TRACE™

WHIZHACK
Securing Digital

Threat Reconnaissance And Classification Engine

CYBER SECURITY CENTRE OF EXCELLENCE AT IIT JODHPUR

AATMA NIRBHAR BHARAT

MAKE IN INDIA

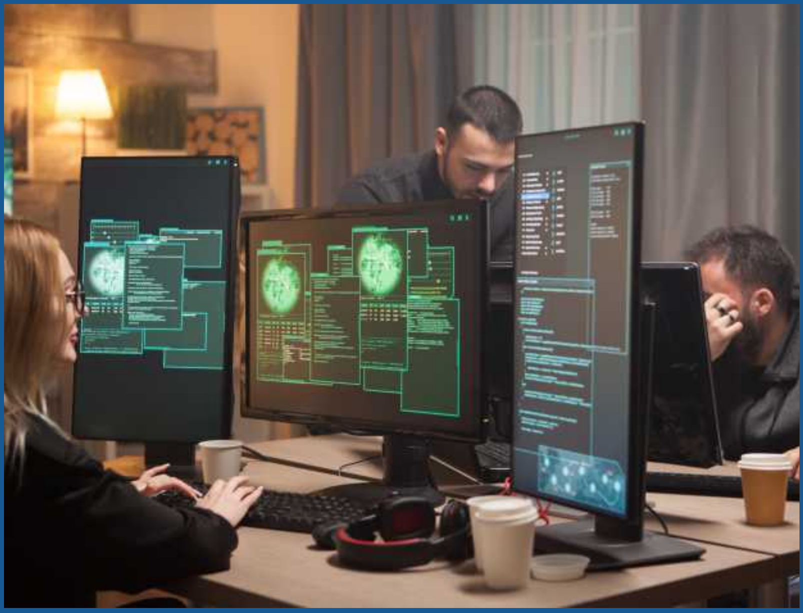
www.whizhack.com

Mail us at : info@whizhack.com

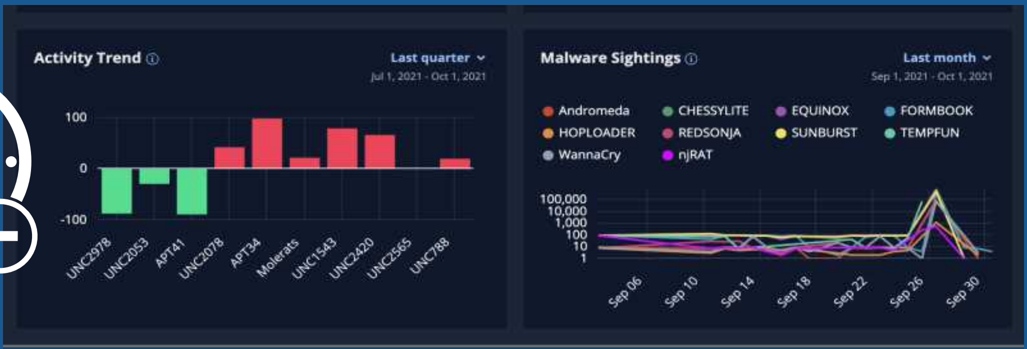
IT security teams recognize that, despite there being a range of security tools and services in place, cybercriminals are still managing to bypass them and gain entry to infrastructures. Clearly, a new approach is required. That new approach is based on cyber deception.

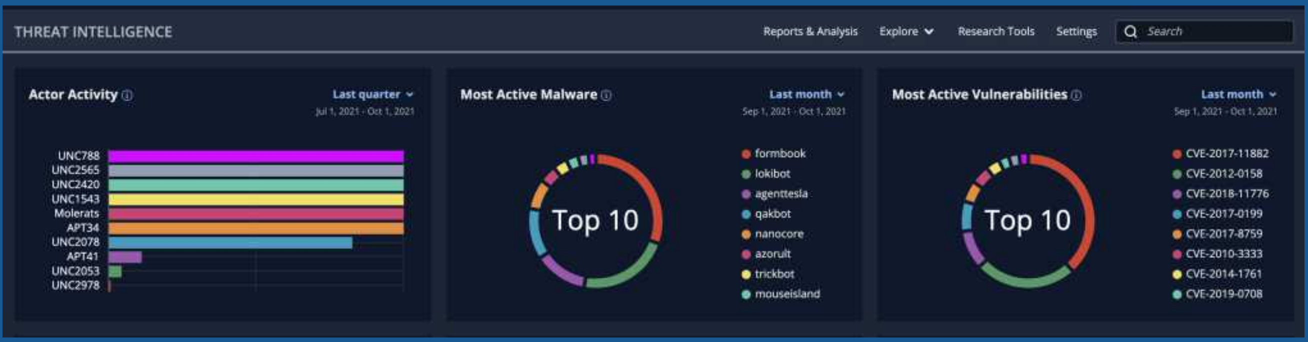
A deception strategy is also a highly effective way to detect insider threats. Any staff accessing deceptive elements is an indication that the person is roaming in parts of the network where they have no authority.

A properly instigated deception strategy, therefore, delivers six key benefits for organizations. It will:



1. Reduce the time taken to detect attacks as a flag is raised as soon as the deception assets are accessed. This gives security teams time to respond to what is going on before damage or loss occurs.





