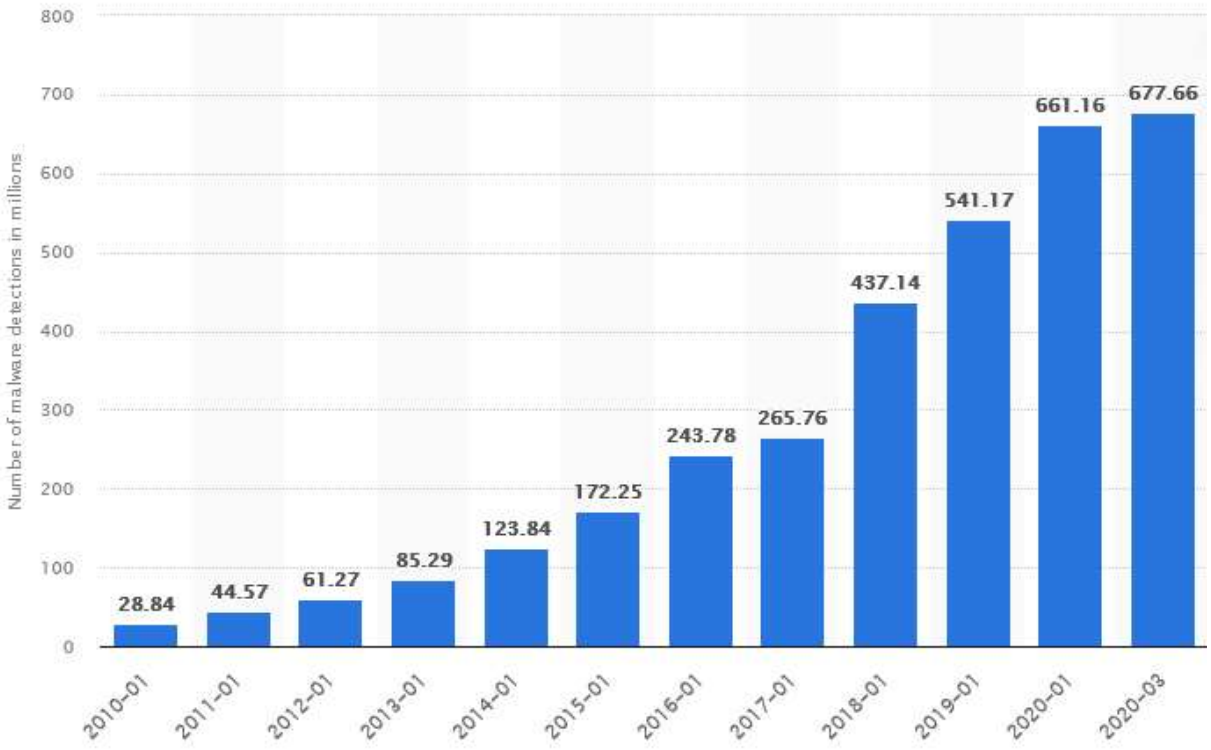
CATTIS
Centralised Tactical Threat Intelligence System

Real-time identification of today's (I)IoT cybersecurity threats, while preventing tomorrow's

Automated capability to identify, and mitigate, new attack vectors like the recent "Log4j" vulnerability

Challenges Today I - Detection

Searching for known “bad” signatures doesn’t work anymore



120 million new malware threats in the last year

329,000 new malware threats every day

Are you able to detect, sample, understand and block each of them, while maintaining normal operations?

