AFKC
Value-Added Distributor

WHITE PAPER

CYBER THREAT INTELLIGENCE

What it is and how to use it effectively

TABLE OF CONTENTS

1. INTRODUCTION

In today's world, threats are becoming higher and smarter than in the past. Security Teams, which are focused on "traditional" network security, are falling behind cyber attackers, getting overwhelmed by information, and trying to analyze artifacts to determine future scenarios.

As organizations try to fill the gap, Threat Intelligence is growing in popularity, and vendors are falling over themselves to offer a confusingly diverse array of Threat Intelligence products.

This white paper is intended as a tool to help decision makers determine if the organization is ready to incorporate Threat Intelligence, or, for those who are already leveraging TI, how to use more effectively the instruments available.

This is not a technical white paper, and it not discuss the budgetary terms of Threat Intelligence Operations and Tools. The focus will be given more to the techniques that will bring value to organizations, no matter the size.

2. WHAT IS THREAT INTELLIGENCE?

Threat Intelligence is the process of acquiring multiple information from sources, to gain knowledge about threats on a particular environment. In 2013 Gartner explained Threat Intelligence as a evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."

As the traditional Security Framework aims to protect assets and devices, it is a natural step to consider TI as the evolution of the normal security processes and procedures. Detecting incident sooner, eventually preventing them, and giving a context on what's going on in terms of threats, is the main goal of Threat Intelligence.

As business competitors suffer Data Breaches, Leaks of Information, executive and stakeholders are going to perceive Cyber Threats as imminent to the organization. The only thing they are interested in is the organization level of protection. **Threat Intelligence aims to align the business expectations with cyber security goals**.

However, **Threat Intelligence shouldn't be integrated into an organization's defense without defining the perimeter.** As an example, consider a Threat Intelligence program that consists in subscribing to Data Feeds. The expectations, would be that Security Teams will be tasked to maintain feeds and TTP's up-to-date. This is not sufficient to meet the initial requirements. The objective would be considering where these Feeds will be deployed on the Network, and "***Will those information be enough to undertake decisions on how to act on network devices to detect specific attacks?***"

3. IMPORTANCE OF THREAT INTELLIGENCE

Executives increasingly seeThreat Intelligence as a valuable tool and the perception is now changing from a luxury tool into a necessity for the business. Security Professionals also realize that attackers often have a better understanding of their organization's network than they do.
Often happens that uncovering Breaches leads security teams to find that attackers moved quietly from a System to another with no detections on the security perimeter. Nowdays attackers can evade whitelists, gaining privileged access on systems, and overtake control on network devices to obtain persistent accesses.
To keep up on this, Security Teams are leveraging multiple tools to hunt for threats on the network, getting to the point that if properly implemented Threat Intelligence, is the only countermeasure against Cyber Threats.

4. SOURCES OF THREAT INTELLIGENCE

4.1 Internal TI Sources

Information and Data Points collected within the organization are considered as an Internal Threat Intelligence Sources. These datapoints can derive from normal day to day operations and detections. As an example of Internal TI, consider some detections made from Endpoint Security Sensors. These kind of events apparently unconnected from other events, could be organized into a meaningful content, to build the normal profile of the organization.

Another example could be the infection made by a ransomware. Despite the negatives, the organization does not consider a ransomware as a targeted attack, as the incident can be easily mitigated. By using Threat Intelligence, security teams, would be able to perform different investigations, to determine the chokepoints that failed the detection during the path to the infected host.

By building internal IoC's Security Teams would be able to recognize similarities also in future attack scenarios. By creating internal catalogs of incidents SOC's can identify weak points across the network, critical assets, and defining priorities for security policy implementations.

4.2 External TI Sources

External Threat Intelligence Sources refers to subscriptions to specific services that let organizations gather informations such as IoC, TTP's or Threat Data Feeds.

The problem is represented by the huge amount of information available. Security Teams needs to plan which subscription is needed by the organization by deciding which is the service that fits the business operations.

It's not unusual to find SIEM's overwhelmed of IoC's TTP's and Threat Feeds that are irrelevant to the organization. This usually happens when TI is not correctly addressed by a shared plan.

The sources available are:

Data Feeds:

Data Feeds are widely used by security teams, as they can be easily ingested by Next-Gen Firewalls / SIEM's and other network devices. Data Feeds can also be organized into subgroups as:

- **Subscriptions:** That represent a list of Indicators Of Compromise (IoC), that describes hashes, IPs, Domain names that can refer to a specific APT. They are usually represented by a json or CSV file that can easily be imported into the majority of commercial SIEMs
- **API:** Scripts can connect to a specific provider via API to extract information. This is widely used when building custom applications.
- **Special Releases:** Usually public report that describes the behavior of a specific, relevant APT.

