Nucleon

HashLife API - Reliable Threat Intelligence

Abstract:

Today world contains many security threats, known and unknown.
The overflow of information and different sources making it time consuming for cyber analysts and investigators to find reliable processed intelligence that can assist them with their tasks and support their decisions

This document will provide brief introduction to Nucleon innovative cyber threat technology and will explain how it can help different organisations from governments affiliated to ,law enforcement and professional security teams to digest reliable constant feeds of high quality reliable intelligence that can be further implemented in its other security tools and systems.

This Document is aimed for security professional that want to get a deeper understanding and overview about Nucleon's technology and how to it can be implemented successfully in different scenarios.

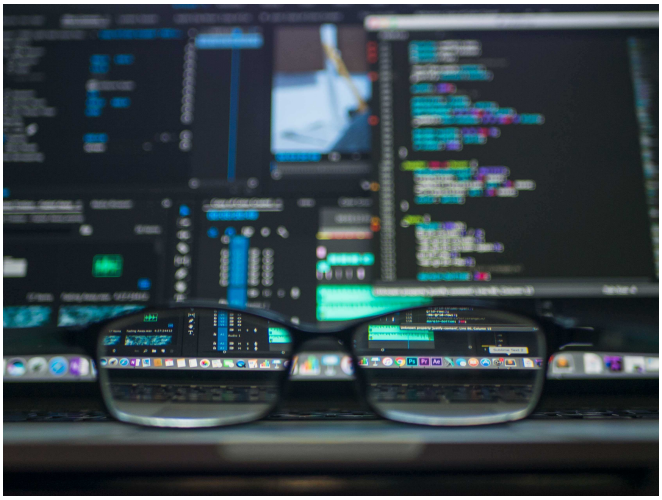
KEY TAKEAWAYS:

- **How Nucleon Gather Intelligence.**
- **How Nucleon Delivers Hash indicators as threat intelligence**
- **How Organizations can benefit from using Nucleon Hash Life API**

Introduction

Sophisticated attacks are becoming more and more common as tools evolving and reducing the time required to launch sophisticated attacks.

This creates a situation where hacking campaigns that used to take months to plan, develop and execute several years ago, can be done and managed by anyone with basic skills.
This creates variety of challenges for those who needs to protect or investigate such networks or incidents.
In order to defend against sophisticated attacks, organizations needs to know how to handle and respond to multiple threats using different vectors (web,mail, etc.) with limited resources.
Many organizations don't have the human power to have dedicated personnel to deal with cyber security and even those that have dedicated security personnel, they don't always have the time or expertise to deal and investegate attacks properly.
Organizations are always left behind the hackers trying to attack them because they are using tools that are reactive by design.Most of the tools today are followers, tools that respond to incidents and events that are identified when or after they are happening.
That is good start but in today's world, it is not enough. A proactive approach is needed to eliminate threats before they are breaching the network and after.



Background

Nucleon provides comprehensive set of solutions offering strategic and tactical cyber threat intelligence.
Nucleon enables security teams to focus on analyzing or handling security threats before they become breaches.
Using Nucleon, security engineers can implement automatic methodologies to block known threats, this white paper will focus on protecting organizations from malicious malware using hash signatures.

Benefits

The Hash Life API is a comprehensive easy to use API that provides constant updating feed of hash files known to be carrying malware.

Using the feed, organizations can implement automatic strategy for blocking and alerting malware trying to access the network.

The API also can be used for cyber investigations, allowing investigators to receive different details about specific hash, including its complete history of where and when the specific hash was seen being used.

The Hash life API is easy to use API and it support most of the major threat exchange formats exists today.The feed can be easily integrated in different cyber security tools such as SIEMs, Mail gateways and endpoint protection devices.

The API not only provides the history of incidents where the hash was seen it also provides details about the binary file it self, information that comes to help investigators to quickly search and find properties that are important for their specific investigation.

0% False Positives

Nucleon Unique approach provides organizations the needed confidence that no false positives will be delivered.
Nucleon is never reaching ut to the internet searching for intelligence, all the intelligence is gathered based on actual attacks that happened.
That enables organizations to safetly activate blocking active threats that Nucleon alerting about.

The Solution

Polymorphic Sensors

Nucleon methodology for extracting and providing relevant malicious hashes begins with its patent pending polymorphic sensors technology.The polymorphic sensors are the places where Nucleon collects its information about cyber attacks to process and turn it into useful actionable intelligence.Nucleon polymorphic sensors allows Nucleon to stay hidden from those trying to identify and mark decoy servers (a.k.a honeypots) over the internet.

Brain

To handle the flow of attacks and find unique quality intelligence Nucleon developed its own unique Neural network (a.k.a Brain) that can deal with huge amounts of data and analyze it in order to find the unknown.
Nucleon Brain network is an autonomous self studying network that is aimed to search and learn about hidden patterns of attacks.
Brain is optimised and focused on examining different cyber attacks that are received constantly analyse and learn about the visible and hidden sides of specific attacks, Brain is able to detect, analyse and verify new security threats on its own which gives the flexibility to send out indicators including details.

