- ThreatBox -

- Technical Presentation -

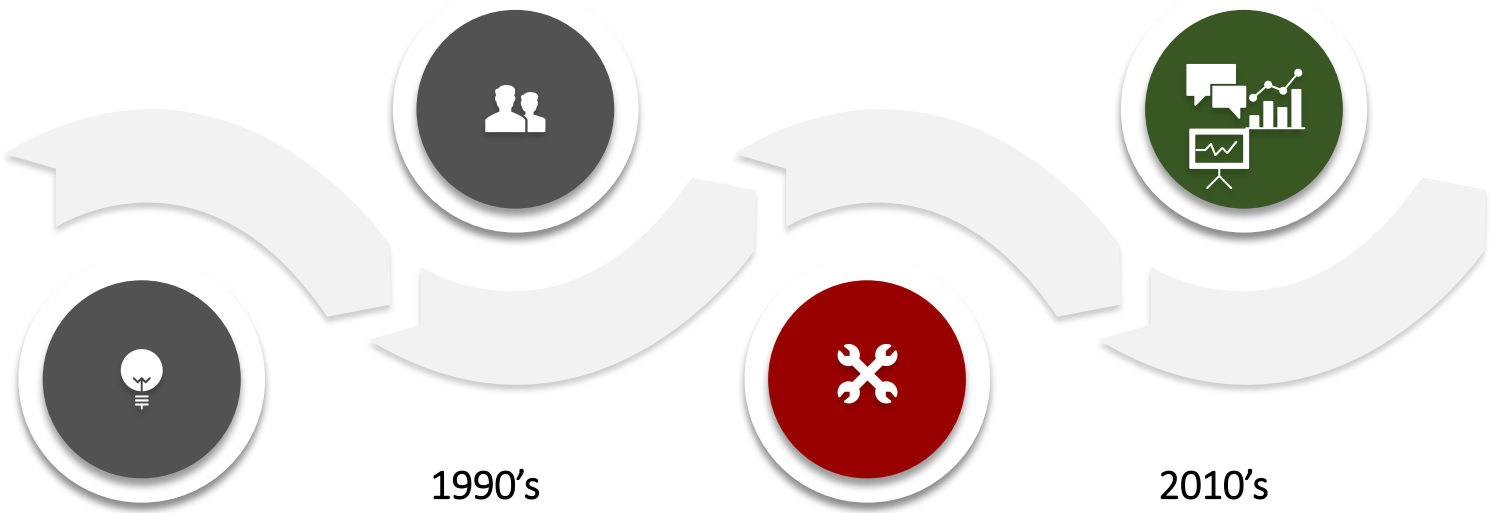
CYBER SECURITY HAS EVOLVED

1980's
The word "Hackers" was coined

1990's
"Hacker" groups appear

2000's
The SIEM era

2010's
The Intelligence Era



And cyber security will keep evolving more rapidly than ever due to the frequency of technological advancements and inter-connectivity. Such as with the increase of IoT devices, there is an ever growing attack surface for hackers.

ThreatBox

Bespoke Layer 7 Adversary Detection

ThreatBox is an application-layer deception-oriented security device, designed to alert you of intruders within your network.

You deploy a ThreatBox with a unique personality, be it a SWIFT(R) Interface, HR Portal, Prepaid Engine or more.