The advantage in using these kind of information is only when the organization implements feeds into their systems such as SIEMS firewalls, or Endpoint Protection Platforms.

Data Feeds can include also attacker TTP's that describes the Tactics Techniques and Procedures to describe a specific threat.

Open Source Threat Intelligence (OSINT) feeds are available. In some cases organizations that monitors an attacker activity aggregate these data to be provided for free to the communities. Feeds are easy to ingest, but in many cases they can increase the false positives. However, as many attackers often exploit well-known vulnerabilities, OSINT feeds may help protect against groups scanning for these.

Commonality:

Threat Actors and Groups often attacks organizations with similar interests, or that operates in the same market. For these reasons industry specific groups are born, to facilitate the sharing of information throughout similar companies.
These groups, including Information Sharing and Analysis Centers (ISACs), often present findings or intelligence with higher fidelity than feeds. ISACs also help facilitate bidirectional sharing of information between the public and private sectors.

Relationships with government and law enforcement:

Many organizations receive as TI source, some kind of information by US government and FBI. Infragard, is a provider represented by a partnership between FBI and the private sector.

Crowdsourced Platforms:

These are hub of Commonalities that shares information across multiple market segments. Access to these platforms are sometimes provided through anonymous access, which result in a benefit for those businesses who want to get a particular TI without revealing the identity.
One possible drawback in the use of these kind of platforms is that the value of the intelligence will suffer if the data gathered from platform members are generic, incomplete or misleading.

5. MAKING THREAT INTELLIGENCE ACTIONABLE

By combining the use of External and Internal Sources, Organization can create a valuable TI program that enables Security Teams give a correct context to their Infrastructure threats.

Internal TI enable contexts around incidents by giving you information on how you have been attacked, what the attacker left behind before disappearing, and also, to prioritize the assets based on business processes.

External TI instead give the visibility on what you don't know, giving you the information on how your organization may be attacked.

The successful combination into a TI Program helps you to reduce the time needed from the infection to detection to remediation.

5.1 Threat Intelligence and Security Posture

One of the successful application of TI in an environment, is when interacting with the organization's security plan. Security Posture is the process that describes the mapping between business and the IT assets. The result of this analysis is to determine the critical assets that must be protected.

TI can help the organization understand which areas of the business attackers are most likely to target and use that insight to more effectively protect key assets.

On the other hand, TI can help discover assets that currently are not perceived by the business as critical.

Of course, this does not mean that TI should be the only benchmark of defense. It merely complements other ways of identifying the portions of a network or enterprise that need protection, as part of a well-balanced information security team's efforts.

5.2 Threat Intelligence and Incident Response Team

Another way to make TI actionable, is when integrated with IR Teams. Usually IR Teams, like Administrators, Analysts and engineers have a deep knowledge of the Organization processes and they could rely on TI to detect suspicious activities faster.

An example could be the use of an IoC to hunt for a specific malware on the Endpoints, or other hashes that might be present in other APT targeting the organization's industry or market segment.

5.3 Using Threat Intelligence to prevent attacks

Threat Intelligence tools can be used in normal day-to-day operations to analyze changes in attacks and trends for a specific threat actor. For example, attackers are now widely using Microsoft Powershell driven attacks to take advantage of the buil-in scripting platform. Through the use of the TTP's an organization might prevent the techniques that mostly like to be used as the next attack vector.

6. WHAT'S NEXT?

AFKC is a value added System Integrator operating in IT Security delivering high end Cyber Security projects. Our main focus is on Threat Intelligence projects and process solutions. The way we deliver threat intelligence is through industry leading products and services that are recognized state-of-the-art from the major analysts such as Forrester and Gartner.

The areas that we cover are mainly related to SOC operations. Our clients identify us as an integrator that simplifies SOC operations processes by increasing their efficiency in investigation and response time.

