CLEVERDetect® for DNS 1.2

Empowering IT Cloud Security Anywhere, Anytime

CLEVER® Business Cloud Security Management

Key Features

- **DNS Diff** exposes changes in DNS records which could be due to malicious activity.
- **DNS Monitor** shows real-time changes in DNS records compared to a baseline with customized interval recording.
- **DNS Dashboard** provides centralized, customizable overview of DNS alerts, DNS DIFF and DNS Lookup performance metrics.
- **Audit report** displays historical details on when a DNS record was different from the baseline.
- Ensures real-time notification of DNS record changes to the appropriate IT knowledge worker with **structured alert levels** and **alert notification reports.**
- **Web Browser and Mobile app** provides enhanced mobility to DNS record changes.
- **Rearm** capability avoids flooding mobile device with repetitive alerts.
- **E2E Reports** displays DNS record Lookup response times.
- Assists in the detection of **cache poisoning**, **amplification**, and **redirection** vulnerabilities.

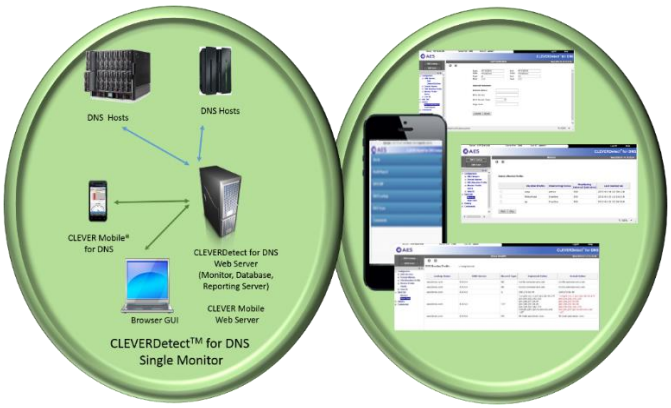
AES
P.O. Box 50927
Palo Alto, CA 94303
650-617-2400
www.aesclever.com
info@aesclever.com

Threats to the DNS system is one of the most exploited infrastructure system by hackers. Since DNS impacts all access to IP things, CIO's are putting major focus on projects to protect and inform about potential DNS server activity that could be due to hacker attacks. Getting the right tools to the DNS Administrator and Forensics Analysts are key.

One of the few things everyone agrees about on cybersecurity is that it is all about reducing and managing risk. The major components of risk are threats and vulnerabilities, and risk levels go through cycles as threats and vulnerabilities wax and wane. The major factors that cause those elements to vary are changes in technology and changes in business processes.

DNS vulnerabilities are second only to HTTP in the number and frequency of exploitation by hackers. With DNS being the 'Internet's Directory Assistance', gaining control of a DNS server can run havoc on your business sending users, clients, and employees to the wrong servers. This can result in misinformation being relayed, userids and passwords or confidential information being acquired by cyber thieves, or malware being placed on unsuspecting systems. Understanding if your DNS servers have been compromised by techniques like cache poisoning, amplification, or redirection is essential to protecting your business, employees, clients and users in general.

CLEVERDetect for DNS 1.2 is designed to help DNS administrators, infrastructure analysts, operations personnel, security analysts, and enterprise knowledge workers effectively understand changes in DNS records entries. **DNS Diff** compares DNS records in either automated monitoring mode or real-time on demand mode against defined baselines. It detects suspected activities like Cache Poisoning which is one of the most important hacking activities to understand immediately to prevent negative impact to the business.



Applied Expert Systems - The Business Cloud Security Company

Highlights of CLEVERDetect for DNS

DNS is vulnerable to attackers. The bad guys can create DNS denial of service, use "footprinting" to discover information about your network resources, spoof IPs, or redirect DNS queries to their own servers ("Cache Poisoning"). Given the critical importance of DNS to normal network operations for both intranet and Internet connections, it's clear that DNS security is an important consideration and something that shouldn't be left to the "we'll get around to that" pile.

- **DNS Diff** exposes changes in DNS records which could be due to malicious activity
- **Web Browser and Mobile app** provide enhanced mobility to DNS record changes
- Ensures real-time notification of DNS record changes to the appropriate IT knowledge worker with **structured alert levels** and **alert notification reports**
- Identifies who will receive specific alert details for decision making with the **user authorization level function**
- **Rearm** capability avoids flooding mobile device with repetitive alerts
- **Audit report** displays historical details on when a DNS record was different from the baseline
- **Commands** provides access to common TCP/IP functions like Ping and Traceroute to aid in forensic diagnosis
- Assists in the detection of **cache poisoning**, **amplification**, and **redirection** vulnerabilities
- **DNS Monitor** shows real-time changes in DNS records compared to a baseline with customized interval recording

New Functions in CLEVERDetect for DNS 1.2 include:

- **Additional Linux Support:** Support has been added for SLES 12 and RHEL 7 for the web server running on z System.
- **New Linux Support on IBM Power Systems:** Support is now provided for SLES 10, 11, 12 and RHEL 5, 6, 7 for the Web Server running on IBM Power Systems.
- **DNS Dashboard Function:** Provides centralized, customizable overview of activity with information on:
  - DNS record change alerts
  - DNS Diff Consolidated Summary and DNS Diff Summary for specified servers
  - DNS E2E consolidated Summary and DNS E2E Summary for specified servers.
- **DNS End-End (E2E) Report:** This report displays DNS record lookup response time. This is the time for the DNS server to look up and return a DNS record. The response time is calculated for all DNS record types or selected DNS record types per server; summarized over a period of an hour or a day. The DNS Lookup Timeout parameter specifies the timeout value in seconds for looking up a DNS record.
- **WHOIS Lookup:** This function allows a user to look up domain registration information for a domain.
- **SIEM Integration:** The ability to send CLEVERDetect alerts and events to a syslog server is now available. This complements its existing ability to send SNMP trap notification details.
- **Real-Time DNS Diff Enhancement:** Import of DNS zone File for real-time comparison improves accuracy and increases operators' efficiency.

System Requirements

- **Linux Servers:** SUSE Linux Enterprise Server 11 or above, or Red Hat® Enterprise Linux® 6 or above
- **Hardware/Processor Platforms:** IBM z Systems, IBM LinuxONE, IBM Power, x86-64
- **Database:** MySQL™ Server 5.0 or above (distributed with Linux)
- **Java Web Server:** Apache Tomcat 7.0 and JDK/JRE Version 7
- **Web Browser:** IE 8.0 or above, Mozilla Firefox 40.x or above, or Chrome

Optional feature CLEVER Mobile for DNS System Requirements

- **Android:** 4.0 or above
- **iOS:** 5.0 or above

AES
P.O. Box 50927, Palo Alto, CA 94303 USA
Phone: (650) 617-2400
Fax: (650) 617-2420
Website: www.aesclever.com Email: info@aesclever.com

MM-10-1610-DS1