Infocyte

PROOF OF CONCEPT (POC) GUIDE

Infocyte HUNT

How to orchestrate, execute, and review a successful HUNT Proof of Concept.

PURPOSE

Expectations, criteria, and processes entailed in an Infocyte proof of concept (POC) to ensure a full and successful evaluation of our threat hunting platform.

ASSET DISCOVERY + THREAT HUNTING + VULNERABILITIES + INCIDENT RESPONSE

SCOPING

Before the POC begins, the Infocyte team will meet with you to develop an understanding of the overall process as well as establish our criteria for a successful engagement. In an appendix to this document you may find a sample table with example criteria for a successful POC.

During our initial meeting, we'll also gather relevant details about your network, assets, data, and environment. Unless otherwise specified, an Infocyte HUNT POC will include forensic scanning of up to 100 nodes (i.e. unique IP addresses, endpoints, and/or servers).

Understanding the makeup and design of your network environment is key to determining which assets need to be scanned/inspected during our POC. In some cases, scanning production or otherwise critical environments is not a requirement of the POC. In others, these high-value critical assets are exactly what we need to scan.

Another consideration is your network's setup and architecture. The HUNT server should be on-premise and requires a network connection from our server to your targeted endpoints/nodes. Our installation guide details network setup and Group Policy Object (GPO) rules for HUNT to deliver the survey to your endpoints.

Please contact your sales representative or email support@infocyte.com if you have any questions related to setting up your HUNT server.

HUNT INSTALLATION AND SETUP CHECKLIST:

1. Activated copy of Windows Server 2012 R2 or Server 2016 that meets the following hardware (virtual or otherwise) requirements:
    - 4-cores available
    - 16GB of RAM available
    - 500 GB+ secondary storage
2. Firewall rules established for communication from HUNT server to endpoints and back
    - Endpoints to HUNT server via 443 (HTTPS)
    - HUNT server to Linux endpoints via 22 (SSH)
    - HUNT server to Windows endpoints via 135 (WMI), 139 (Remote Scheduled Tasks), 445 (SMB), 5986 (Powershell Remoting)
3. Windows Defender uninstalled on HUNT server (not on endpoints)
    - Infocyte HUNT is designed to safely inspect malware, so having Windows Defender on the HUNT server can disrupt HUNT from performing its analysis
4. HUNT binaries whitelisted on endpoint protection tools
    - A list of hashes of our executables are available in the HUNT Installation Guide (Appendix A)

Operating systems Infocyte HUNT currently supports:

- Windows XP SP3 - Windows Server 2016
- Linux, post 2009
    - Debian
    - Ubuntu
    - Redhat
    - Fedora
    - CentOS
    - OpenSUSE Server

FYI: Workstations with a high volume of human interaction are ideal targets because they are the most likely to have malware. We can help you choose which of your hosts will demonstrate the most value during our POC.

Note: HUNT requires WMI + SMB, Remote Scheduled Tasks + SMB, or Powershell Remoting + SMB.

We prefer WMI + SMB for delivering the dissolvable survey.

5. Administrative credentials for endpoints
    - Please have credentials available to authenticate on your endpoints and have the correct administrative privileges
    - For Windows, a service account with admin privileges
    - For Linux, we require an account that is a part of the sudo group
6. Three (3) endpoints you want to target
    - After installing HUNT, Infocyte may provide training
    - During training, we'll scan your endpoints and review the results so you understand how to use Infocyte HUNT like a pro

According to a recent study by the Aberdeen Group, organizations that limit their dwell time to 7 days realize a reduction in business impact of a breach by 77%. Further reducing dwell time to 1 day delivers a reduction in business impact of 96%.

COMMUNICATION DURING POC

As the POC progresses, we'll communicate regularly to ensure a successful POC and streamlined resolution of any obstacles or issues. If any issues arise, we're here to help and support is only a call or click away.

During the POC, you can use the full suite of features available within our threat hunting platform, Infocyte HUNT, for the selected nodes in your environment.

HUNT'S CORE FEATURES (TESTED DURING THE POC):

1. Asset Discovery

HUNT performs asset discovery using IP addresses, hostnames, CIDR blocks, and domains to query your environment. This is especially helpful in environments where virtual hosts are heavily used.

Once a query is created, HUNT looks for live hosts in your environment and checks if specific ports are available (SSH, WMI, RST, PSRemote, SMB). Then, HUNT tests if the supplied credentials can be authenticated on your endpoints.

2. Threat Hunting & Intelligence

Once hosts are discovered, HUNT can scan your environment. In the Analyze view, you'll see the hosts, processes, modules, drivers, memory injections, hooks, artifacts, accounts, scripts, and connections discovered during the HUNT scan.

The Analyze view also includes information collected from your hosts, enriched with data from our cloud server, including our Incyte™ threat intelligence engine and static analysis tools.

Infocyte HUNT provides multiple data points, enabling you to understand whether or not an object in your environment is malicious.

3. Vulnerabilities & Management

During the scanning process, HUNT looks at your installed applications and compares them to a CVE database (NIST's NVD).

The CVE advisories are displayed in the Applications section of the Analyze view. These scores do not impact the general threat scores of items found during the HUNT scan. Rather, the CVE advisories are designed to help you decide where to focus your time updating software in your environment to prevent vulnerability exploitation.