7. WHAT WE DO

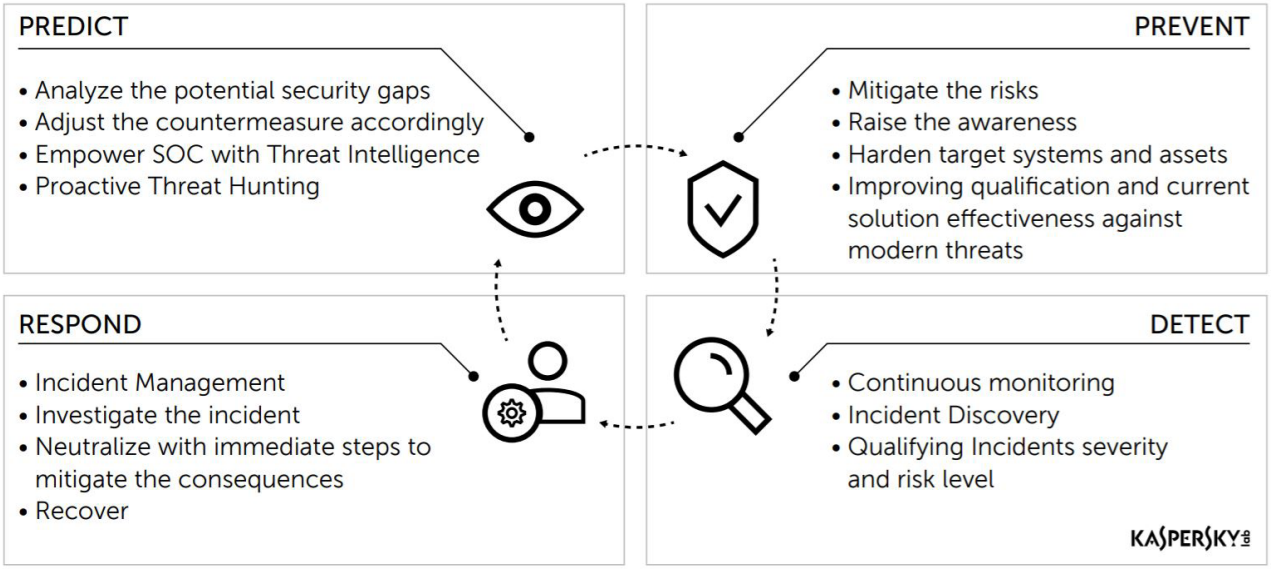
AFKC is a Value-Added Distributor for Kaspersky Enterprise Business technologies. All the points covered in this document can be applied to real environments through the following technologies:

7.1 Anti Targeted Attack

KATA (Kaspersky Anti Targeted Attack Platform) is a technology built by Kaspersky Lab in 2008 that is dedicated to detect Advanced Persistent Threats in a network. Kaspersky Lab's Adaptive Security Strategy is founded on the most viable security architecture as described by Gartner.

While the majority of simple cyberthreats can be blocked by traditional, signature based and heuristics-enhanced security products, today's cybercriminals and hackers are using increasingly sophisticated attacks to target specific organizations. Targeted attacks – including Advanced Persistent Threats (APTs) – are now one of the most dangerous risks that enterprises have to deal with. However, while the threats – and the techniques that cybercriminals and hackers employ are constantly evolving, many businesses are failing to adapt their security strategies

FIG.1
KATA's approach to APTs



1. ICSA Labs tested the Kaspersky Lab's KATA advanced threat defense solution using the primary threat vectors leading to enterprise breaches according to Verizon's Data Breach Investigations Report (DBIR).
2. ICSA Labs tests with malicious threats that other security products typically miss.
3. Kaspersky Labs' KATA demonstrated excellent threat detection effectiveness against nearly 600 new and little-known threats.

The Kaspersky KATA platform had zero false positives during this test cycle, which is excellent

The approach is to provide a cycle of activities in four key areas: **Prevent**, **Detect**, **Respond**, and **Predict**:

- **Prevent** – reduce the risk of advanced threats and targeted attacks
- **Detect** – identify activities that could signal a targeted attack
- **Respond** – close security gaps and investigate attacks
- **Predict** – where and how new targeted attacks could appear

Essentially, this assumes that traditional prevention systems should function in coordination with detection technologies, threat analytics, response capabilities

ICSA certification in fact is a guideline for the enterprise companies which

7.2 Threat Data Feeds

This service offers continuously updated Threat Data Feeds to inform your SOC team about risks and implications associated with cyberthreats, helping you to mitigate threats more effectively and to defend against attacks even before they are launched.

Feeds available:

IP Reputation Feed — a set of IP addresses with context covering suspicious and malicious hosts.

Malicious URLs — a set of URLs covering malicious links and websites. Masked and non-masked records are available.

Phishing URLs — a set of URLs identified by Kaspersky Lab as phishing sites. Masked and non-masked records are available.

Botnet C&C URLs — a set of URLs of botnet command and control (C&C) servers and related malicious objects.

