Alto Networks Unit42	Unit 42	Enabled	428	06/22/2016 4:40:26am	0
4H	Palo Alto Networks Unit42	Unit 42	Enabled	49	06/11/2016 1:03:26am	5
7ev3n	Palo Alto Networks Unit42	Unit 42	Enabled	11	05/06/2016 8:59:40pm	0
7ev3nHONEST	Palo Alto Networks Unit42	Unit 42	Enabled	142	06/23/2016 7:21:32am	0
7ev3nHONEST	Palo Alto Networks		Enabled	0		0
9002	Palo Alto Networks Unit42	Unit 42	Enabled	49	05/29/2016 7:24:37am	2
a	Palo Alto Networks		Enabled	0		0
AbaddonPOS	Palo Alto Networks Unit42	Unit 42	Enabled	49	11/25/2015 1:21:20pm	0
AccesMembre	Palo Alto Networks Unit42	Unit 42	Enabled	388,461	06/21/2016 7:01:51pm	0
AccessDigitalCurrency	Palo Alto Networks Unit42	Unit 42	Enabled	150,223	06/23/2016 11:51:45am	0
AccessLocalAdminSAM	Palo Alto Networks Unit42		Enabled	197,398	06/23/2016 7:00:21am	0
AccessSMS	Palo Alto Networks Unit42		Enabled	702,002	06/23/2016 12:09:52pm	0
AccStealer	Palo Alto Networks Unit42		Enabled	8	01/31/2016 10:25:11pm	0
AccuTrack	Palo Alto Networks Unit42		Enabled	55	06/21/2016 5:35:05pm	0
AddBHO	Palo Alto Networks Unit42	Unit 42	Enabled	67,211	06/23/2016 10:56:12am	0
AdLoad	Palo Alto Networks Unit42	Unit 42	Enabled	241,982	06/23/2016 10:47:00am	0
Adposhel	Palo Alto Networks Unit42		Enabled	4,921	06/23/2016 9:48:13am	0
Adsms	Palo Alto Networks Unit42		Enabled	8	01/12/2016 4:57:38pm	0
Adware	Palo Alto Networks Unit42	Unit 42	Enabled	1,589,182	06/23/2016 10:36:04am	0
Adwind	Palo Alto Networks Unit42		Enabled	288	06/17/2016 8:26:59pm	0
AgentTSI	Palo Alto Networks Unit42		Enabled	856	06/23/2016 11:05:20am	0
AgentTesla	Palo Alto Networks Unit42		Enabled	582	06/23/2016 9:03:23am	0
AirAdminstaller	Palo Alto Networks Unit42	Unit 42	Enabled	338,380	06/23/2016 11:18:14am	0

# Exports画面

- Wild Fireがマルウェアで検出したIP、URLやドメイン情報を、AutoFocusでエクスポート可能。(CSV形式)
- SIMEソリューションやPAN-OSが持つダイナミックブロックリストで利用可能。

The screenshot displays the 'Exports' section of the AutoFocus interface. The left sidebar contains navigation options: Dashboard, Search, Alerts, Tags, Exports (highlighted with a red box), and Settings. The main content area shows a table of 36 items found, with columns for Label, # Entries, # Samples, Last Entry, First Entry, Author Email, and Actions. The table lists various items such as 'WF-cryptowall', 'tesla', 'Dridex', 'ctb locker', 'locky', 'anand', 'Josh', 'Roularta', 'bio-demo', 'Blocklist', 'APT123', 'pglynn-test', 'HighlySuspect-Virut', 'ChrisMTest', 'rbarrett-test', 'nmx', 'fpinheiro', 'Export Blacklist', 'Export IOC', 'sam-utd', and 'TDK-EDL'. Each row includes an 'Export' button in the Actions column.

Label	# Entries	# Samples	Last Entry ↓	First Entry	Author Email	Actions
WF-cryptowall	2	2	06/22/2016 1:46:37am	06/08/2016 4:16:43am	dschueler@paloaltonetworks.com	Export
tesla	9	2	06/21/2016 10:46:35am	02/19/2016 5:48:05am	wvechamaneesri@paloaltonetworks.com	Export
Dridex	1	1	06/21/2016 1:43:26am	06/21/2016 1:43:26am	ssimkin@paloaltonetworks.com	Export
ctb locker	3	2	06/20/2016 5:01:23pm	06/01/2016 5:44:24am	ktjenhan@paloaltonetworks.com	Export
locky	8	1	06/12/2016 3:34:08am	06/12/2016 3:34:08am	wvechamaneesri@paloaltonetworks.com	Export
anand	1	1	06/10/2016 10:50:12am	06/10/2016 10:50:12am	amuthaiyan@paloaltonetworks.com	Export
Josh	1	1	06/08/2016 4:16:43am	06/08/2016 4:16:43am	jjost@paloaltonetworks.com	Export
Roularta	1	1	06/08/2016 2:16:05am	06/08/2016 2:16:05am	sdepauw@paloaltonetworks.com	Export
bio-demo	3	1	06/07/2016 8:11:49am	06/07/2016 8:11:49am	lharsh@paloaltonetworks.com	Export
Blocklist	4	2	06/07/2016 2:44:10am	05/25/2016 3:09:59pm	aabdullah@paloaltonetworks.com	Export
APT123	3	2	06/06/2016 6:18:47am	05/25/2016 3:09:59pm	pdejong@paloaltonetworks.com	Export
pglynn-test	3	1	06/05/2016 3:46:05pm	06/05/2016 3:46:05pm	pglynn@paloaltonetworks.com	Export
HighlySuspect-Virut	77	1	06/03/2016 4:56:11pm	06/03/2016 4:56:11pm	lharsh@paloaltonetworks.com	Export
ChrisMTest	1	1	05/31/2016 3:23:05am	05/31/2016 3:23:05am	chmotley@paloaltonetworks.com	Export
rbarrett-test	4	1	05/30/2016 9:44:33pm	05/30/2016 9:44:33pm	rbarrett@paloaltonetworks.com	Export
nmx	1	1	05/30/2016 9:41:48pm	05/30/2016 9:41:48pm	cperez@paloaltonetworks.com	Export
fpinheiro	12	3	05/30/2016 1:42:27am	05/25/2016 12:55:50am	fpinheiro@paloaltonetworks.com	Export
Export Blacklist	3	2	05/28/2016 10:18:37am	05/10/2016 11:05:26am	yctan@paloaltonetworks.com	Export
Export IOC	811	2	05/28/2016 10:18:37am	05/10/2016 11:05:26am	yctan@paloaltonetworks.com	Export
sam-utd	15	1	05/26/2016 6:02:19am	05/26/2016 6:02:19am	scook@paloaltonetworks.com	Export
TDK-EDL	1	1	05/17/2016 1:43:31pm	05/17/2016 1:43:31pm	tkirk@paloaltonetworks.com	Export