# Predictive Threat Intelligence "PTI"

Threat intelligence platforms (TIPs) provide a multi-layered approach to understanding and fighting cyber threats. TIPs analyze and contextualize threat information and integrate it with security operations centers (SOCs) to detect and mitigate cyber risks effectively in a reactive/proactive fashion. But our PTI is a platform that exceeds all TIPs by predicting cyber threats in advance with enough period of time to make sure the end-user is aware, ready, and fully protected before the threat occurs "**Zero-Day Protection**".

Figure (1): **Zero-Day**
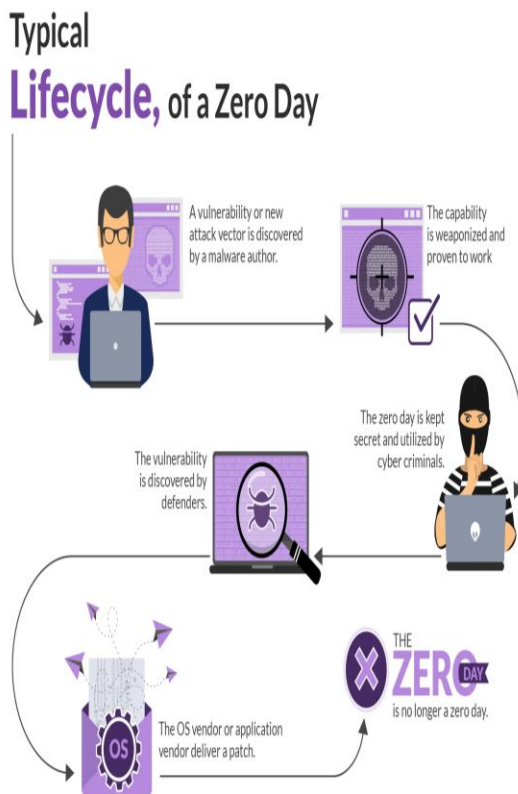
Why Our PTI Platform:

- **Gartner**-ranked Predictive TIP
- Assures **97% accuracy**
- **0.01 False/Positive**
- The best early warning system and your insurance policy **against Zero-Day Threats**
- Over **1 Million IP** predictions per **year**
- **+400K** predicted **IPs** are **confirmed yearly** by 3rd party research
- Customer telemetry detects attempted connections on +200K predicted IPs each year
- Average early **warning time +50** days
- Average Patient Zero protection time **+20 days** (time between detection of a predicted IP in customer network traffic and its first report by 3rd party sources)

- customers with suitable offer monetizing through advertising channels or direct sales

- **DPI vs Firewall:** DPI can identify dangerous data packets that may slip by firewalls in high-speed networks. DPI also gives advanced controlling options for traffic flow much beyond a firewall.

Figure (2): **How Does it Work?**
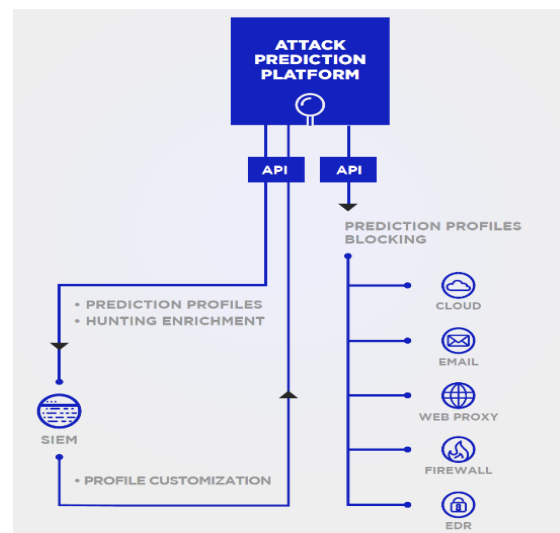
How it works

Our **Predictive Threat Intelligence "PTI"** scours the internet daily analyzing changes in the IP space (IPv4 and IPv6), domain name registrations, DNS resolution, and BGP announcements. Then leveraging supervised and unsupervised learning PTI generates potential cyber-criminal profiles and labels these profiles. In the unsupervised learning phase, the PTI generates profiles and assigns them to potential cyber-criminal and threat actor groups. During the supervised learning labels the generated profiles and labels them with a predicted threat category.

Our PTI Platform Modules:

- **Predictive Threat Intelligence**. Don't Become Patient Zero
  o Advanced Zero-day Protection
  o Delivered Directly via API

- **Predictive Detection and Response "PDR"**
  o Centralizes/aggregates and normalizes data from multiple security products across the threat surface.
  o Correlates, prioritizes and provides context and enrichment for security data and alerts. Yup.

o Adds a layer of intelligent analysis to the data rather than just pushing massive volumes of raw threat alerts.
o Provides a centralized response capability that can implement actions and change security policies.
o Simplifies and unifies security technologies to make the whole greater than the sum of its parts.

- **Threat Investigation Dashboard "TID"**
  o With access to rich threat intel sources (including our unique predictive threat intel), attribution analysis, context and enrichment data, malware samples, dark web data, and powerful search and visualization tools, our TID provides analysts with a powerful, streamlined & unified threat hunting platform.

- **Threat Data Products "TDP"**
  o Our threat data products are a must-have for mature SOCs looking to:
    ▪ Add proactive protection with predictive threat intelligence
    ▪ Rationalize threat intel costs by consolidating expenditures
    ▪ Get cost-effective access to malware samples and hashes
    ▪ Access dark web data to reduce the risk of breaches.