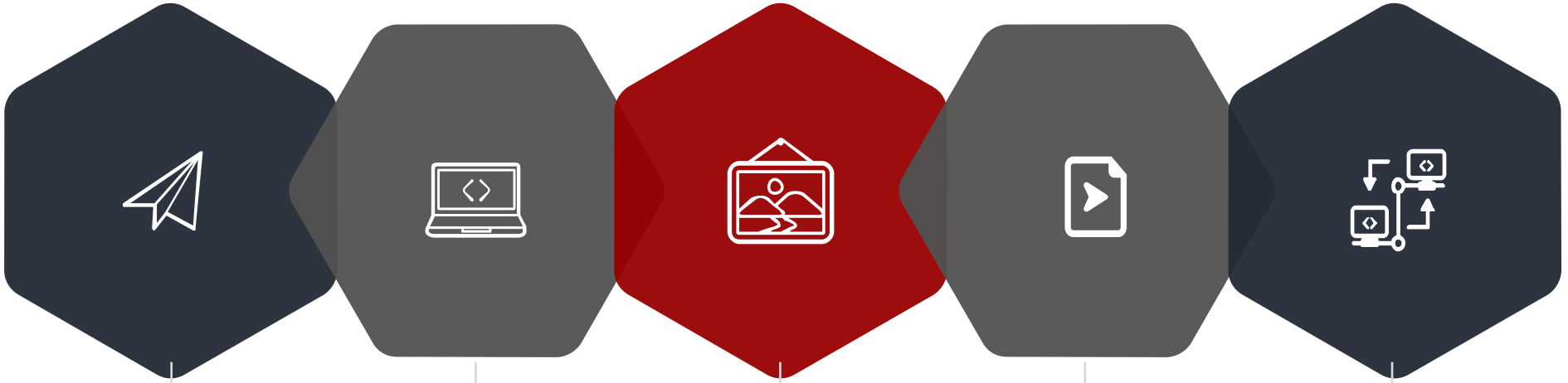
ThreatBox exposes sensitive indicators (not real ones) that respond to attackers queries, scans and general interest.

ThreatBox waits for an attack to target it and then keep them in a captive "attack" scenario all the while alerting you of the attack occuring within your network.

You are alerted of intrusion activity within your network via your dashboard, email, SMS and/or IVR Phone Calls.

ThreatBox : Features

Bespoke Layer 7 Adversary Detection



Ready-to-Plug

No Configuration Needed

Hardware

Custom-built OS & Layer 7 Application Deception Personality

Dashboard

Easily View your ThreatBox Alerts

Setup Instructions

Installation Instructions (or On-Site Consulting as an Optional Extra)

Customizable

For Large Orders Only

FAQ

"Isnt ThreatBox just a Honeypot"?

It is. But its not. A Honeypot is far more simplistic in approach, and designed to mimic network services.

Honeypots do not provide the level of sophistication that ThreatBox provides. Right down to the OS build, Mac Address and TCP header information we make sure a ThreatBox does not look like a Honeypot. Ever.

What's more, ThreatBox is designed to indicate core web applications and services.

FAQ

"Does this device scan all our traffic"?

No, A ThreatBox is a passive intrusion detection system. It does not scan any data.

It is waiting for an attacker to be active within your network, so that you know they are there.

"Are there other products like this?"

Yes, there are some products operating on a network/operating-system level, however ThreatBox is specifically targetted at attacks that occur on your web-application or "Layer 7" protocol stack.

This is where lucrative application data and systems are. This is where you want to make sure you know if someone is attacking you.

FAQ

"We use a Machine-Learning/AI Anti-Intrusion system. How does this compare?

ThreatBox is not there to replace your ISP/ISD or Machine-learning protection systems.

ThreatBox operates on a different level by being there for WHEN somebody successfully bypasses your other security layers and mechanisms.

When a ThreatBox gives an alert, it indicates the possibility of an internal breach - no matter what entry point was used for the adversary to gain access to your internal network.

FAQ

"How can an intruder access my internal network?"

The possibilities are many. But the majority come down to;

- Breach of an external server/application that is being used to "pivot" to the internal network.
- An internally placed covert device that is breaching your network (such as Ethernet->3G/LTE conversion for remote hacking)
- A Breach of your wireless network, which is allowing external attackers to gain local access.
- A compromise of a user's workstation that is allowing an attacker to access internal systems through the workstation.

There are many other paths as well.

READY TO BOOST YOUR CYBER SECURITY POSTURE?

Ask Us Anything