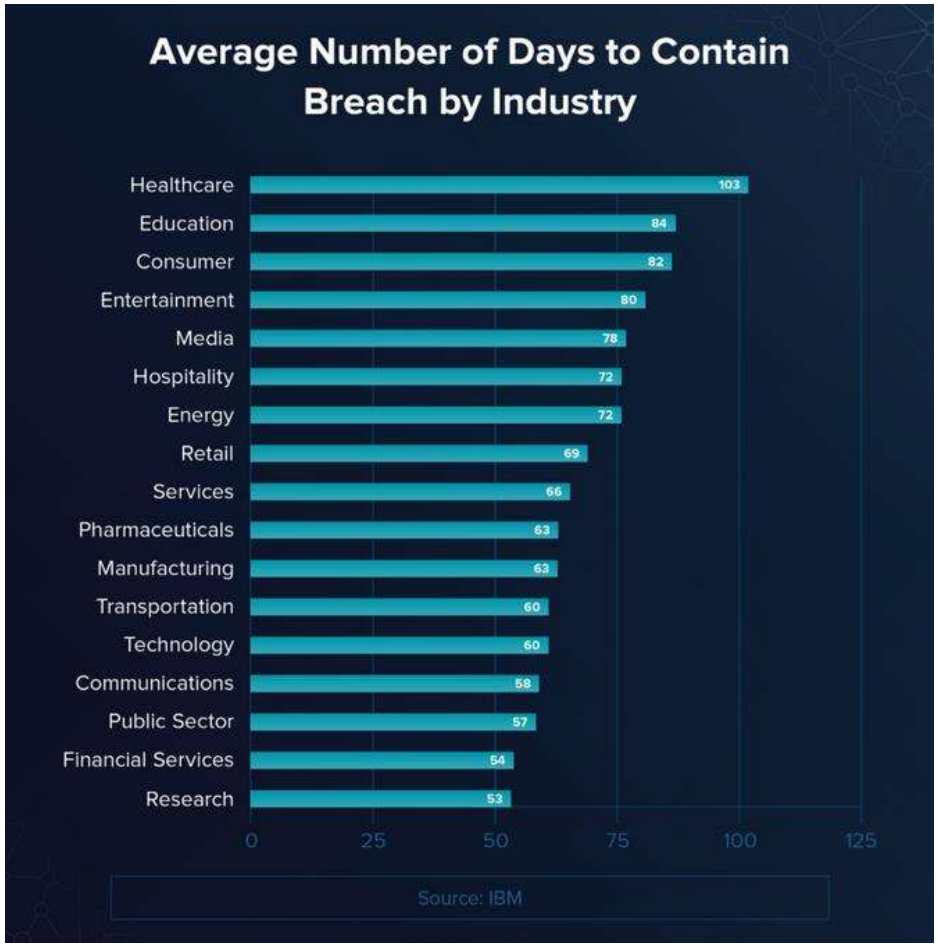
Can you detect new, unknown attacks?

Cumulative detections of newly-developed malware applications worldwide from 2015 to March 2020 in millions

https://www.statista.com/statistics/680953/global-malware-volume/

Challenges - Reactive

Days to contain an attack once detected



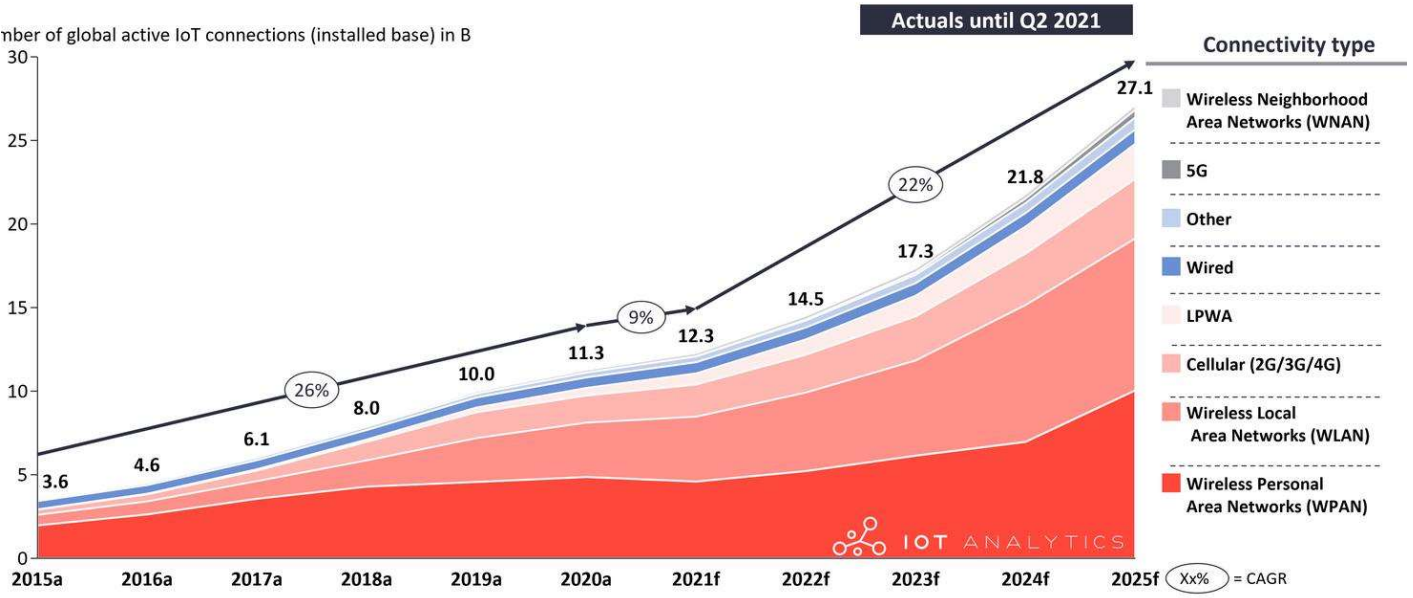
- **50 – 100 days** on average to contain an attack
- By national agencies and corporations, with **huge budgets**
- What is average time to contain an attack for SMB's who don't have security teams?

