activebytes innovations

Datasheet

THREAT HUNTING SERVICES

Activebytes Innovations utilize the in-house automated technology to proactively search for cyber threats that lurk undetected in your IT network. In order to provide a pro-active approach than a reactive one after getting an alert, we perform a three-approach based threat hunting. During threat hunting, we actively search for suspicious activity or remnants of any potential malicious activity within the clients infrastructure.

Our approach

Hypothesis-driven investigation

Once a new TTP has been identified, our threat hunting team will look to discover if the attacker's specific behaviors are found in the enterprise's own environment.

An investigation based on known Indicators of Compromise or Indicators of Attack

Here our team leverages tactical threat intelligence to catalogue known IOCs associated with new threats. Then based on this they uncover potential hidden attacks or ongoing malicious activity.

Advanced analytics & machine learning investigations

This combines powerful data analysis and machine learning to sift through massive amount of information to detect irregularities. These anomalies become hunting leads that are investigated by our team to identify 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 whether it has occurred in the enterprise environment or not.

Once the hypothesis is proven right, the threat hunting process shifts to a quick and appropriate incidence response plan, thereby reducing the impact on critical assets. Also, we make sure that your infrastructure is continuously analyzed for new threats that evade the existing detection techniques. We perform customized services so as to include threats from insiders that masquerade as legitimate activity, systems that were left out during security implementation and to consider the network system based on importance of related assets. The new threats detected will be added to threat intelligence knowledge pool.

Key Features

- High level of protection against targeted attacks and malware
- 24x7 monitoring and investigation support
- Accurate detection of non-malware attacks
- No time-wasting false positives
- Onsite data collection and early incident response
- Behavioral Analysis
- Report preparation
- Remediation recommendations

Benefits

- Reduced overall security costs since no need of different specialists in internal team
- Insights into attackers, their motivation
- Threat intelligence gathering
- Targeted Attack Discovery
- Detect attack at earlier stage
- Rapid incidence response
- Customized Threat hunting programs

Contact us

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

www.active-bytes.com