Whitelisting Data Feed — a set of file hashes providing third-party solutions and services with a systematic knowledge of legitimate software.

Malicious Hash Feed — overing the most dangerous, prevalent and emerging malware.

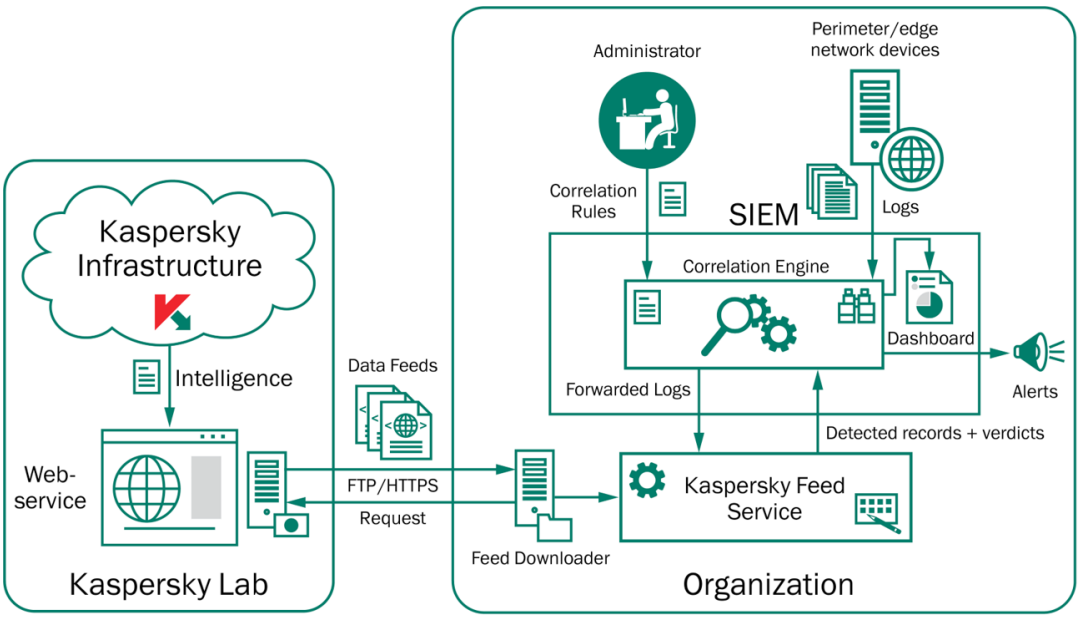
Mobile Malicious Hash Feed — a set of file hashes for detecting malicious objects that infect mobile platforms.

P-SMS Trojan Feed — a set of Trojan hashes with corresponding context for detecting SMS Trojans ringing up premium charges for mobile users as well as enabling an attacker to steal, delete and respond to SMS messages.

Mobile Botnet C&C URLs — a set of URLs with context covering mobile botnet C&C servers

The integration of such information can be done on all the SIEMs available on the market. Fig 2 explains how the integration can be done out of the box.

