CyberSentinel DNS

Jeskell CyberSentinel Threat Detector

The Problem

Organizations of every size, sector, and mission are confronted with an ever proliferating threat environment. The traditional "rules-and-signatures" approach to cyber security analytics can work, if you're targeting known threats. But this approach can fall short in the face of an increasingly sophisticated threat environment.

To combat these emerging threats, organizations must also take a more sophisticated approach. **CyberSentinel** DNS offers a more adaptive defense by leveraging machine learning, predictive analytics, and heuristic methods to uncover the "unknown-unknowns" in your environment.

Benefits of CyberSentinel DNS

- ***Lower information security risk***
The threat environment is rapidly evolving, and traditional security solutions are falling short. CyberSentinel's adaptive approach targets tactics and techniques used by today's most advanced threats
- ***No need to worry about setup***
CyberSentinel is a 1U appliance that comes standard with installation and configuration services, giving customers quick time-to-value
- ***Lower total cost of ownership***
Leverages industry leading predictive analytics models and machine learning algorithms so your staff spends more time on what really matters
- ***Performance focused***
Can process over 10K/tuples per second within in a reliable streaming data analytics framework

The Solution

The CyberSentinel DNS appliance uses adversarial tactics, techniques, and procedures, rather than simply targeting signatures that can be easily changed and obfuscated. CyberSentinel DNS detects the following:

- **Domain Generation Algorithms**–Utilized by malware to generate a large number of domain names where they can use to communicate with command and control servers. This technique is used by crimeware families like Conficker, Murofet, BankPatch, Bonnana and Bobax to obfuscate the botnet command and control servers as well as avoid domain blacklisting.
- **Malicious Domain Behavior**–Utilizing predictive analytics and machine learning behavioral analysis can be completed on queried records and their response patterns. Utilizing this technique utilizes over 20 feature vectors to accurately predict if the behavior of a domain is outside of normal behavior. This targets adversarial tactics and while the adaptive approach provides limitless possibilities one example would be the Angler exploit kit.
- **DNS Amplification Attacks**–A popular type of Distributed Denial of Service Attack in which attackers flood target systems with redirected DNS Response messages.
- **DNS Tunneling Attacks**–Used to pass information via different protocol from within the DNS system. Can be used for command and control or exfiltration.

Click the QR code to learn more, or visit the URL listed below:

www.jeskell.com/cybersentinel-advanced-persistent-threat-detection