Datasheet

# Threat Hunting Services

Activebytes Innovations utilize in-house automated technology to proactively search for cyber threats that lurk undetected in a network. The hunting process is mainly based on 3 approaches

## 1. HYPOTHESIS-DRIVEN INVESTIGATION

Hypothesis-driven investigations are often triggered by a new threat that's been identified with a large pool of attack data, giving insights into attackers' latest tactics, techniques, and procedures (TTP). Once a new TTP has been identified, threat hunters will then look to discover if the attacker's specific behaviors are found in their own environment.

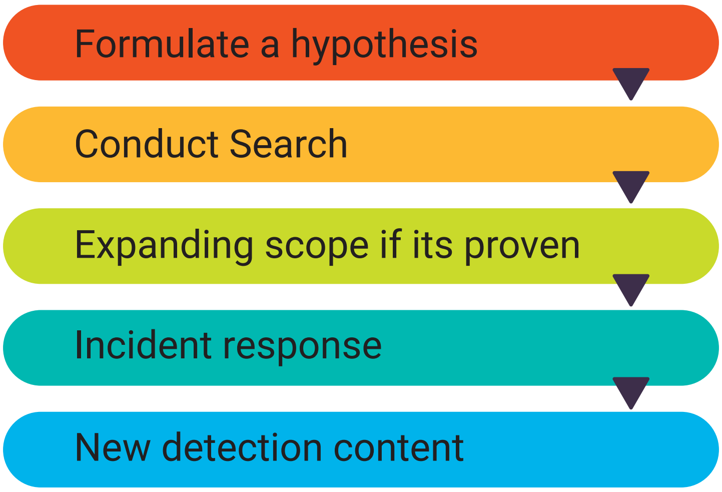
## 2. AN INVESTIGATION BASED ON KNOWN INDICATORS OF COMPROMISE OR INDICATORS OF ATTACK:

This approach to threat hunting involves leveraging tactical threat intelligence to catalogue known IOCs associated with new threats. These then become triggers that threat hunters use to uncover potential hidden attacks or ongoing malicious activity.

## 3. HYPOTHESIS-DRIVEN INVESTIGATION

The third approach combines powerful data analysis and machine learning to sift through a massive amount of information to detect irregularities that may suggest potential malicious activity. These anomalies become hunting leads that are investigated to identify stealthy threats.

We use an assumed-breach approach in threat hunting, compared to the alert-driven approach in security monitoring. We formulate a hypothesis to look for a possible attack and then confirm it has occurred or not.



Formulate a hypothesis

Conduct Search

Expanding scope if its proven

Incident response

New detection content

**For Quote Contact us @**

✉ contact@active-bytes.com ☎ +971 50 513 3973

🌐 www.active-bytes.com