FIG.2
Integration with SIEM



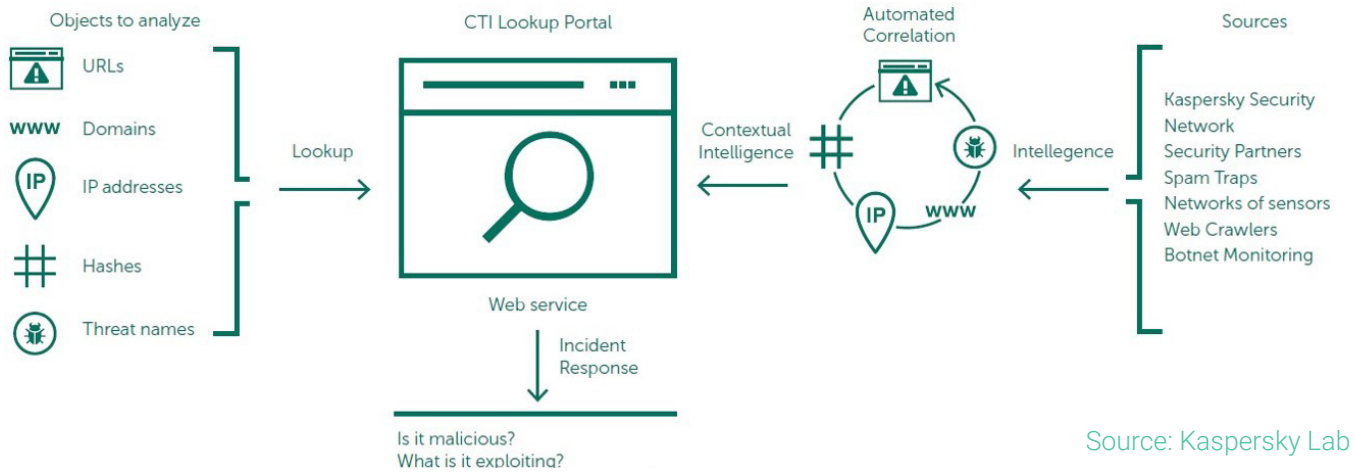
Source: Kaspersky Lab

7.3 Kaspersky Threat Intelligence Portal

Kaspersky Threat Lookup delivers all the knowledge acquired by Kaspersky Lab about cyberthreats and their relationships, brought together into a single, powerful web service.

The goal is to provide your SOC teams with as much data as possible, preventing cyber-attacks before they impact your organization. The platform retrieves the latest detailed Threat Intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, file attributes, geolocation data, download chains, timestamps, etc. The result is global visibility of new and emerging threats, helping you secure your organization and boosting incident response.

FIG.3
Intelligence for SOC



Source: Kaspersky Lab

7.4 APT Intelligence Reporting

Increase your awareness and knowledge of high profile cyber-espionage campaigns with comprehensive, practical reporting from Kaspersky Lab. Leveraging the information provided in these reports, you can respond quickly to new threats and vulnerabilities - blocking attacks via known vectors, reducing the damage caused by advanced attacks and enhancing your security strategy, or that of your customers.

As a subscriber to Kaspersky APT Intelligence Reporting, we provide you with unique ongoing access to our investigations and discoveries, including full technical data provided in a range of formats, on each APT as it's revealed, including all those threats that will never be made public.

7.5 Tailored threat reporting

What's the best way to mount an attack against your organization? Which routes and what information is available to an attacker specifically targeting you? Has an attack already been mounted, or are you about to come under threat? Customer-specific Threat Reporting answers these questions and more, as our experts piece together a comprehensive picture of your current attack status, identifying weak-spots ripe for exploitation and revealing evidence of past, present and planned attacks.

Developed using open source intelligence (OSINT), deep analysis of Kaspersky Lab expert systems and databases and our knowledge of underground cybercriminal networks, these reports cover areas including:

Identification of threat vectors: Identification and status analysis of externally available critical components of your network –including ATMs, video surveillance and other systems using mobile technologies, employee social network profiles and personal email accounts – that are potential targets for attack.

Malware and cyber-attack tracking analysis: Identification, monitoring and analysis of any active or inactive malware samples targeting your organization, any past or present botnet activity and any suspicious network based activity.

Third-party attacks: Evidence of threats and botnet activity specifically targeting your customers, partners and subscribers, whose infected systems could then be used to attack you.

Information leakage: through discreet monitoring of underground online forums and communities, we discover whether hackers are discussing attack plans with you in mind or, for example, if an unscrupulous employee is trading information.

Current attack status: APT attacks can continue undetected for many years. If we detect a current attack affecting your infrastructure, we provide advice on effective remediation.

8. CONCLUSION

Threat Intelligence is not to be intended as a device, or a platform. And it's not even a checkbox. Threat Intelligence, gives the organization the capability to transform an alert into an Incident by adding context information to the detected threats.

Threat Intelligence helps to make faster decision, by reducing the time needed to give priorities to business risks.

9. WHY AFKC

Despite its recent foundation in 2016, AFKC relies on a team of professionals with many years of experience in Cyber Security and Anti-Fraud

AFKC operates through offices located in Italy and The Netherlands, ensuring a consistent presence on the National and International territory.

Adding our knowledge to Kaspersky Lab's solutions, we are able to help our Partners protect End User's Business, Information and Infrastructures from Advanced Threats, Cyber Attacks and Cybercrime. We work in cooperation with our Partners (System Integrators, Solution Providers, MSPs, VARs and Resellers) offering highly specialized services and dedicated contact persons.

Our Services

SALES ENABLEMENT

PRESALES ENABLEMENT

INTEGRATED SOLUTIONS

EDUCATION

PROFESSIONAL SERVICES

TECHNICAL SUPPORT

AFKC
Value-Added Distributor

CONTACTS

AFKC B.V.

Papendorpseweg 100
3528 BJ Utrecht, Netherlands
+31 030 799 1037
info@afkc.eu

AFKC s.r.l.

Via Fiume Giallo, 3
00144 Rome, Italy
+39 06 522 44040
info@afkc.eu

WWW.AFKC.EU