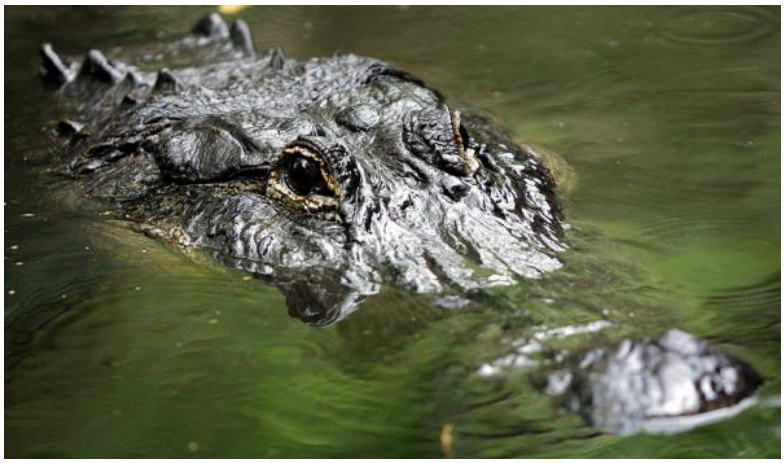
CYBER THREAT INTELLIGENCE

DEKENEAS NEXT-GEN TECHNOLOGIES SRL

www.dekeneas.com

DEKENEAS CYBER THREAT INTELLIGENCE

What is Cyber Threat Intelligence



Today's cyber security climate is constantly evolving and changing, with new threats and new threat actors emerging almost every day. From ransomware gangs to Advanced Persistent Threat nation-state actors, from financially motivated cybercrime gangs to the lone wolf hacker hacking from his mother's basement, the Internet is a dark place with unknown threats waiting to attack the next victim. Traditional antivirus products and security devices can no longer keep up with the growing complexity of threats they are facing. Cyber Threat Intelligence is *knowing who these threats are* and *what techniques, methods or tools they are using* in order to be able to defend against them even before they attack your infrastructure and cause significant damage to your business.

How it works

In order to learn such information, researchers deploy honeypots, which are computer systems or devices, that imitate with different levels of interaction vulnerable computer systems or devices in order to lure attackers and convince them it is a real system or user while analyzing the behavior, tools and techniques they are using.

DEKENEAS NEXT-GEN TECHNOLOGIES S.R.L.
Bd. Libertatii, 20
Bucuresti, Romania

SCAN ME

https://www.dekeneas.com
dekeneas@dekeneas.com

The right Cyber Threat Intelligence feed

There are many Cyber Threat Intelligence feeds available, but how to choose the right one? The right Cyber Threat Intelligence feed should *be relevant to your geographical location, relevant to the industry sector, relevant to the technologies you are using, percentage of unique data, periodicity of data* and *measurable outcome.* Because Cyber Threat Intelligence feeds tend to contain a lot of Indicators Of Compromise (IOC) and each IOC comes with a cost to the device in terms of resources. You do not necessarily need information about attackers targeting Middle East if you operate in Europe, and you are not quite interested in attackers targeting the energy sector if you operate in pharma. You don't necessarily need IOCs for SMB if your network does not have Samba. And you want a CTI feed with high percentage of unique data, because many commercial feeds simply compile open-source feeds. While open source feeds are of great value to the community, their downside resides in the fact that they are not maintained and sometimes they contain old IOCs who are no longer relevant to today's climate.

DEKENEAS AND ORANGE Romania operate a network telescope and a vast network of honeypots with low, medium & high levels of interaction, for generic services such as HTTP/S, DNS, SMTP, SSH, TELNET, etc. but also for ICS/SCADA and IoT devices specific to certain industries such as pharma, energy, financial, etc. We use the network telescope to understand the latest trends in service attacks in order to be able to deploy if needed new or custom honeypots specific for the attacks we observe. Also, on request we can deploy a honeypot to a specific service you require. Our system collects *IP addresses or domains involved in attacks, command & control IP addresses or domains, attacked services information, file names* and *hashes.*

DEKENEAS NEXT-GEN TECHNOLOGIES S.R.L.
Bd. Libertatii, 20
Bucuresti, Romania

SCAN ME

https://www.dekeneas.com
dekeneas@dekeneas.com