



"Crowd Cyber Immunity"
Patented solution for
prevention of unknown, zero
days attack.



ADVANCED SECURITY
TECHNOLOGIES

ZEBRA
SYSTEMS

THE CHALLENGE

The variety of cyber-attacks is growing at an exponential rate.

Most organizations use standard, reactive solutions to detect attacks and respond to incidents.

These tools are unable to detect ever-changing attacks, hidden in large amounts of data, nor to prevent attacks based on business context and threat intelligence information.

With the new, advanced cyber threats that the world is facing, businesses need to move from traditional detection platforms to new integrated data-driven tools.

OUR APPROACH, BASED ON REACH INTERNATIONAL EXPERIENCE

Through its CATIS platform, AST collects information on ongoing live attacks at 70+ locations worldwide; we collect data from patent pending solution - clone traps, we analyse them in real time (in less than 10 milliseconds) and create dynamic threat lists with a list of all IOAs - indicators of attack) that can be used to PREVENT attacks. The IOA can be an IP address, domain name, URL, file hash or any other segment of information obtained during an attack on our clients or traps.

We also integrate third-party TI resources, both commercial and publicly available, to further enrich our threat knowledge base.

These dynamic lists are integrated with client firewalls and endpoint detection and response agents (EDRs) to prevent connecting to any malicious site, IP address or URL.

This approach achieves the effect of "Crowd Immunity" - after the first attempt of an attacker to interact with the clone trap / system of one of the group members, the entire group acquires immunity to that attacker and its attack vector.

The best proof of the success of our approach is same day protection against one of greatest vulnerabilities ever, log4j.

Contact us at vt@astltd.co

IMMUNITY OF THE GROUP

Organizations must defend together. Self-defense is no longer enough.

The sharing of threats intelligence between various organizations in your territory is the basis for collective defense.

It is a unified, thus stronger approach to detecting and more important preventing cyber-attacks, which is very necessary in the midst of the evolving nature of attacks that pose a serious threat to your national security.