Hewlett Packard
Enterprise

HPE Security ArcSight DNS Malware Analytics

Software Version: 2.4

User's Guide

February 8, 2017

Chapter 1: Introduction

DNS Malware Analytics (DMA) is a scalable, cloud-based threat detector that monitors DNS traffic and rapidly identifies an infected system, enabling immediate remediation in real time. The application can function in a stand-alone configuration as well as in a Security Operations Center (SOC), using HPE - Security ArcSight Enterprise Security Manager (ESM) as the Security Information and Event Management (SIEM) tool.

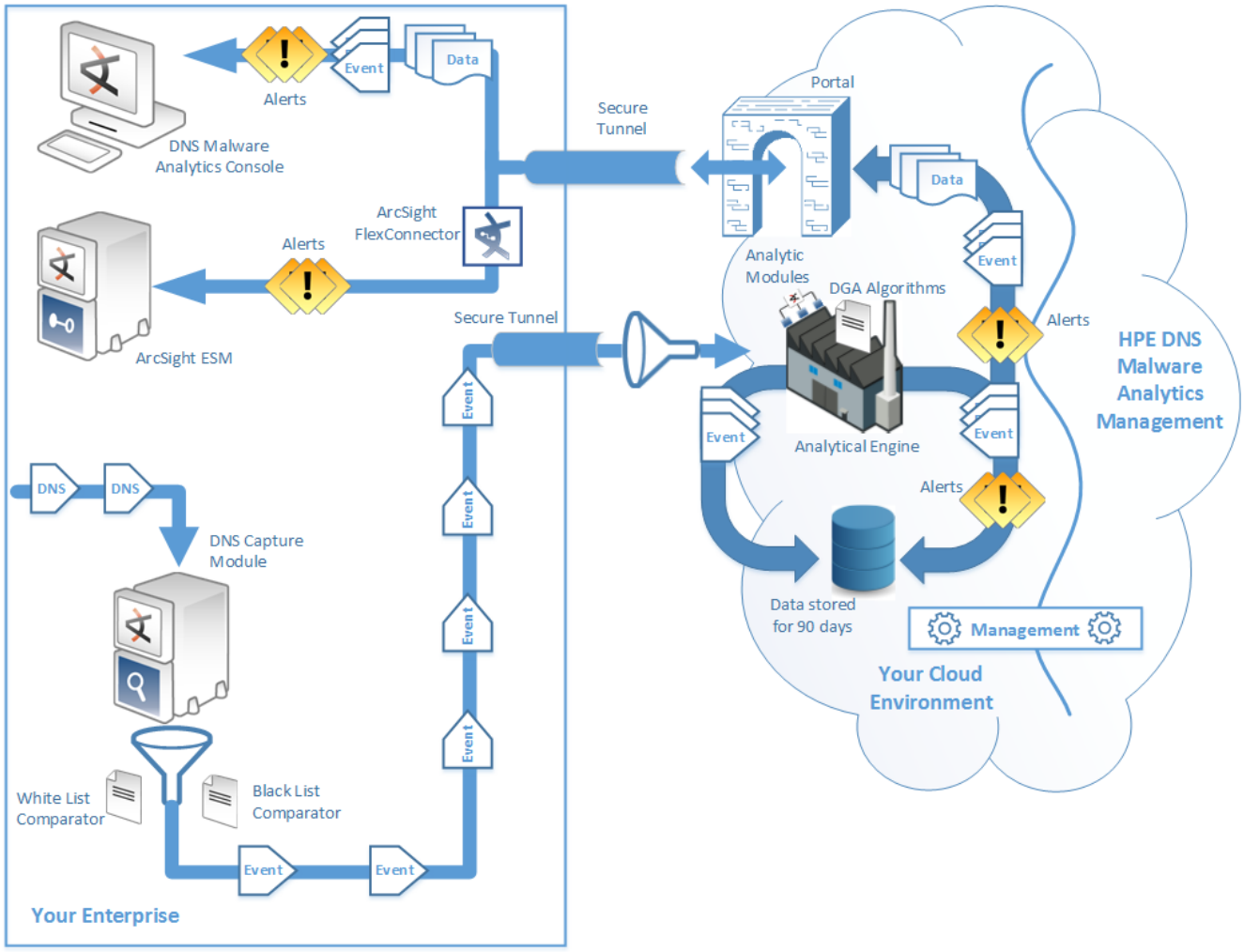
DMA is uniquely differentiated in terms of speed (analyzes billions of DNS packets daily), cloud delivery (cloud-delivered functionality), and scalability with seamless SIEM integration. DMA provides you with an automated infection detection system, allowing enterprises to detect the unknown threats that are the biggest source of risk to enterprise applications, systems, and data.

