DATA SHEET

Seceon® aiSecureDNS empowers Enterprise and MSSP SOC teams to identify and analyze DNS based attacks and respond to security threats in real-time.

Key Benefits:

Secure DNS infrastructure

- Identify and Alerts against the Amplification DDoS Attacks on the infrastructure
- Identify and Alerts against the Volumetric DDoS attacks on the infrastructure
- Artificial Algorithms to identify DDoS Attacks

Identify suspicious Domains

- Proactively detects domains generated using DGA algorithms
- Identify blacklisted domains based on Threat Intelligence

Real time DNS traffic inspection

- Deep Packet inspection of DNS traffic to identify threats
- Real time analysis of DNS queries and responses such as increase in number of failures, etc.

Behavior Analysis

- Traffic pattern changes such as DNS packets/sec, DNS flows/sec etc. to identify APTs
- Artificial Algorithm to identify C&C communications and malicious behavior
- DNS Changer

Flexible and Scalable Deployment

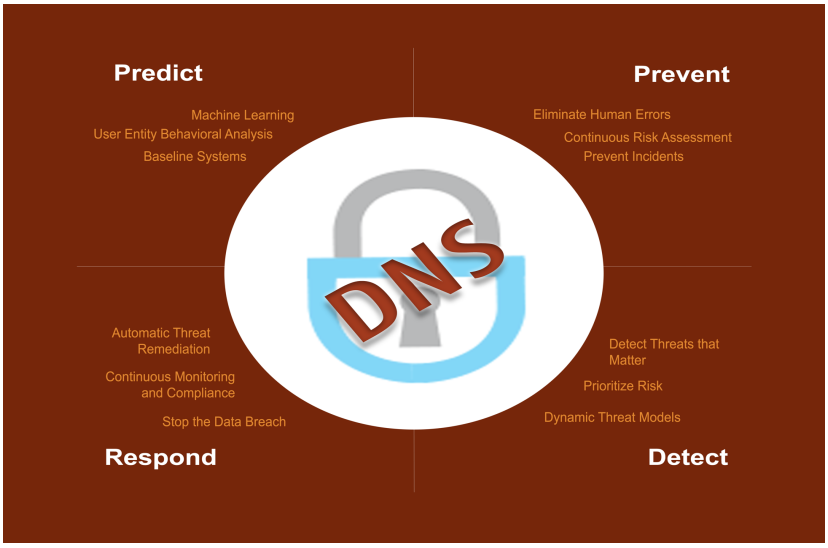
- Solution available for on-premise with single or multiple sites, in the cloud or hybrid deployment
- Scalable architecture with full support for multi-tenancy and data segregation

Automatic Containment of Threat

- Solution is capable of automatically remediating a threat by pushing a policy to block the communication with malicious domains

The Domain Name System (DNS) is the part of internet infrastructure that resolves easily remembered domain names that human's use into more obscure IP addresses that internet-connected computers use. Malware authors are using DNS protocol to keep their communications covert and evade detection. DNS today is one of the major attack vectors used by malware author for DNS command and control (C&C) and DNS exfiltration because DNS is part of internet's infrastructure and also DNS traffic is not analyzed by the firewalls and IDS/IPS devices.

Seceon® aiSecureDNS solution conducts deep packet analysis of DNS traffic to identify protocol abuses and behavior analysis to identify C&C communications, data exfiltration, APTs, DDoS attacks, Malware, DNS Tunneling etc. The solution uses Seceon Threat Intelligence (STI), an aggregation of more than 30 Threat Feed sources, to identify blacklisted domains and URLs. In addition, the solution has integration with the APIs of many Firewalls to automatically, if configured; push policy to block communication with blacklisted domains, C&C communications etc.



For more information and pricing, please contact Seceon at sales@seceon.com