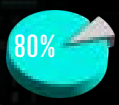
FITSEC CTI
CYBER THREAT INTELLIGENCE

WITH DIVERSE FORMAT OPTIONS:

- VECTRA NDR
- PALOALTO
- MISP
- TAXII
- STIX
- CSV
- OPEN IOC
- FORTIGATE
- MICROSOFT E5



80% OF OUR APT IOCS
(INDICATORS OF COMPROMISE)
ARE UNIQUE, NOT FOUND WITH COMPETITORS

PROACTIVELY DISCOVER ADVANCED THREATS AFFECTING YOUR ASSETS

COMPETITIVE ADVANTAGES

EASY IMPLEMENTATION:
FITSEC DELIVERS THE DATA IN A FORMAT THAT THE CUSTOMER NEEDS OR WANTS, AT NO ADDITIONAL COST

WHY IS FITSEC'S FEED BETTER THAN COMPETITORS'?

When using competing products, the customer has to go through a lot of effort to integrate the data into customers own systems.
Fitsec delivers the data in the format the customer needs effortlessly

ALL- IN-ONE SOLUTION:
THE CUSTOMER DOESN'T HAVE TO DECIDE WHAT PART OF THREATS THEY WANT TO COVER, WE OFFER IT ALL:

- APT
- DDOS
- SINKHOLE
- SANDBOX
- APT PLATFORM

Fitsec's **all-in-one** solution also includes an **exclusive APT platform**, where the customer can view APT actors and their **tools**, **techniques** and **procedures** in a **visual form**, at **no additional cost**

WHY IS FITSEC'S FEED BETTER THAN COMPETITORS'?

A LARGE PART OF OUR DATA IS THE RESULT OF **CONTINUOUS RESEARCH** WORK FROM FITSEC'S EXPERTS. OUR CTI HAS BEEN PRODUCED FOR OVER **13 YEARS**

WHY IS FITSEC'S FEED BETTER THAN COMPETITORS'?

Competitors produce their data mainly with automation, **we produce it as a result of our own research work**

A STRONG EMPHASIS ON APT MALWARE

Targeted attacks (**APT**) are the most dangerous and Fitsec's data places **great emphasis on targeted attacks** and protection against them

DIVERSE APPLICATIONS AND BENEFITS

THREAT DETECTION AND PREVENTION

MALWARE DETECTION
IDENTIFYING AND MITIGATING MALICIOUS SOFTWARE

NETWORK TRAFFIC MONITORING
DETECTING MALICIOUS NETWORK TRAFFIC

EMAIL PHISHING FILTERING
PROTECTING AGAINST PHISHING ATTACKS

DDOS ATTACK TRENDS
UNDERSTANDING AND MITIGATING DDOS ATTACKS

IDENTIFYING PHISHING ATTEMPTS
TOOLS AND TRAINING TO RECOGNIZE PHISHING SCAMS

SECURITY AUTOMATION AND MONITORING

AUTOMATING SECURITY PROCESSES
REDUCING MANUAL EFFORT THROUGH AUTOMATION IN SECURITY WORKFLOWS

MONITORING NETWORK TRAFFIC
OBSERVING NETWORK ACTIVITY TO DETECT ANOMALIES AND THREATS

ANALYZING AND REPORTING SECURITY EVENTS
PROVIDING INSIGHTS INTO INCIDENTS FOR FASTER RESPONSE

IMPROVING DEVICE SECURITY
IMPLEMENTING MEASURES TO SECURE DEVICES AND EDUCATE USERS

INFRASTRUCTURE AND DATA PROTECTION

PROTECTING CRITICAL INFRASTRUCTURE
SAFEGUARDING ESSENTIAL SYSTEMS AND SERVICES FROM CYBERATTACKS

DATA LOSS PREVENTION (DLP)
ENSURING SENSITIVE DATA IS NOT LOST, MISUSED, OR ACCESSED BY UNAUTHORIZED USERS

SECURING WEBSITES
PROTECTING WEBSITES FROM VULNERABILITIES AND UNAUTHORIZED ACCESS

SAFEGUARDING CLOUD SERVICES
ENHANCING THE SECURITY OF CLOUD-BASED APPLICATIONS AND SERVICES

INTEGRATION AND VERSATILITY

INTEGRATING WITH SECURITY SYSTEMS
COMBINING TOOLS LIKE FIREWALLS AND ANTIVIRUS FOR STRONGER DEFENSE AND AUTOMATED RESPONSES