DMA can detect:

- Blacklist matching — Clients infected with malware that uses blacklisted command-and-control (C&C) domains.
- Botnet to C&C servers — Can be from the client or the domain.
- Cloud platform abuse — Malware infections.
- Standard behavior and conduct violations — Forbidden domains.

How DNS Malware Analytics works

DNS Malware Analytics (DMA) consists of two analytic platforms. The first is the on-premise DNS Capture Module (DCM) which is a packet-capture device that “listens to” DNS traffic from network links that are connected to internal DNS servers. The second platform is the cloud-based DNS Analytics, which acts as a “black-box” analyzer of DNS events sent from the DCM. These two servers identify infected systems and issues alerts to an upstream SIEM, such as HPE - Security ArcSight Enterprise Security Manager (ESM).



The DCM "sniffs" DNS packets using a TAP (network switch) or SPAN, located between end-point stations and the DNS Server or cluster on the network. The DCM then converts the packets to metadata while discarding packets that are not DNS.

The DCM then filters out “good” DNS queries and responses using a white list comparator. The module only keeps the metadata which is anomalous (suspect or unknown), which is a subset of the overall DNS traffic. (Experience shows that the “good” or discarded traffic is about 99% of the total traffic.)

The anomalous traffic is then passed through another comparator, a blacklist which identifies and labels domain names which are malicious or dangerous. Any remaining anomalous metadata that is unknown is labeled as graylisted.

Next, the DCM converts the anomalous metadata into Common Event Format (CEF) format, to be transported out of the module as DNS events.

The DNS events are sent from the DCM to the DNS Analytical Cloud through a secured tunnel. The DNS events from various DCMs are collected and aggregated in the Analytic Cluster, which is located in a public cloud instance.

The cloud-based Analytical Engine stores the DNS events and also processes them through a set of Analytic Modules, which are a set of plug-ins that provide the intelligence to identify infected clients. These modules are automatically updated by HPE data scientists at regular intervals—and when new threats and conditions are found in the wild. The updated modules are then added to the Analytical Engine so that the latest threat algorithms and detectors are used. You cannot configure the Analytic Modules.

The Analytical Engine can detect seemingly random domain names generated by Domain Generation Algorithms (DGA).

Based on scoring and weighting algorithms, the Analytical Engine generates an alert when an infected IP address is detected. The alert, along with related data (timestamp, alert type, and client IP) can be sent to HPE - ArcSight ESM through the ArcSight Smart Connector for analysis. Other SIEMs can also be used.

DMA pages

DMA enables you to investigate an alert by completing various tasks from the following DMA Console pages:

- Dashboard — Comprised of four widgets, which provide overall status of alerts and infections for a selected daily period. Using these widgets, you can learn about infected client IPs, the domains that the malware on the infected systems are trying to contact or are being contacted by malicious domains, and the alerts triggered by DNS events.
- Alerts — For a specified time range, displays a summary of alerts that were triggered as the result of infected client IPs. It also displays exactly when an alert occurred and the type of alerts that occurred. It also displays the client IPs that were infected.
- Alerts > Alert Details — Shows details around a single IP address (alert). Also provided is a table of triggering DNS events, where the query and response details surrounding a particular alert are given. This includes offending malware, requested domain, event category, and any possible resolution.
- DNS Finder — Enables you to search, based on a time period, the entire database in order to discover infected client IPs or suspicious domains. For both of these searches, you can also learn of the alerts and DNS events associated with each. The results of these searches can be filtered by client IPs or domains, depending on the search type.

From the DMA Portal, you can use the following product pages to manage the service:

- Devices — Where DCMs are managed. This can include adding content to the blacklist and whitelist, controlling the DNS packet flow from the DCM to the Device Manager, and naming the DCM.
- Users — Where users (analysts) are managed. This includes adding analysts and managing their information, along with setting analyst activation. Also from here, the name of the organization can be changed.

The Analytical Cloud—where the Analytical Engine resides, is managed by the HPE DNS Malware Analytics Management Team. While the DMA service retains your data for up to 90 days, in no way can the data be accessed or viewed by anyone but you.

Roles and functions

- HPE administrator — Member of the HPE DNS Malware Analytics Management Team

  Access

  HPE DMA Portal (Customers page and Clusters page)

  Functions

  - Provision (add) and remove SOC administrators in the Analytical Cloud database
  - Start and stop the Analytical Cloud
  - Enable and update DCMs
  - Enable and update Analytics Modules
  - View status of processes
- DMA administrator

  Access

  DMA Portal and DMA Console

  Functions

  - Manages the analysts and DCMs of the organization
  - Can operate as an analyst
  - Add analysts
  - Start and stop the DCM
  - Modify and update the blacklist and whitelist
  - View statuses of processes
- DMA Analysts

  Access

  DMA Console, but not the DMA Portal

  Functions

  - Analyze network activity
  - Export alerts (in CVS format)