Infocyte®

Threat Hunting

Hunt Advanced Threats with Infocyte

Security Operations Centre Top Concerns

A recent Report on Threat Hunting published by Crowd Research Partners[1] indicated while 75% of respondents believe that threat hunting is of major importance, and 42% consider it a top priority, there are specific concerns that stand out. Based on survey findings, the top two challenges facing SOCs today are the:

- Detection of Advanced Threats (hidden, unknown and emerging)
- Lack of expert security staff to assist with threat mitigation

Secondary, yet significant, concerns were:

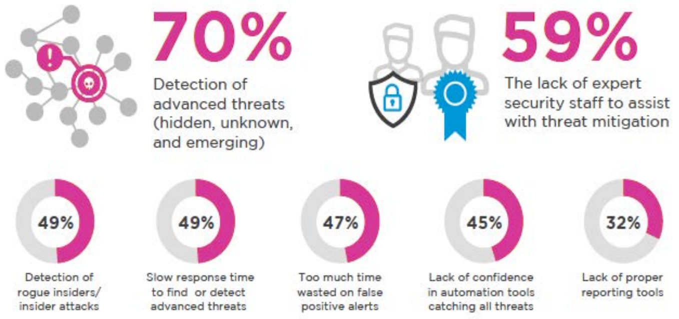
- Detection of rogue insiders/insider attacks
- Slow response time to find or detect advanced threats
- Too much time wasted on false positive alerts
- Lack of confidence in automation tools catching all threats
- Lack of proper reporting tools

So threat hunting is top of mind for SOCs, and rightfully so considering the constant stream of malware attacks hitting every industry - a trend that seems set to continue.

We know that malware will breach defences, as surely as day follows night. The survey found that 44% of threats go undetected by automated security tools. Yet the survey also showed that security industry professionals do not have confidence in their abilities to detect advanced threats, nor in their in-house expertise level to mitigate these threats.

This is where Infocyte HUNT steps in and stands up. Infocyte HUNT addresses every one of the top seven identified concerns plaguing SOCs today.

2017 THREAT HUNTING REPORT



Infocyte HUNT is the only true malware hunt technology currently on the market. The solution is not an EDR nor an SI (Security Intelligence) tool - it is a post-compromise detection tool.

INFOCYTE CHECKS EVERY BOX

Infocyte HUNT is the only true malware hunt technology on the market today. Infocyte's unique solution addresses every one of the seven top concerns SOCs have today.

- Scans detect malware, whether it is active or dormant, known or unknown
- Even junior IT admins and security professionals can successfully hunt malware, backed up by Infocyte's lab
- Can detect unauthorized or rogue software deployed by trusted insiders
- Scans can be run as frequently as desired
- Does not raise false positives; software that is identified as suspicious needs to be examined
- Delivers definitive proof if you have been breached
- Delivers reports that are easy to read and action

Key Features of Threat Hunting

The most appealing features of threat hunting platforms are the forensics detail, automated and packaged analytics and searchability.

Infocyte HUNT delivers all three.

Many solutions purport to hunt threats, however they are defensive tools, that are designed to first protect an enterprise from malware.

As the survey results show - with a rate of 44% of threats overcoming defences undetected - these defensive tools cannot be relied upon to find the very threats that have breached them.

Infocyte HUNT is built to hunt malware - period. It is a proactive tool that presumes compromise has occurred, and sets out to track down the malware.

The Infocyte HUNT Methodology

Infocyte's methodology combines agentless scans with File Intelligence Services and our Digital Forensic Analytics Services into statistical models that determine the risk profile of endpoints.

Infocyte HUNT scans:

- Validate everything currently running or scheduled to run on endpoints
- Analyze each system’s volatile memory to discover signs of manipulation or hidden processes using patent-pending techniques
- Are agentless and do not require software to be pre-installed
- Typically take just minutes to complete
- Do not rely on a potentially compromised host operating system to deliver results

Why the Resistance?

While the risks of malware become increasingly clear, and are the cause of great concern for SOCs, we know that the majority of organizations do not currently use a threat hunting platform. The need is recognized, yet resistance remains.

When the true costs of hacks are assessed, it becomes clear that budget should not be an issue. Indeed, 75% of survey respondents would like to invest in a threat hunting solution, and 65% did not cite lack of budget as the main reason for the decision not to purchase.

It appears that the perceived lack of training and proper reporting tools, along with platform fatigue could be some of the reasons.

Choose Wisely

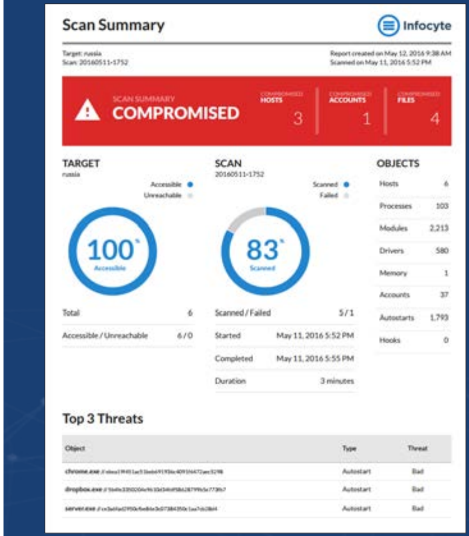
Infocyte HUNT is lightweight and affordable, does not require users to have forensic expertise, delivers easily digestible reports and most importantly, hunts down malware that has breached defences and is persisting undetected.

Invest in a solution that delivers on its promise, and does what it claims.

Benefits

- Definitively answers if you have been breached
- Advanced detection combines forensic automation and patent-pending memory analysis
- Fast - Infocyte HUNT scans upwards of 25,000 endpoints per day on a single server deployment
- No training required to effectively use Infocyte HUNT
- Final report provides collected intelligence and drills down into identified issues to allow your team to take action with swift remediation and incident response

Start Hunting. Contact us to learn how.



Scan Summary

Target: russia
Scan: 20160511-1752

Report created on May 12, 2016 9:38 AM
Scanned on May 11, 2016 5:52 PM

SCAN SUMMARY
COMPROMISED

COMPROMISED HOSTS	COMPROMISED ACCOUNTS	COMPROMISED FILES
3	1	4

TARGET
russia

Total	6
Accessible / Unreachable	6 / 0

SCAN
20160511-1752

Scanned / Failed	5 / 1
Started	May 11, 2016 5:52 PM
Completed	May 11, 2016 5:55 PM
Duration	3 minutes

OBJECTS

Hosts	6
Processes	103
Modules	2,213
Drivers	580
Memory	1
Accounts	37
Autostarts	1,793
Hooks	0

Top 3 Threats

Object	Type	Threat
chrome.exe // [illegible]	Autostart	Bad
dropbox.exe // [illegible]	Autostart	Bad
server.exe // [illegible]	Autostart	Bad

Infocyte HUNT is lightweight and affordable, does not require users to have forensic expertise, and delivers easily digestible reports.

Infocyte®

CORPORATE HEADQUARTERS

110 E. Houston St. Floor 6
San Antonio, TX 78205
+ 1.844.INFOCYTE (844.463.6298)
sales@infocyte.com

www.infocyte.com
@InfocyteInc

[1] 2017 Threat Hunting Report, Crowd Research Partners, images and contents published with permission.