Threat Hunting (TH)

Service Description

One eSecurity’s threat hunting service provides our customers with an iterative and proactive process for searching through networks to detect and isolate advanced threats (APT) that evade existing security solutions. This approach transforms traditional threat management from reactive to proactive.

Introduction

Threat hunting has traditionally been a manual process, in which a security analyst sifts through data and information using their own knowledge and familiarity with the network to create hypotheses about potential threats. The results would then be stored so that they could be reused to train automated detection systems and to serve as a foundation for future hypotheses. Nowadays, due to the sheer number of servers used by companies, along with the large number of known threats, it is completely inefficient to perform this activity without the help of the right tools.

“Cyber attackers operate undetected for an average of 99 days, but obtain administrator credentials in less than three days, according to the Mandiant M-Trends Report. The study also showed that 53% of attacks are discovered only after notification from an external party.”

One eSecurity’s threat hunting service is an automatic, proactive and iterative process, using bulk data. It applies different hypotheses to discover suspicious activity that may have slipped past your existing security measures.

In order to detect this suspicious activity, we assume that you have already been compromised and investigate past activity in your infrastructure until we can prove otherwise. In short: “The attacker has got past the perimeter; now we must look for them.”

“The average company takes 170 days to detect an advanced threat, 39 days to mitigate, and 43 days to recover, according to the Ponemon Institute”.

Our offensive, proactive cyber activities and active cyber defense facilitate anticipatory threat reduction while informing protection, detection and incident response, giving you the ability to engage the adversary at distance, on detection.

We can confirm our approach:

- Has greater efficacy than reactive systems.
- Drastically reduces the volume and severity of attacks leading to an order-of-magnitude fewer alerts, incidents, and costs.
- Provides early warning and indicators to model zero-day signatures to incident response mechanisms and enumerate attack networks through cyber threat intelligence.
- Is not subject to the scalability issues around performance and cost that reactive systems struggle with.

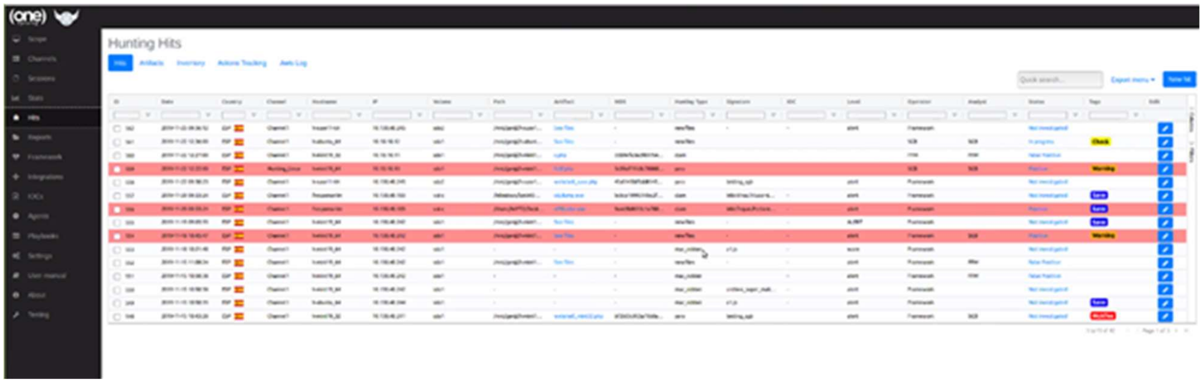
One eSecurity threat hunting decisively engages the adversary and includes hunt and adversarial pursuit activities.

Service Description

Our service is a combination of resources, technology and processes directed by a graded crisis management system.

Having our own hunting and threat intelligence framework enables us to:

- Analyze and generate all kinds of IOCs, from the simplest hash files to the most elaborate TTPs, based on our malware analysis ability.
- Perform these analyses on large banks of servers and equipment, quickly detecting the type of attack, the artifacts found and patterns on files, processes, ports, registry entries, installations, memory logs and disks; regardless of their platform (Window, UNIX).
- Integrate the framework with the customer´s own tools (antivirus programs, EDRs ...) and reuse all the information generated to achieve rapid detection and containment of any type of malware.



The **deployment is simple, fast and secure**, admitting different architectures based on the needs of our customers. Our crowns (servers) can be accommodated in the client's own facilities or in our own CPD´s.

Our **CybOps operations group triage findings and escalate** them for deep analysis by the relevant team. Every day you will receive a report of their activities and findings.

We **increase and increment our activity using a system of distinct threat levels**. These are reviewed based on threat status, detection of new campaigns, information from our intelligence sources, etc. We define the **5 levels** as:

- ***Level 5 – Low***: Everything is normal and no significant new threats are known.
- ***Level 4 – Moderate***: Newly detected campaign from a relevant threat actor; an attack is possible, but not likely.
- ***Level 3 – Substantial***: Relevant activity from a threat actor or campaign targeting the same industry.
- ***Level 2 – Severe***: Recent campaigns or threat actor activity are likely to have affected your company.
- ***Level 1 – Critical***: An incident is highly likely based on CTI information.

