THREAT INTELLIGENCE SERVICES

activebytes
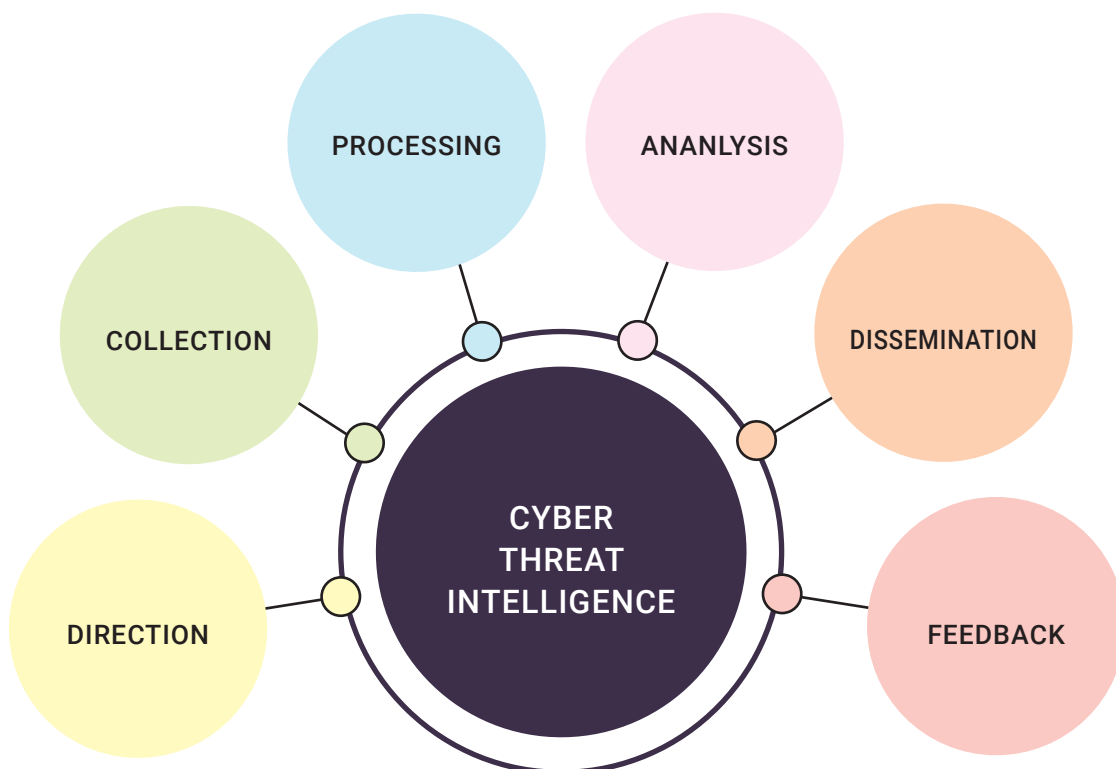innovations

Understanding the adversaries is important for any organization. ActiveBytes Innovations provide you with cyber threat intelligence, to better prepare for, and even prevent, threats from causing irreparable harm. Raw data derived from multiple sources is monitored by our experts and automated tools, then with expert research and analysis assisted by AI, this data is turned into curated threat intelligence feeds to be used by security teams. This filtered, finished data helps the SOC stay on top of new risks, vulnerabilities, and threat sources.

We leverage intelligence that is relevant and contributes to time-sensitive remediation steps. This demands planning, execution, flexibility and continual iteration to stay on target — this is known as the Cyber Threat Intelligence Cycle.

PROCESSING

ANANLYSIS

COLLECTION

DISSEMINATION

DIRECTION

CYBER THREAT INTELLIGENCE

FEEDBACK

![activebytes innovations]

DIRECTION

We first understand What needs protecting in your enterprise & why, their priorities, types of TI information required, who will be receiving the TI and how.

COLLECTION

Our dedicated intelligence team gathers information from sources such as social media, deep and dark web, network data and other open-source intelligence (OSINT) and context that fulfils the requirements learned in the initial phase.

PROCESSING

Our team then formats the data and makes it meaningful for the user based on the requirements outlined in the Direction phase.

ANALYSIS

Various techniques are used to determine if suspicious behaviors are correlated and relevant. Context and priority are added, turning the data into finished intelligence.

DISSEMINATION

Once the threat Intelligence is ready, we share it through a report, feed, or automated platform. The security team will use the TI to build and act on priority plans for mitigation and proactive protection, focusing on alerts of the highest importance or impact to their organization. Automated remediation actions may also occur – such as takedown requests, publishing of attack indicators, defense hardening, etc.

FEEDBACK

Feedbacks make threat mitigation faster and more accurate. organizational efficiency is constantly refined by redirecting assets.

Benefits

- Improve efficiency of your security team
- Collaborative knowledge
- In-depth insight into cyber threats
- Guides in incident response with IOCs and TTPs
- Provide innovative security strategies to tackle latest threats
- Leverage innovative threat modeling