Core Network Insight 6.4 Release Notes

In This Document:

Contact Core Security Support to coordinate an upgrade to Core Network Insight 6.4.

Email:support@CoreSecurity.com
Phone: 678-304-4485

About the Core Network Insight 6.4 Release

Core Network Insight 6.4 is the latest release in the Core Security product line. It includes enhancements like HAM (Host Account Mapping), which enables users to see which accounts are logging into which devices. For example, if user A's device just became infected and is seen logging into other devices they have never logged into, it must be addressed. Additionally, this release adds exploit and vulnerability context, a threat-hunting search for domains and operators, and the ability to kick off a workflow in ServiceNow.

New Features and Enhancements

Network Insight 6.4 includes these major features:

- **HAM (Host Account Mapping)** – Network Insight 6.4 includes HAM to give incident responders context around which users are logging into which devices. This combination of device behavior with user activity allows responders to quickly determine if an attacker is misusing credentials.

- **Threat Hunting Search** – Network Insight 6.4 includes a new threat hunting capability. Threat hunting allows searches for threat operators and different domain names to see if they exist in Core Labs database.

- **Exploitable Vulnerability Context** – Network Insight 6.4 includes the ability to add device vulnerability and exploitability context. A responder can search for infected or suspected devices that have common exploits or vulnerabilities across the entire organization to quickly see if an attacker is using an exploitable vulnerability to move laterally across your network.

- **ServiceNow Ticketing Integration -** Network Insight 6.4 now integrates with ServiceNow ITSM to kick off a workflow and take action. Responders can easily create a ticket from Network Insight manually based on infected or suspicious devices, or automatically based on user-defined criteria.

Core Network Insight 6.4 also includes these additional enhancements:

- Carbon Black integration and GUI improvements (Support for Carbon Black 6.x API and port)
- Upgrade pre-requisite "readiness" enhancements
- Improved IP to hostname resolution (HAM adds a 3rd and best method to resolve IP address to hostnames)
- Product reinstall option to keep or wipe ILO config
- Sensor to MC VPN performance improvements
- System messaging and disk usage performance improvements

Features in Detail

HAM (Host Account Mapping)

Network Insight 6.4 includes HAM to give incident responders context around which users are logging into which devices. This combination of device behavior with user activity allows responders to quickly determine if an attacker is misusing credentials.

HAM is a new module that integrates with Active Directory using an unprivileged account. It offers the following features:

1. A new and better way to get asset hostname resolution. This resolves an IP address to a hostname. IP addresses can often change (using DHCP). To track device/host behavior over time the computer hostname or hardware MAC address must be tracked. HAM offers a 3rd and superior method for hostname resolution, behind the 2 existing methods (reverse DNS and NetBIOS).

2. Even more important is the ability to log which users are logging into which devices. This is how we begin to infuse our identity expertise into our threat management tools. Identity has been one of the major areas lacking in security space. Verizon DBIR reports 81% of breaches in 2017 were due to weak or compromised credentials.

HAM is the most accurate IP to hostname resolution method and ensures that as a devices IP address changes over time, NI is able to track all suspicious behavior to that one asset by hostname.

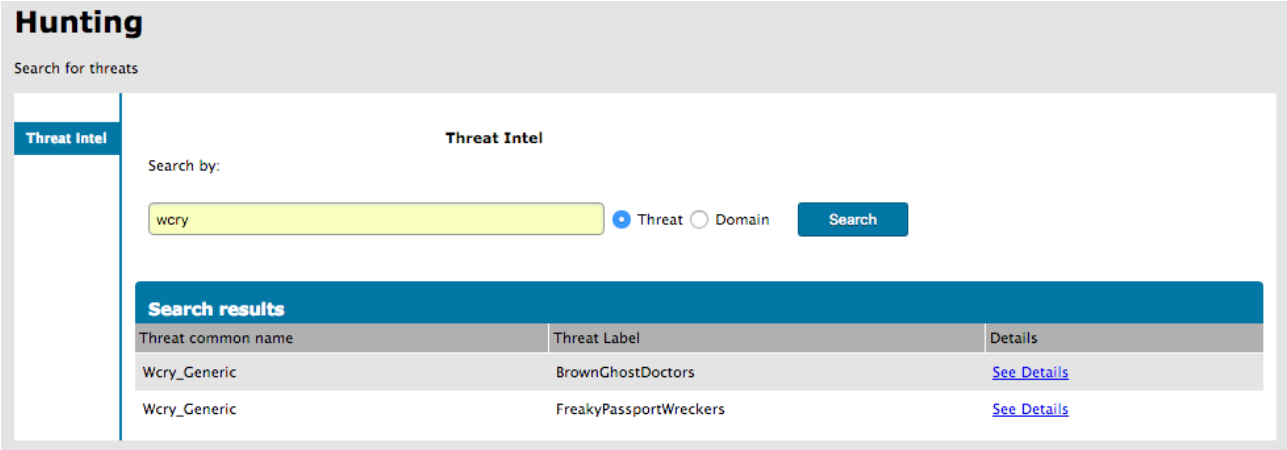
HAM connects the users to the suspicious and infected devices allowing a SOC analyst or an incident responder to understand which credentials might be compromised.

