vehere

DNS Threat Analytics

Detect malicious threats and proactively protect your business

Vehere PacketWorker DA is a DNS Threat Analytics solution that passively sniffs and analyses, naming services data (DNS, NetBIOS, DHCP and, LLMNR) by using a purpose-built sensor - profiles behavior & proactively detect issues and malicious actors on the inside using a combination of automated & manual techniques.

Access to resources on the network happens by connecting to familiar names. Obtaining IP Addresses to names is an action performed when the client queries a Name Server for the information. Thus, analysing Naming Services data offers a treasure trove of insight into entity and network behavior that enables quicker issue resolution and prudent risk assessment.

PacketWorker DA provides complete visibility into DNS transactions, detect threats and, identifies user or client misconfiguration.

KEY HIGHLIGHTS

- Real-time analysis of DNS transactions.

- Insight about frequently queried domain names & talkative clients

- Speeds up detection of infected systems, provides supporting information including user and, device information for better management of issues.

- Detect lookup failures

- Identify clients trying to resolve malicious domains

- Troubleshoot performance bottlenecks

- Detect Automate security response through integrations by providing indicators of compromise lookup failures

KEY BENEFITS

Detects and decodes DNS, NBNS, DHCP and, LLMNR for full coverage across all naming services protocols

Purpose-built sensor deployed in promiscuous mode eliminates the need for network or client reconfiguration

Speeds up resolution of troubling outages and misconfiguration

Pre-empt security risks before they happen

▪ Detect DNS Tunneling and data exfiltration.

DIFFERENTIATORS

Zero client impact

AI/ML–powered algorithms to detect malicious domains & anomalies with actionable insights

Empowers security personnel with the context to optimize their security posture, confidently craft policies and rapidly remediate issues

Predictive analytics to identify attacks that use DNS for C2 or data theft

ABOUT VEHERE

Vehere builds intelligent and active solutions for real time Cyber Situational Awareness which forms the core component of Enterprise Cyber Defense and Homeland Security. Harnessing the power of advanced Big data Analytics, Artificial Intelligence (AI) and Machine Learning (ML), Vehere's Cyber Situational Awareness solutions have acquired a high level of efficiency, to effectively reduce the risk of a breach and to proactively defend against threats.

Book a Demo of PacketWorker DA

Learn more at **www.vehere.com**

in Vehere   🐦 InVehere   f Vehere

vehere