DIVERSE APPLICATIONS AND BENEFITS
ADAPTING TO VARIOUS ENVIRONMENTS (CLOUD, IOT, INFRASTRUCTURE) TO MEET SECURITY AND COMPLIANCE NEEDS

100% FINNISH WORK

ADVANCED PERSISTENT THREAT

MINIMIZE DAMAGE BY BLOCKING THE **APT** ATTACK IN THE EARLY STAGES

OUR EXPERT TEAM **MANUALLY ANALYZES** APT GROUP ACTIVITIES FROM VARIOUS SOURCES AND CLASSIFIES DATA INTO DIFFERENT INDICATOR CATEGORIES

WHEN NEW INDICATORS ARE ADDED, THEY'RE **AUTOMATICALLY** FORWARDED TO YOUR SYSTEM

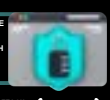
IOCS

- DATA BREACHES
- FINANCIAL LOSS
- CYBER ESPIONAGE
- POLITICAL MANIPULATION
- OPERATIONAL DISRUPTION
- NATIONAL SECURITY THREATS

.. AND MUCH MORE..

APT PLATFORM

A BROWSER-BASED SERVICE WHERE YOU CAN **TRACK APT ACTORS** AND THEIR CAMPAIGNS **WORLDWIDE** WITH A VISUAL VIEW OF ONGOING AND PAST ATTACK CAMPAIGNS



IDENTIFY RELATIONSHIPS BETWEEN INDICATORS AND **SPEED UP INCIDENT RESPONSE** BY VISUALIZING ASSOCIATED TOOLS, TACTICS, AND BEHAVIORS

ATTACK CAMPAIGNS ↔ CASES

APT OPERATORS ARE **ORGANIZED INTO GROUPS** AND MORE DETAILED CASES OR ATTACK CAMPAIGNS

USERS CAN RECEIVE **EMAIL ALERTS** FOR CASE UPDATES OR ADDITION OF NEW CASES TO THE PLATFORM

CASE PAGES CONTAIN DETAILS ABOUT THE TOOLS, TECHNIQUES, TARGETS, AND A **LISTING OF ALL INDICATORS** RELATED TO THE THREAT ACTOR

USERS CAN **SEARCH** FOR MORE INFORMATION ABOUT **THREAT ACTORS** AND THEIR TARGETS, TOOLS, AND TECHNIQUES

DDOS

(Distributed Denial of Service)

Keeps you aware of latest Denial of Service threats and malicious activities

Who Should use DDOS feed?
- Operators monitoring information security status of their networks

DDoS data feed includes malicious command and control commands issued and origin of the attack in real time

DDOS FEED INDICATORS
Timestamp
The original command
Destination address
Source address

BENEFITS
- Real-time Threat Awareness
- Malicious Command Detection
- Track the origin of Attack
- Block Traffic to C2 servers
- Detect Infected Machines

CSV The DDOS feed is available in an **easily parseable** CSV format and can be integrated to many different systems

SANDBOXIOC

Detect infected information systems with the help of IOC

Provides information on various types of malware and their C2 servers

SANBOXIOC FEED INDICATORS
- MD5 checksum of the malware
- IP address
- Malicious DNS address
- HTTP request URI

BENEFIT
Block traffic to malicious addresses

CSV The SandboxIOC feed is available in an **easily parsable** CSV format and can be integrated to many different systems

SINKHOLEIOC

Provides visibility into infected systems detected on the Internet

Who should use SinkholeIOC feed?
- Operators
- Governmental Institutions

THE SINKHOLE FEED PROVIDES ACTIONABLE INTELLIGENCE ON HUNDREDS OF THOUSANDS OF INFECTED, MALICIOUS SYSTEMS GLOBALLY

CSV The SinkholeIOC feed is available in an **easily parseable** CSV format and can be integrated to many different systems

Benefit
With the Sinkhole feed you can **locate infected devices** and prevent devices in your network from communicating to malicious addresses

In average we find **700.000** infected IP addresses daily