> Example- if a device is compromised by a threat actor/operator and then a user logs in to that device there is possible that those users' credentials are compromised. If that user account then logs into 5 new devices after logging into the compromised device, this could be an indication of compromised credentials being used by an attacker to move laterally through an organization.

Threat Hunting Search

Core Network Insight 6.4 includes a new threat hunting capability. Threat hunting is used to search for threat operators and different domain names to see if they exist in Core Labs database.

This gives responders the ability to search all of Core Security's threat intelligence and access to Core Labs threat operator intelligence to aid in investigations. In addition, responders can search for domain names, and 13.8 Billion PDNS records for malicious domains to aid in investigations.



Exploitable Vulnerability Context

Core Network Insight 6.4 includes the ability to add device vulnerability and exploitability context. A responder can search for infected or suspected devices with common exploits or vulnerabilities across the entire organization to quickly see if an attacker is using an exploitable vulnerability to move laterally across a network. Vulnerability Assessment scan results are required for import.

Note: Core Network Insight does not scan for vulnerabilities.

This gives additional rich context to determine if a device under attack has any exploitable vulnerabilities. This can help responders remediate a device, as well as see signs that an attacker might be using an exploitable vulnerability to move laterally inside a network.

> *Example*: If one device gets infected with vuln_xyz, then 4 other devices also become infected with vuln_xyz, then an attacker could be exploiting this vulnerability to pivot from one host to another. A responder can kick off a ticket to patch ALL devices that have vuln_xyz asap, before patching anything else to help stop an attack that might be underway.

ServiceNow Ticketing Integration

Core Network Insight 6.4 now integrates with ServiceNow ITSM to kick off a workflow and take action. Responders can easily create a ticket from Core Network Insight manually based on infected or suspicious devices, or automatically based on user-defined criteria.

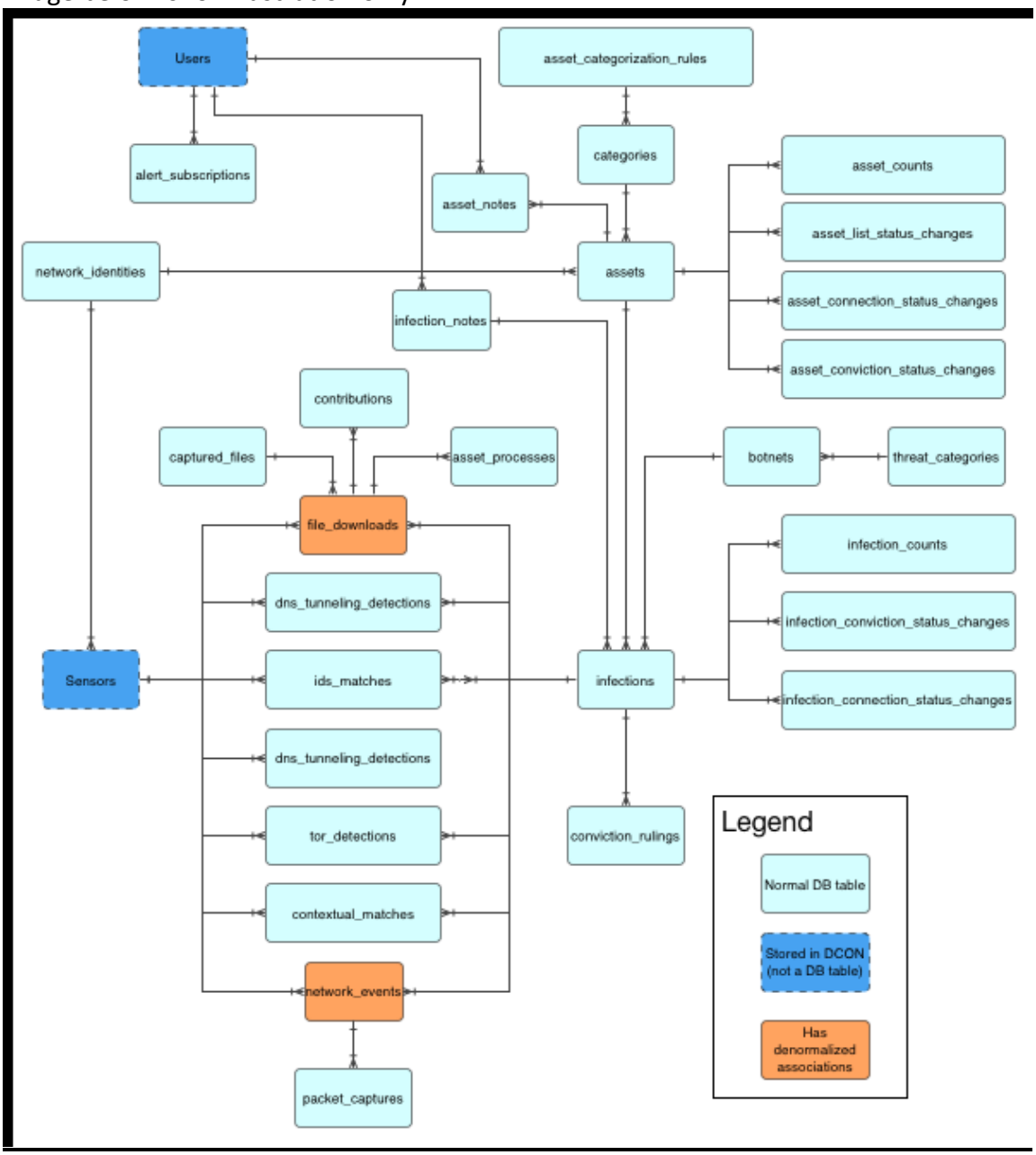
The ability to kick off a workflow to remediate an infected device, reduces response time.

