# THREAT ANALYTICS PLATFORM

CLOUD-BASED THREAT DETECTION AND INVESTIGATION

## OVERVIEW

Organizations are fighting an asymmetric battle. Adversaries are elusive, polymorphic, well funded and able to bypass legacy security technologies to exfiltrate your most critical data. Organizations are understaffed, overwhelmed with alerts and lack the visibility and information they need to detect and investigate cyber threats.

FireEye is transforming detection and incident investigation with our cloud-based Threat Analytics Platform (TAP). TAP provides enterprise-wide visibility, codified detection expertise and guided investigation workflows to amplify your defense against today's most sophisticated cyber attacks.

### Built by Security Practitioners

FireEye built TAP from the ground up — by security practitioners, for security practitioners. TAP combines threat insights gained from responding to the worlds' most consequential breaches with big data security analytics and codified security expertise so you can quickly identify and investigate cyber threats.

### Enterprise-Wide Visibility

Your attackers can enter anywhere. You need visibility everywhere. TAP provides enterprise-wide visibility by aggregating alerts from the diverse range of security technologies throughout your organization. Our thin network sensors provide real-time visibility to distributed environments, aggregating events from remote locations and sending them to a centralized location for log retention, threat analysis and investigation.

### Adaptive Detection

Your adversaries are constantly changing. Your detection and investigation capabilities must evolve just as quickly. FireEye has a dedicated TAP team made up of data scientists and security researchers that codify extensive front-line incident response experience into detection rules, behavioral analytics and guided investigations. Within hours of discovering an emerging attack, they create new rules and perform retrospective analysis of your environment to determine the potential impact and feed these rules back into the TAP product. Upon discovering malicious activity, TAP generates alerts enriched with supporting data, such as attacker context, to aid the investigator in validating and scoping the incident.

## HIGHLIGHTS

- **Purpose-Built** – the cloud-based platform was built by security practitioners for security practitioners
- **Answers, Not Alerts** – identify known and unknown threats by applying real-time threat intelligence to enterprise event streams
- **Codified Detection Expertise** – enhance detection and investigation capabilities with codified expertise from FireEye security researchers and data scientists
- **Integrated Threat Insight** – streamline incident investigation by enriching alerts with detailed attacker context
- **Sub-Second Search** – improved search time across billions of events helps security analysts proactively hunt for covert behavior on the network
- **Rapid Deployment** – operational in hours instead of months or years
- **Easily Scalable** – elastic, cloud-based infrastructure makes it easy for organizations to scale as business needs or seasonal requirements change
- **Predictable Costs** – software-as-service provides predictable operating expense for software, support, infrastructure, threat intelligence and security expertise

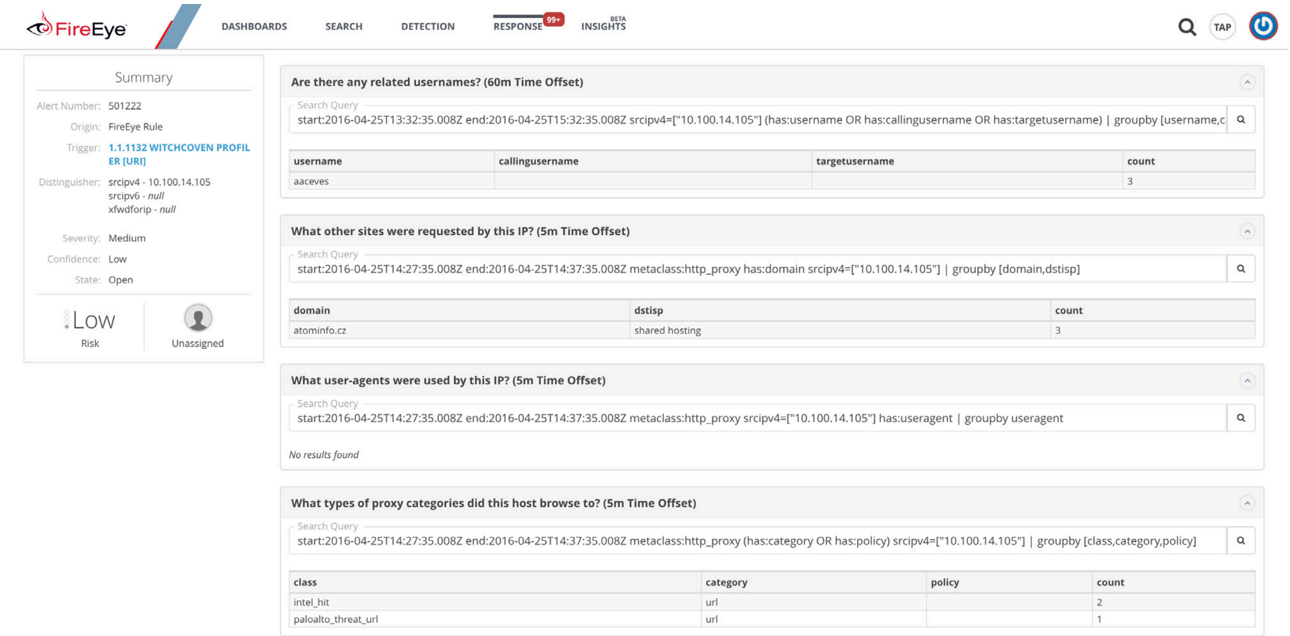
## Accelerate Threat Investigations

Your team's ability to respond to an ever-increasing number of cyber attacks is stretched to the breaking point. You need a dramatic increase in security operations productivity and effectiveness that will accelerate your incident response lifecycle.