https://www.varonis.com/blog/data-breach-response-times/

A Growing, Evolving Challenge

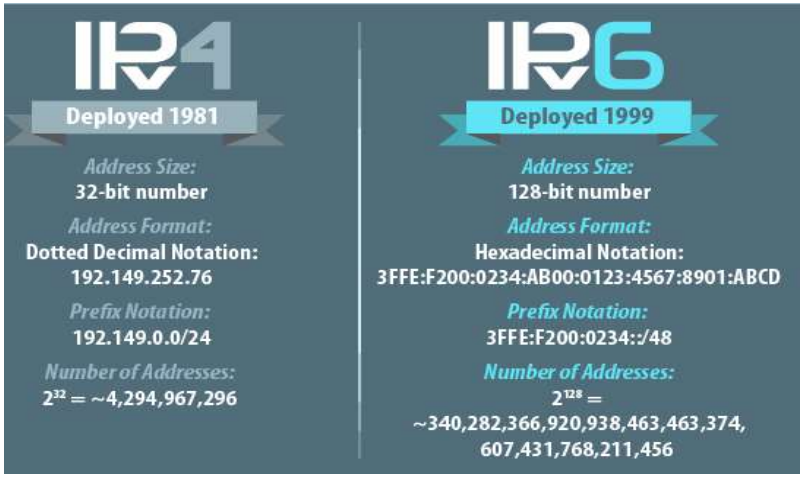
As attack vectors increase, patching becomes impossible

A: (I)IoT – **Billions of smart IoT devices** make it difficult to update and patch, and each is a potential target.



https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

B: IPv6 – Exponential increase of visible IPs on Internet. Most of IPV6 will be publicly visible as there is no need for NAT.



Number of potential attack targets = A x B

As attack vectors constantly evolve, updating and patching IIoT devices becomes impossible.
With mobile networks 5th generation, every device will be connected to the internet.

“Zero Day” – The Most Dangerous Security Threat

Zero day threats are a major problem for businesses today. They can cause serious risks, with the damage sometimes irreversible.

- Zero-day threats can be the source of some of the **most dangerous** kinds of cyberattacks. Zero-day attacks take advantage of vulnerabilities that haven’t been discovered or are not publicly known yet. One of the things that makes these threats so dangerous is that they often come without warning, posing a huge risk to the companies or individuals at stake.

- And even when discovered, **zero-day vulnerabilities can take weeks to fix**, leaving those who use the affected software at risk. And once a fix is available, the onus is on users to have a strong patch management program in place to apply the fix.

- Zero-day vulnerabilities can range from simple bugs to new and undocumented risks in the software. Why do these vulnerabilities pose such a major security risk? The basic answer is because the risk is unknown to potential victims, and the attackers using zero day vulnerabilities are often sophisticated, sometimes operating with nation-state backing.