If a responder is reviewing an asset in the Core Network Insight UI, they can click “Create Ticket” in the Action column on the asset screen. If ticket automation is enabled, tickets to remediate a device are dropped into a responder’s queue effectively reducing the dwell time of a compromised device.

Database Schema Changes

Once connected, the Customer database schema is accessible. The relationships between tables related to assets are tracked within the system. Customers can independently discover table-related data using relevant queries and a tool that is compatible with postgres.

Image below is for illustration only:



Product Improvements

Reference ID	Description
FS-6388	Tor evidence not part of the global counts
FS-6436	Check Point sending "::" as an asset
FS-6579	ArcSight Key Value Pair wrong for Destination Port
FS-6640	FSE packet loss calculated wrong
FS-6686	500 Error on CSV download of asset events
FS-6731	Transaction Profiler - Server IP is being marked as suspected asset instead of Client IP
FS-6759	Duplicated domains are being shown with Domain Fluxing profiler
FS-6929	UI: Diagnostics : Missing stats info
FS-7122	Transaction profiler evidence duplicated on multiple sensors
FS-7133	Sharp drop off of sensor evidence submissions
FS-7243	Sensor VPN performance issues
FS-7306	destination_port missing from Execution Profiler's "view execution details in Carbon Black" URL
FS-6800	Remove support for SSLv3 and TLSv1.0
FS-6801	Remove support for SSL/TLS compression

Known Issues

- Sensor to MC VPN now uses UDP and not TCP (Must ensure UDP port/access is enabled)
- Users who wish to utilize HTTP Open Access or Database Open Access must first log into the UI before their credentials are accepted for the Database or the HTTP Artifacts folder.
- STIX-formatted imports of custom threats only support exact IP matches, not ranges or CIDRs.
- When enabling the Syslog Receiver on a combo box, the box must be restarted before the receiver starts listening on interfaces.
- In Core Network Insight Diagnostics, under the "Requests" tab, the "HTTP Connections" count does not include file downloads.
- If a new user is created in the Core Network Insight web wizard before Threat Updates are finished downloading, Core Network Insight won't send a link to that user for them to assign a password to their account. The work around for this is to manually assign a password through System -> Users, or have the user manually click the reset password link on the login page.
- In rare cases, the total connection and file counts in the executive report may be underreported.
- Unpredictable behavior may result when utilizing the Bit9 and Carbon Black integration tabs at the same time.
- The configuration export includes only values that changed from the system default.

Available Hotfixes

No hotfixes are currently available

Installation / Upgrade

Contact Core Security Support to coordinate an upgrade to Core Network Insight 6.4
Email: support@CoreSecurity.com

Phone: 678-304-4485