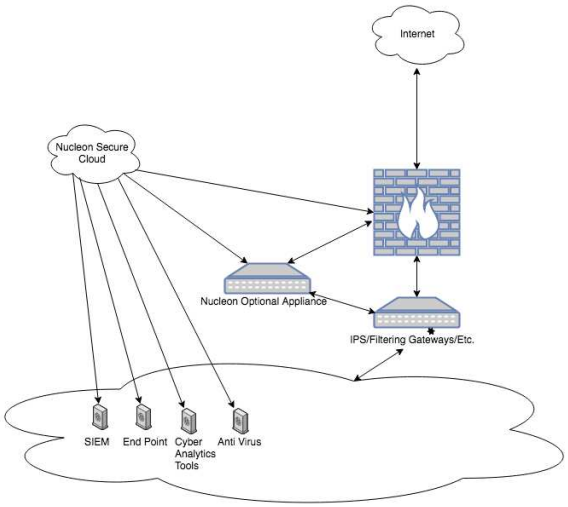
The API

Nucleon RESTful API allows clients to deliver intelligence quickly to clients.
The API supports different output formats, whether the output needs to be read by commercial SIEM or by custom software, Nucleons provides an easy and efficient way to connect and start working.

Integration options

SIEM and Gateways Integration

Nucleon feeds can be integrated with various kinds of security tools.
From complicated SIEMs systems to FW,IDS,IPS and other gateways, Nucleon offers solutions to connect the feeds and integrate Nucleon Threat Intelligence in the organisation. Nucleon intelligence is already integrated and supported by many leading cyber security tools with native support.



Appliance Integration

Nucleon Appliance allows clients to install a box at their own network and start alerting or blocking threats automatically.
The appliance can act as active network component stopping threats or only monitor and alert.
The appliance can also communicate with other security tools and constantly update them about the security status.

Features of Nucleon's Threat Intelligence framework

Unlimited 24x7 access to secure REST API	Clients can access intelligence data using the most modern RESTful API available 24x7
JSON,CSV,STIX,CEF,LEEF Support.	Threat information can be passed as industry standards
Dynamic Active Threat Table (IPs, URLs, hashes)	Multiple IoC indicators
Virtual Appliance support	Install Threat Predictor on EC2 from AMI.
Threat Predictor appliance	Supports several configurations as Amazon,Docker,Physical and more.
Active Botnet Intelligence	Get Threat Intelligence from inside the botnets.
Real-time feed update	API is being updated real time, ability to broadcast alerts.
Access to context	Add context as what methods where used, which ports, where the attack came from and more.
Graphical Portal Access	Detailed graphical portal allows to manage and visualize threats on strategic and tactical level.
Suitable for SIEM	Supports many common SIEMS such as ArcSight,Qradar and more.
Suitable for Threat Intel Platform	Integrated support with systems such as MISP and others.
Advanced filtering & Targeted Intelligence	Get targeted intelligence tabout threats tailored for you.
Strategic Cyber Intelligence and Planning	Gain Strategic perspective about what is going out there and plan accordingly.
Tactical Planning and Intelligence	Implement Tactical Cyber Intelligence plans with a click of a button.
Technical support.	24x7 Support is available.
Analyst Support	Several analyst level support available.
Access to history	Detailed textual and graphical history and reports about indicators.

Technical Details

Connecting and using the API is simple, the Hash Life API expects each request to be authenticated as detailed below.
All the requests are done using RESTful API with POST request.

Authentication

Authentication requires 2 sets of credentials.
A basic authentication and POST parameters authentication.
The following table shows the POST parameters that are required in order to use the API.

Field Name	Type
clientID	string
usern	string

Optional POST request parameters:

Field Name	Type
reset	bool (1 or 0)
limit	bool

Hash Life API response

Each response is built with a summary and data lists. The data field is an array that holds the objects of the response.

Feed object properties

Field Name	Description	Value Type
status	bool	
timeStamp	string	
summary	array	
data	array	

Data object fields description

Name	Description	Value Type
associated_ip_list	List of IP addresses related to the hash indicator.	array
exiftool	Analysis of the malware, providing details such as what OS the file is running and file architecture.	Object
associated_hashes	List of hashes related to the specific indicator.	Array
md5	MD5 signature	string
sha1	SHA1 signature	string
sha256	SHA256 signature	string
associated_url_list	List of urls related to the indicator	Array
last_seen	Timestamp	string
history	Detailed history of the last attacks that the hash is related to. Each object holds many other details about the specific attack.	Array

use case of the Hash Life API

For security professionals, usually the data from the Hash Life API is being retrieved every several hours, and being stored in local database, such as MongoDB or Elastic Search. Nucleon framework provides scripts and tutorials that might be needed in order to quick start using the API in private environments. The data can be either used to search for specific indicators and alert when they appear or the data can be used along with other tools as part of security investigation.

Placing an appliance at the clients network, provide the client with the ability to analyse the data being gathered and have graphical representation of the intelligence on a world wide global scope or local regional scope..

Software Vendors Integration

Software and Hardware vendors that build products and wants to offer their clients additional security can integrate the Hash Life API inside their own products using a documented SDK that makes sure that the implementation process goes smooth and simple.
Leading software vendors are using Nucleon services to offer additional security to their clients, If you are interested in learning more about integrating threat intelligence in products, you are welcome to contact us.

CONCLUSION:

Threat Intelligence is no longer optional, Organisations that wants to ensure they are safe or Organisations which needs to get reliable details about indicators, finds Nucleon offering compelling as it allows them to reduce the efforts needed on collecting,validating and verifying intelligence related to specific indicators and allow them to focus on the important things.
Nucleon Threat Intelligence framework is flexible and simple to integrate, it can be integrated with existing security tools such as Firewalls and other gateways or it can be provided as an appliance that can utilise intelligence and block threats before they are able to breach the network.

Lux in tenebris

NUCLEON