Level	Operational Mode	Reporting	Hunting Review CybOps
5	16x5	Daily: • Stats • Executive report by country • Agents status by country Hourly	Hourly
4	16x5	Daily: • Stats • Executive report by country • Agent status by country	Every 45 minutes
3	16x7	Twice daily: 09:00-16:00 • Stats • Executive report by country • Agent status by country	Every 30 minutes
2	18x7	Twice daily: 09:00, 16:00 • Stats • Executive report by country • Agent status by country • Investigation follow up	Real time
1	24x7	Three times a day: 09:00, 14:00, 21:00 • Stats • Executive report by country • Agent status by country • Investigation follow up	Real time

Table 1.- Hunting Levels and SLAs

Thanks to our hunting we are able to:

- Improve and automate the prevention of security incidents through control measures.
- Feed information to other perimeter security devices.
- Focus on specific campaigns or conduct beats to identify APTs.
- Automate security operations and remediation activities.
- Improve incident detection.
- Provide information to different company areas of operation.

Our reliable external sources of threat intelligence obtained from different feeds (OSINT, HUMINT, CCI, IOCs, Malware analysis) combine with your company's own internal sources to form the perfect cocktail of information necessary to counteract and prevent possible attacks.

What objectives do we pursue?

Our team follow a repeatable and well documented set of steps to:

- Provide rapid detection and incident containment.
- Reduce disruption to your business and minimize damage in the event of an attack.
- Contextualize security intelligence information so it is relevant to your business.
- Detect campaigns and attacks against your infrastructure, and identify the actors responsible.
- Improve and assist in automating the detection of incidents by your SOC.
- Detect existing APTs in your systems.
- Improve your tools (SIEMs, FWs, IDS / IPS, WAFs) for IOC detection, avoiding false positives.
- Estimate the potential impact of malicious activity on the victim and assess the actor's intention.
- Improve and automate your OPSEC.

Service Model	Focus	Pricing
*TH on Demand **Entry***	New customers or companies who think that they have been compromised by an actor, or want peace of mind.	One time service price for time and material.
*TH Campaign **Core***	Customers who are concerned about a new campaign that could affect their systems.	Based on campaign duration.
*TH as a Service (Continuous TH) **Enhanced***	Any company wanting the security of a continuous TH program.	Set service price based on scope of customer requirements.

Exceptions

This list shows typical exceptions; however, the actual list will depend on the elements selected by the customer.

- Logistics, storage and transport, unless specifically included.
- Software licensing and hardware costs where not explicitly stated as included.

Inclusions

Software and hardware

One eSecurity works with carefully selected industry leading strategic security vendors to provide best in class cybersecurity solutions. One eSecurity uses hardware and software tools, commercial and open source, chosen depending on design, specific purpose or broader functionality.

Forest TH

After more than ten years delivering EIR services as Incident Handlers and Forensic Analysts in many environments, reviewing thousands of systems, we have been progressively developing our own internal TH analysis system known as Forest.

The Forest platform has been designed not only to automate most of the usual orchestration work needed to manage DF/IR/CTI/Hunting infrastructure but also to be an automated investigation and analysis system that is able to process evidence with the specific tools needed and integrate the results in to a centralized analysis environment for review by the relevant personnel.

Forest's modular design was created to make it possible to handle different kinds of cases, processing the multiple types of evidence found on victim systems such as media (hard disks), memory, network traffic and specific artifacts such as malware.

Optional Services

Professional Services

These provide our customers with advice and expertise to help address their challenges. They can be in the form of fixed-price work-packages or assignment-based engagements. The professional services may include:

- Digital Forensics
- Emergency Incident Respond
- Cyber Threat Intelligence
- CyberOps
- Consulting and others

Please visit our portfolio of solutions and services for more information.

Service Levels Agreements (SLAs)

KPIs	Description	Value
Forest rollout time	Time between contract signing and completion of installation of forest framework and agents by a One eSecurity team.	< 5 days
Hunting Review time	See table 2	See table 2
Report time	See table 2	See table 2

Customer Obligations

- Provide One eSecurity with accurate and up-to-date information, including names, emails, landlines, mobile and pager numbers for designated customer points of contact, together with backup points of contact.

- Provide One eSecurity with accurate and up-to-date information, including name, email, landline, mobile and pager numbers for these designated customer points of contact, together with backup points of contact.

Why One eSecurity?

- The One eSecurity Incident Response Team have worked with some of the world's largest enterprises and responded to some of the most devastating and high profile cyber-attacks of recent times.

- Our staff working in incident response activities have achieved the most prestigious cybersecurity certifications in the market (SANS). One eSecurity is the only company in Spain with SANS instructors who teach cybersecurity courses worldwide.

- Our different service levels lets you pay only for services consumed.

- Our innovative Forensic Framework tool (Forest) automates the hunting process and generation of reports, greatly reducing required manpower.