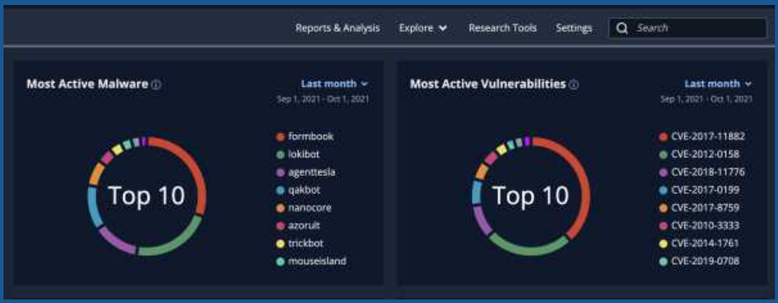
TRACE™

WHIZHACK
Securing Digital

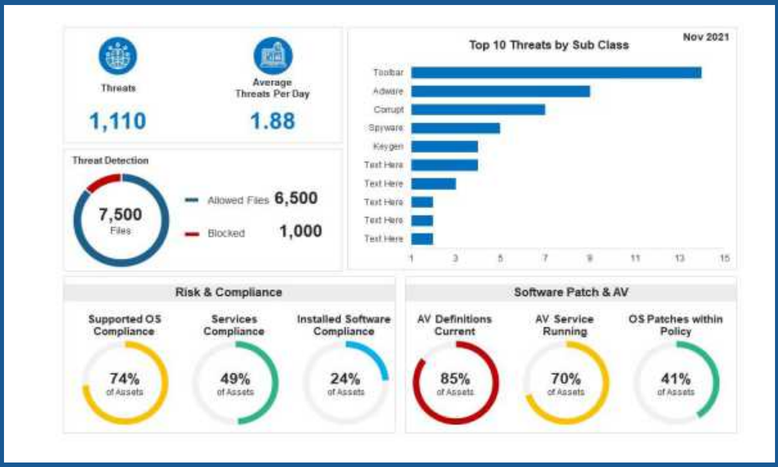
2. Trick attackers into revealing their presence within a private and public network. As soon as they begin to move laterally and encounter any deception assets, their presence will be known. This serves as an ideal safety net for when conventional protection tools have missed the intrusion.

3. Generate only high-quality, actionable alerts. Since a unique feature of Deception technology is absence of False Positives, so IT teams can be confident that deception alerts have been triggered by a substantiated event and give them priority attention.

4. Capture information about the type and nature of an attack that is taking place, enabling other defenses to be strengthened.



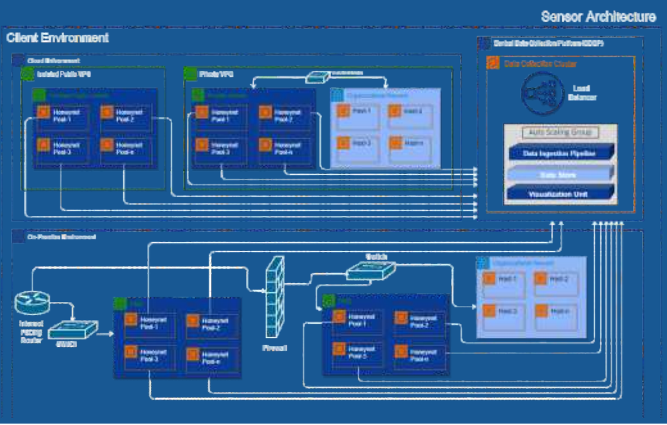
5. Deliver a Threat Intelligence Dashboard that gives security teams a clear, real-time view of exactly what is occurring within their environment.



TRACE™

WHIZHACK
Securing Digital

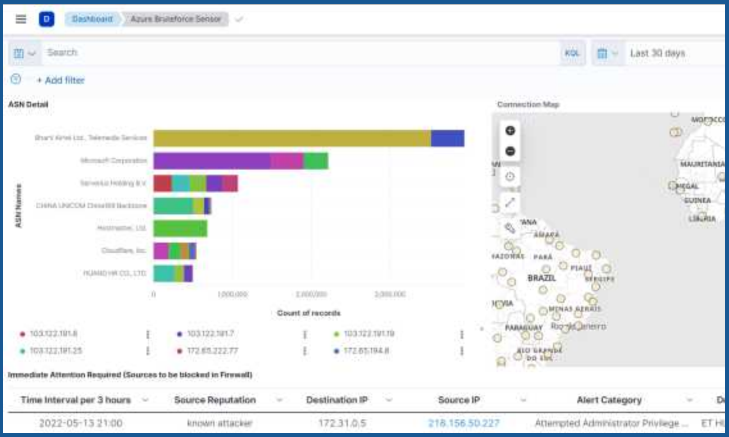
6. Create new signatures to catch even zero-day exploits before they can cause damage once DPI in the sensor data is activated.



ABOUT TRACE

TRACE is a highly scalable Cyber-Deception software (patent pending), which uses Sensors in private and public network running in a hybrid environment to detect threat in an organization's environment. It has been designed to capture and analyse live and real attacks on any enterprise. TRACE comprises of Honeynets including software scanners that are deployed, to fingerprint malicious activities, classify traffic accurately in real time and to unlock the full potential of AI-based analysis methodologies. The customer updates will consist of new product features and new Signatures for attacks not presently captured by known signatures.

A deception strategy provides businesses with another layer of protection and the ability to rapidly respond to attacks as soon as they occur in their environment. As a result, an organization can become alert and provide further security layers resulting in securing of production systems and sensitive data stores against unauthorized access, thus reducing the likelihood of disruption and loss. Taking the time to put a deception-based strategy in place will reduce overall risk and safeguard against both current threats and those that are just around the corner.



Immediate Attention Required (Sources to be blocked in Firewall)

Time Interval per 3 hours	Source Reputation	Destination IP	Source IP	Alert Category	De
2022-05-13 21:00	known attacker	172.31.0.5	218.156.50.227	Attempted Administrator Privilege ...	ET H