Cyber Defense Methodology

LTI Framework

LTI

Cyber Defense Methodology

LTI we understand & believe that there is urgency and requirement to combat Advance Threats & Attacks which are subtle & persistent in nature

Within last 10 years of Cyber Security experience, I've encountered multiple challenges related to Cyber attacks & have resolved multiple incidents with assistance from Vendor tools & ever evolving technologies. As I matured in the process of handling known attacks through upgrading myself with trainings & certifications.

I had passion to come-up with my own analogy & Innovative process, I accepted the challenge of bringing in a solution which is not only innovative in nature but also handle unknown threats based on multiple combinations of Use Cases by developing clustered correlated scenarios based on inputs from Industry best practices, especially building my own TTPs(tactics/techniques & procedures).

I decided to publish my innovative solution to my leaders, which was not easy but based on my leaders inputs I decided to be part of Center of Excellence(CoE) for Cyber Defense Resiliency Center. I initiated Use Case & playbooks inputs from different Vendors and clustered all of them by streamlining common attack patterns. And finalized 1000s of Use cases to 123 Unique Playbooks which would serve help to the Cybersecurity Industry, to start with I implemented for existing clients At LTI and this proof of concept was successful to contain many attacks which would have adverse effects.

Cyber Defense Methodology

KEY CYBERSECURITY CHALLENGES TODAY

Clustered Data to Analyse

Multiple Security Tools working in Solo

Need of Highly Skilled Resources

Challenges

Lack of End-to-End Visibility

Time Consuming and Inefficient

Response And Remediated

Expensive Resources and platforms

Cyber Defense Methodology

LTI's methodology will enable defense from cyberattack starting from early reconnaissance stages to the exfiltration of data. These clustered Use Cases will help combat kill chain attacks such as ransomware, security breaches, and advanced persistent attacks (APTs).
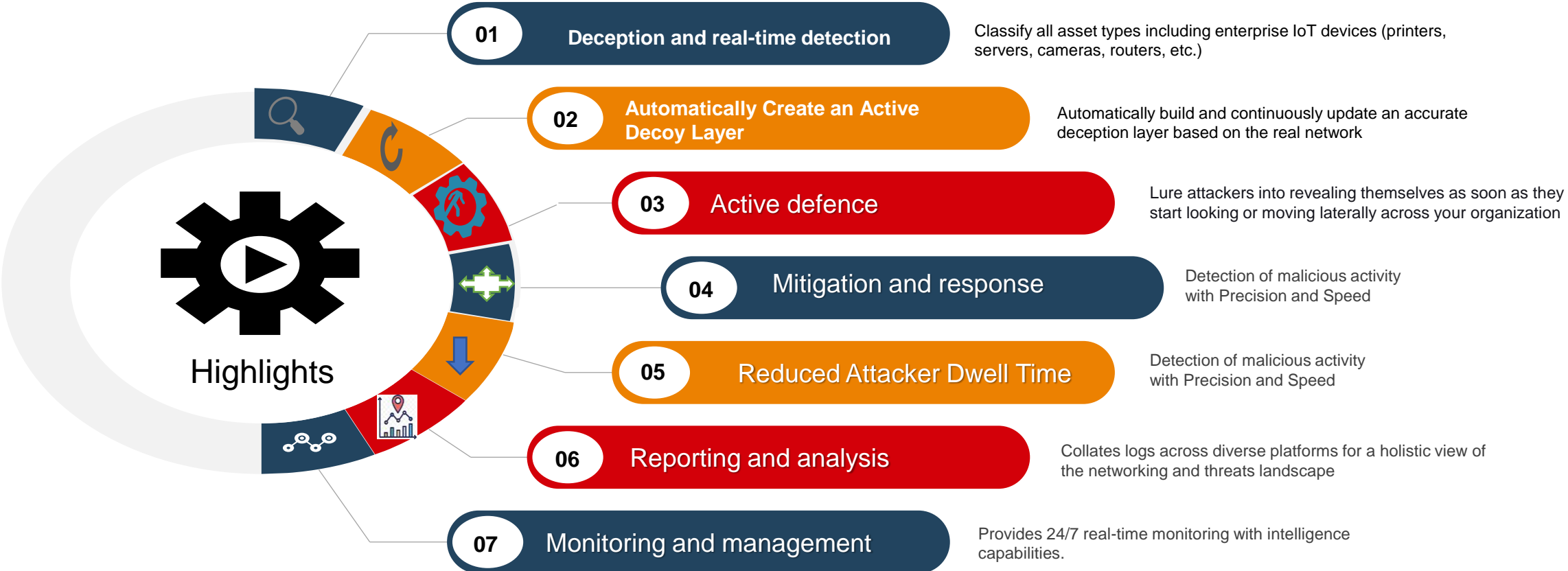
Automated Actions & Responses by Threat analysis and Investigator

- ✓ Correlation of use cases
- ✓ Defining Playbooks
- ✓ Active Threat Hunting
- ✓ Instantaneously Act

LTI

LTI Defense Methodology model Helps to understand and combat ransomware, security, breaches, and advanced persistent attacks (APTs)

Preparation | Intrusion | Active Breach

Reconnaissance — 1
Weaponization — 2
Payload — 3
Exploitation — 4
Installation — 5
Command & Control (C2) — 6
Action — 7

Hours to Months | Seconds | Months