https://www.esecurityplanet.com/threats/zero-day-threat/

THE “CATTIS” SOLUTION

Vision, Strategy, Technologies

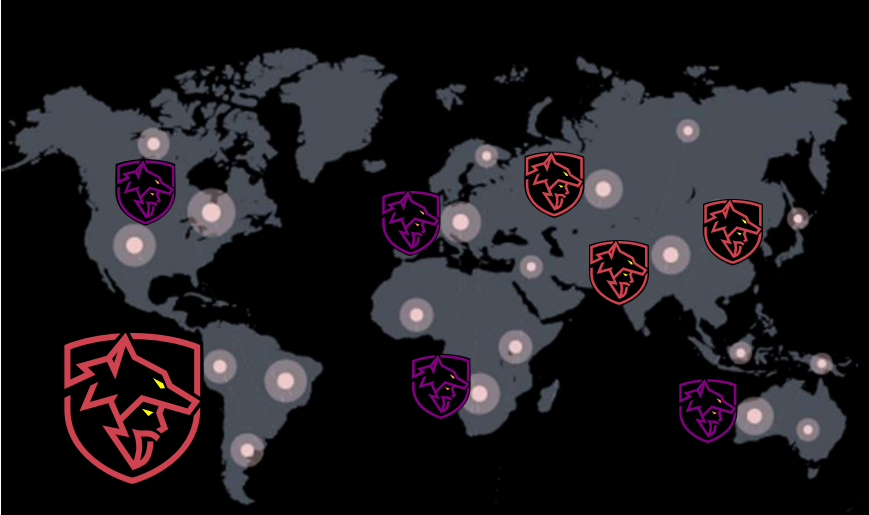
“CATTIS” VISION

The only Threat Intelligence Solution able to
proactively prevent
real-time attacks, globally.

CYBER SAFETY WITHOUT TECH HEDACHES

How It Works

Cloned IIoT/IT traps deployed globally gather real-time cyber intelligence, with continuous analysis of attack data translated into actionable insights to perform real time, automated blocking of threats for your customers



WHO | HOW

real time
attack analyses

< 10ms

Continuous Learning

BLOCK | LISTS

Real Time Threat Intelligence Data

Who, Whom, How Attacked Which IIoT Device

Detect New Attack Vectors

Correlate Advanced Attackers

Collect IoT Device specific Attack

Deliver Block Lists to EDR/NGFW with

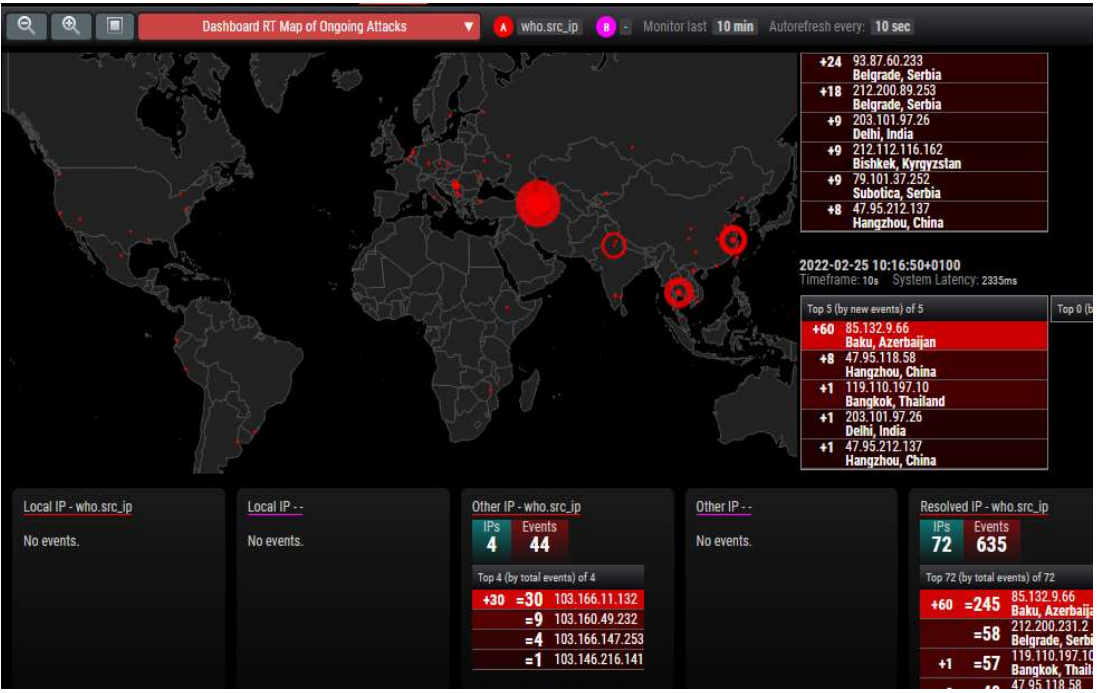
Malicious IPs, Domains, URLs, Hashes

“CATTIS” CAPABILITY

- Create cyber clones of government and corporate systems: using Go language, executing on any CPU, including IIoT & ICS CPU’s
- Expose clones to external attacks to learn and gather intelligence
- Real-Time Correlation with tokenisation: advanced sub 10ms detection
- Crowd Intelligence System: collecting ~140,000 attacks per day
- Detect, understand and prioritise attacks, with automated actions to neutralise threats
- Proactively identify new unknown Zero-Day threats and attacks specific to your country or organization