TAP expedites investigation by enriching alerts with supporting data. Threat intelligence, point-in-time context regarding users affected, actions taken and hosts involved help you validate and scope the incident.

TAP also offers Guided Investigations to help amplify the investigation efficiency of incident responders. Our Guided Investigation capability leads analysts through industry-leading investigative strategies by providing pre-populated queries based on FireEye knowledge from specific attack scenarios.

Upon receiving an alert, TAP selects and presents the relevant next step queries providing a best practice workflow to guide and inform your threat investigation.



Summary

Alert Number: 501222
Origin: FireEye Rule
Trigger: 1.1.1132 WITCHCOVEN PROFILER [URI]
Distinguisher: srcipv4 - 10.100.14.105
srcipv6 - *null*
xfwdforip - *null*
Severity: Medium
Confidence: Low
State: Open

Low
Risk

Unassigned

**Are there any related usernames? (60m Time Offset)**

Search Query

```
start:2016-04-25T13:32:35.008Z end:2016-04-25T15:32:35.008Z srcipv4=["10.100.14.105"] (has:username OR has:callingusername OR has:targetusername) | groupby [username,c
```

| username | callingusername | targetusername | count |
|---|---|---|---|
| aaceves | | | 3 |

**What other sites were requested by this IP? (5m Time Offset)**

Search Query

```
start:2016-04-25T14:27:35.008Z end:2016-04-25T14:37:35.008Z metaclass:http_proxy has:domain srcipv4=["10.100.14.105"] | groupby [domain,dstisp]
```

| domain | dstisp | count |
|---|---|---|
| atominfo.cz | shared hosting | 3 |

**What user-agents were used by this IP? (5m Time Offset)**

Search Query

```
start:2016-04-25T14:27:35.008Z end:2016-04-25T14:37:35.008Z metaclass:http_proxy srcipv4=["10.100.14.105"] has:useragent | groupby useragent
```

*No results found*

**What types of proxy categories did this host browse to? (5m Time Offset)**

Search Query

```
start:2016-04-25T14:27:35.008Z end:2016-04-25T14:37:35.008Z metaclass:http_proxy (has:category OR has:policy) srcipv4=["10.100.14.105"] | groupby [class,category,policy]
```

| class | category | policy | count |
|---|---|---|---|
| intel_hit | url | | 2 |
| paloalto_threat_url | url | | 1 |

## Think Like Your Attacker

To move from reactive response to proactive defense, you must think like your attacker. TAP includes access to the FireEye Intelligence Center (FIC) to help you understand your adversaries' methods and motivations as well as anticipate their next moves. FIC streamlines incident investigations by providing users with actionable intelligence. FIC's comprehensive profiles detail the tools, techniques and procedures used by threat actors specifically targeting your industry.

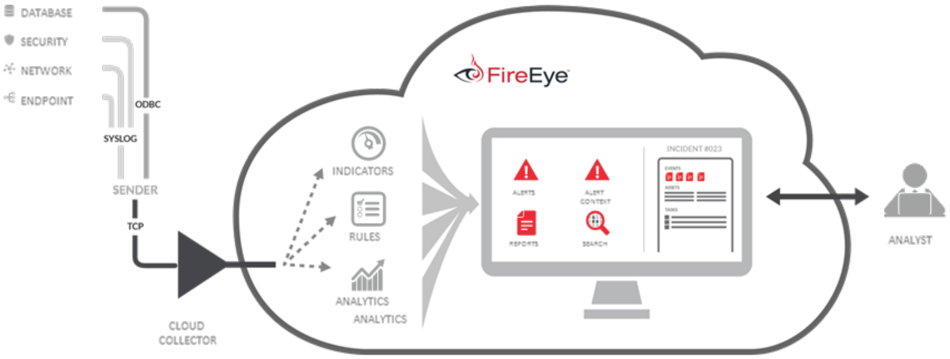
### Discover Covert Activity

When an adversary evades detection, there is no evidence of compromise, no starting point for your investigation. To discover emerging attack campaigns, you must pre-emptively search for evidence of covert behavior. TAP enables nimble data exploration via sub-second search across billions of events so security analysts can proactively hunt for hidden indicators of compromise. Once identified, agile investigation tools help analysts pivot from one indicator to the next, evaluate the full context of newly discovered artifacts, reconstruct the attack storyline and ultimately limit the impact of the breach.

### Simplified Deployment Expedites Time to Value

TAP requires minimal onsite configuration, simplifying deployment and eliminating costly professional services engagements. Our elastic, cloud-based infrastructure scales seamlessly, allowing you to adapt faster as business needs or seasonal requirements change. The TAP subscription includes software, support, infrastructure, threat intelligence and codified security expertise, ensuring predictable operating expense.

FIGURE 1 FIREEYE THREAT ANALYTICS PLATFORM



For more information on FireEye, visit:
**www.FireEye.com**

**FireEye, Inc.**
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

**www.FireEye.com**

© 2016 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc.
All other brands, products, or service names are or may be trademarks
or service marks of their respective owners. DS.TAP.EN-US.062016