4. Reporting

- Generate reports featuring malicious items found during the scan.
- View all hosts scanned, all compromised accounts, and all malicious items.
- Reports can be downloaded as PDFs via the Print PDF button in the UI.

There are two main reasons why scans may fail:

1. There is an endpoint protection tool preventing the HUNT scan from executing.

   Solution: Whitelist the HUNT survey (the binary that scans your endpoints and sends data back to the HUNT server).

2. There is a firewall rule in place preventing communication from the endpoint to the HUNT server over port 443.

   Solution: Adjust your firewall rules to allow traffic over port 443 to the HUNT server.

POC CONCLUSION

A POC typically concludes 14 days after Infocyte HUNT is fully deployed in your environment. Upon completion, we'll review our success criteria to ensure the POC was completed to agreed upon standards.

Your HUNT license keys will expire at the end of the POC period, so it is important to facilitate this review prior to license expiration. In the unlikely event we did not meet the established success criteria, or extenuating circumstances prevented a full evaluation of HUNT, licensing may be extended to achieve a more complete and/or successful POC.

If further technical discussions about our threat hunting platform are necessary, bringing in the right resources to have that conversation is key. We also aim to gain general feedback from you upon completion to identify opportunities for improvement of our product, processes, workflows, and overall customer/user experience.

Need help?

(844) 463-6298
support@infocyte.com

Infocyte

3801 N. Capital of Texas Hwy.
Suite D-120
Austin, TX 78746

(844) 463-6298
sales@infocyte.com
www.infocyte.com

THE INFOCYTE HUNT ADVANTAGE

FORENSIC DEPTH

- Detects post-compromise indicators that antivirus and event monitoring tools (EDR) are prone to miss
- Unique, scalable volatile memory analysis finds all fileless implants
- Autostart and Forensic Artifact analysis finds all threats laying dormant

BECOME THE HUNTER

- Automates & integrates the threat hunting process into your risk and vulnerability management process
- Continuously hunt or perform periodic assessements to mitigate risk
- Go beyond vulnerabilities and identify any threats that may have exploited them

EASY TO IMPLEMENT

- Agentless and lightweight
- Survey thousands of endpoints simultaneously vs. 'single-host' forensic tool alternatives.
- Download and deploy HUNT within a day

FAST ROI

- "Zero to Hero" in hours to days — not months or years
- Reduces dwell time to limit breach damage and costs
- Ensures you are prepared for the next one

APPENDIX A: TECHNICAL POC SUCCESS

COMPONENT	DESCRIPTION	PASS / FAIL
Installation	• Was HUNT installed successfully? • Did we complete HUNT configuration, scanning of one host, and were we able to view the Analyze details within a reasonable timeframe? • Are we able to enumerate machines/endpoints within your network? • Do we have the right administrator credentials to authenticate on the machines/endpoints and scan? • Are we finding the machines within your network?	
Interface	• Are users able to navigate our interface to find how to build queries, scan hosts, and view results? • Are users able to find where to enable integrations and manage user accounts? • Are users able to find where to edit credentials and queries? • Are users able to create new target lists and populate them in the interface?	
Analysis	• Are scans succeeding? If not, are we able to identify why they are failing and fix the issue(s)? • Are the scan results providing comprehensive results (including what software is running) on the endpoints at the time of scan? • Are we providing enough data to reasonably showcase that objects are malicious or benign? • Are we finding all of the running processes?	
Use Cases	• Do we fit your particular use case(s) and add value to your organization?	
Alert Validation	• Can users integrate our tool within their SIEM of choice? • Can users access our API endpoints via the explorer? • Can users isolate an endpoint to scan it to confirm alerts?	
Threat Hunting	• Can users schedule scans on a target list? • Can users receive results over time with the HUNT scans? • Can users view all scans, specific target lists, and/or individual scans? • Can users create reports based on the findings?	
Compromise Assessments (Partners)	• Can users scan a target network and receive results? • Can users access our Compromise Assessment kit and understand it? • Do users understand the process of a Compromise Assessment and how to generate/interpret reports based on what they find? • Can users leave comments on the objects in memory and include those comments in their reports?	

APPENDIX A: BUSINESS POC SUCCESS

COMPONENT	DESCRIPTION	PASS / FAIL
Risk Mitigation, Breach/Attacker Dwell Time	• How much did HUNT reduce attack/malware dwell time? • How long were the identified threats living in your environment prior to HUNT finding them?	
Employee Productivity	• Did HUNT amplify your employees' ability to detect breaches? • Did HUNT effectively help you scale your threat hunting operations to investigate multiple endpoints at a time and pulling all results back into a singular view (as opposed to hunting one machine at a time)?	
Cost & ROI	• Did HUNT reduce the amount of time and resources you are currently dedicating to threat hunting activities? • If so, what measurable impact did HUNT provide? (i.e. hours, dollars, and/or both) • What is the ROI associated with a HUNT subscription vs. the cost of a potential breach for your organization?	
Brand Reputation	• Did HUNT enable you to identify threats that could lead to loss of consumer confidence, customer attrition, and/or that might have a negative impact on your company/brand?	