Proactive Threat Intelligence

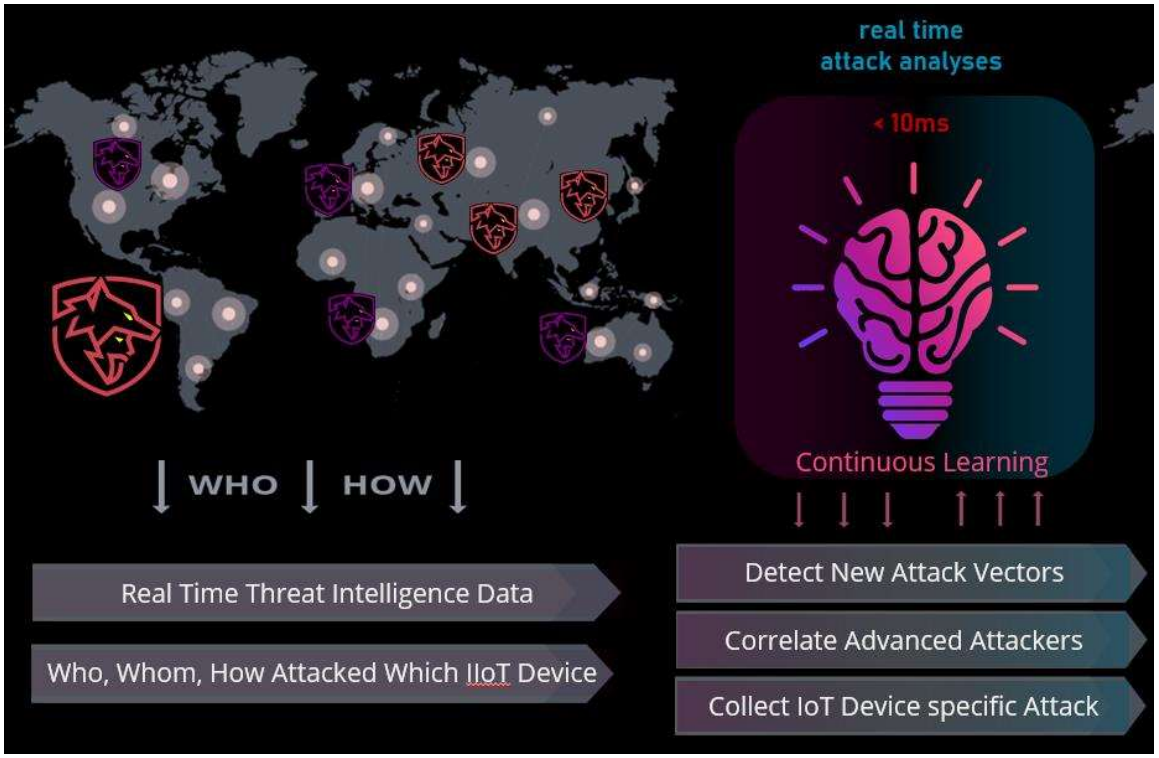
Deception to learn attack methods, applied to real-time for prevention



Baithive deception system capability:

- Clone any web interactive system (IT service, IoT interface)
- Integrates with existing customer production systems, including firewalls and EDR devices for local prophylaxis immunity
- Preventive external firewalls/IDS placed on edge Internet connections to block bad IP, bad domains, bad URLs
- Simulates standard services (SMB, FTP, MSSQL…)
- Real-time information about each attacker / attack vector
- Integration with external Threat Intelligence feeds from friendly nations
- Threat updates performed every 60s Can be executed on any platform (RaspPI, i386, IoT, virtual)
- Support for all major platforms: Fortinet, Firepower, Palo Alto..
- Whitelisting
- Data pseudonymisation

Central Intelligence Processing - ASPEN



ASPEN (Advanced Security Processing Engine)

- Collects and processes huge amounts of data in real-time (<10ms)
- Recognizes new attack vectors
- Categorizes attackers by various parameters (e.g., country of origin, reputation of IP address, slow scanning…)
- Correlates with external sources of information (3rd Party Threat Intelligence, Threatbook, MISP…)
- Recognize targeted and / or aggressive attacks
- Implements any specific detection model requirement

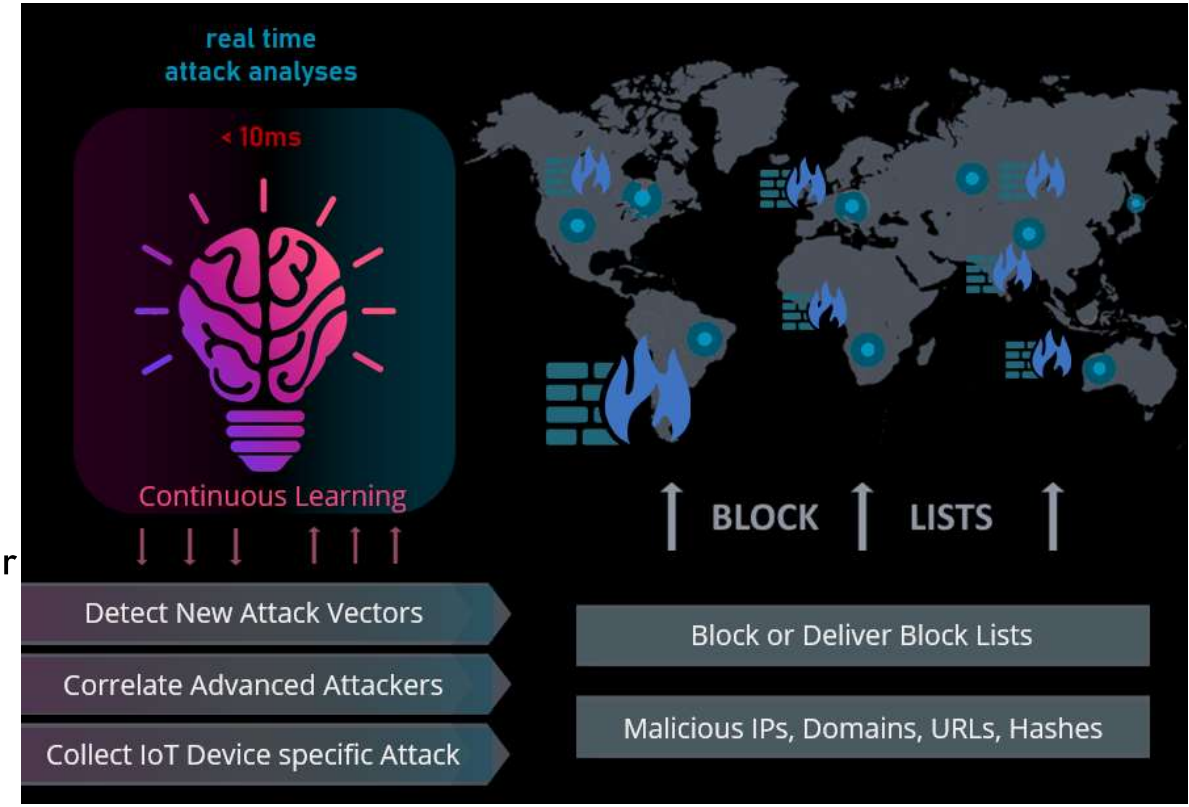
Every day we can see ~130,000 attacks (90 attacks every minute) with ~ 2.4% tools not detected by ANY antivirus (0/60)

Prevention

CATTIS – Collective immunity

CATTIS Threat Feed system capable of

- Process all IOCs from all traps
- Processes open-source threat intelligence sources
- Processes commercial threat intelligence sources
- Dynamically creates "threat feeds" depending on user preferences on any parameter, including:
  - "Confidence level" of the information source
  - type of processed IOC (IPv4, IPv6, URL, hash, netmask)
  - output format (pure text, IOC XML, STIXX XML, JSON)
  - geological location of the attacker
  - any other parameter
- Creating so-called "White lists" or exception lists for each customer individually, as well as for the entire system globally, to eliminate the possibility of blocking critical communications for the organization.
- PREVENTIVE BLOCKING is done at NGFW, EDR
- ..all this on every 60 seconds



ADVANCED SECURITY TECHNOLOGIES

"Every battle is won **BEFORE** it is fought."

Sun Tzu

Advanced Security Technologies

http://astltd.co
pr@astltd.co

Vladan Todorovic
Managing Director
vt@astltd.co