SANS

BLUE TEAM

SUMMIT & TRAINING

Live Online

Summit: September 9–10, 2021

Adversary Simulation: Close the Gaps in Your Security Posture

Don Murdoch, GSE #99, MBA, MSISE

Director, Security and Risk Organization

RSA Inc., NetWitnessDivision

Personal Twitter: @BlueTeamHB

Don Murdoch Intro … or $whoami

- 25+ years in IT, 17+ in Information Security
- Digital Combat training in the Wild, Wild, West of Academic Computing
  - Only looked back once for a brief Strategy and Planning / Enterprise Architecture respite
  - Commercial, defense, non profit, ran a Cyber Range , …
- SANS Instructor, Author, Blue Team Handbook Author
- Director, SRO for RSA’s NetWitness Business Unit

Where do you start? What is your Value Chain?

The Blue Team defends it while the Red Team emulates the attacker who tries every day...

- A value chain is “a set of activities that a firm operating in a specific industry performs in order to deliver a valuable product (i.e., good and/or service) for the market.” – M. Porter, 1985.
- WHY do we, as infosec, care?
  - Provides ready made **catalog** of exposure points
  - Roadmap to the valuable **data**
  - Ensures you are business **relevant**
  - Advises what systems you absolutely cannot **adversely** affect
- Consult:
  - Business Continuity / Disaster Recovery Planning team should know all of the details you need in priority order

The Security Architecture Protects the Value Chain

Think Red to find the threats, Act Blue to design and test defense

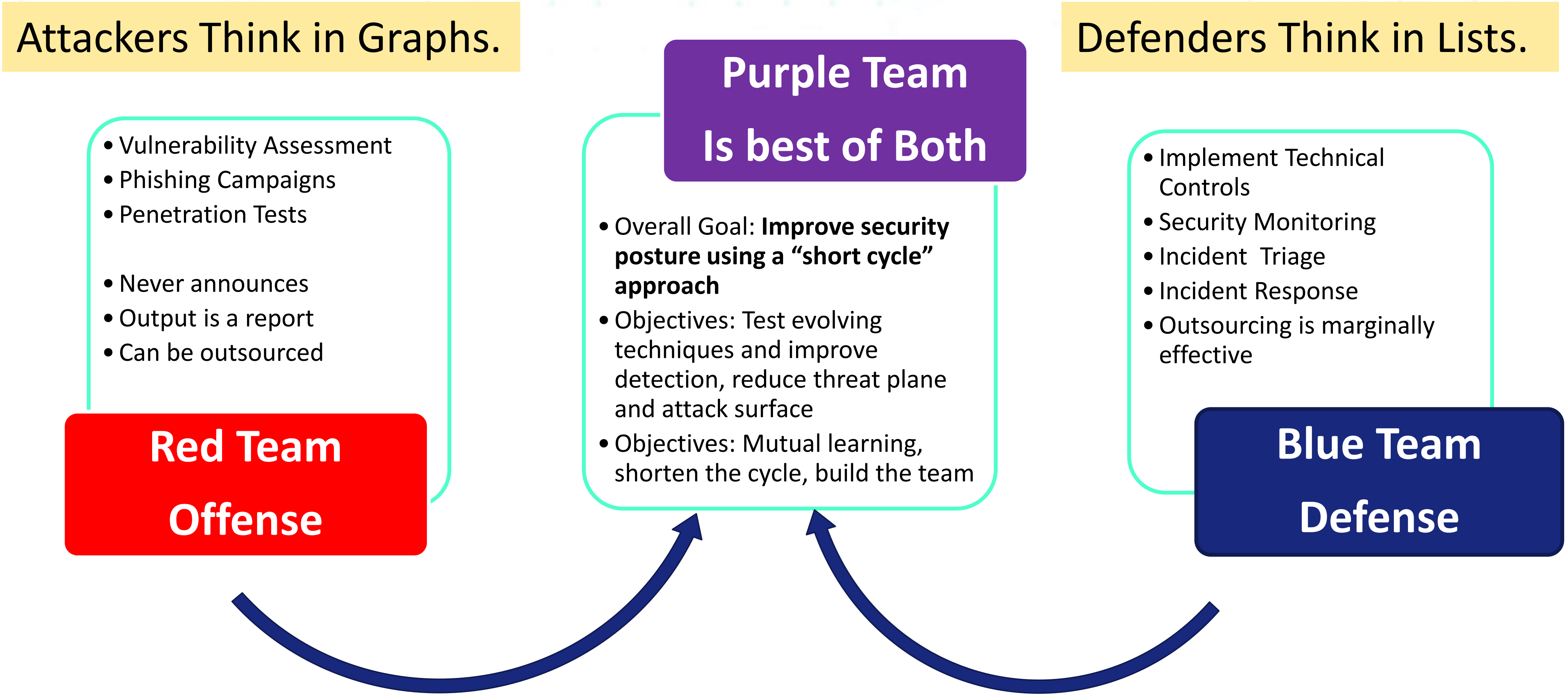
People and Process

- Security awareness
- Change Management
- Push Security Left (DevSecOps)
- Role Based Access control
- Compensating controls
- Third Party Risk Assessment
- . . .

Technology

- Web Proxy, DNS protection
- Endpoint detection and Response
- TLS Break and Inspect
- Application aware Firewall
- Authenticated vulnerability scans
- Network Segregation
- Cloud systems
- . . .

Historically: Organizations performed security assessment in isolation. Today we Integrate



Attackers Think in Graphs.

Defenders Think in Lists.

- Vulnerability Assessment
- Phishing Campaigns
- Penetration Tests

- Never announces
- Output is a report
- Can be outsourced

Red Team

Offense

Purple Team

Is best of Both

- Overall Goal: **Improve security posture using a "short cycle" approach**
- Objectives: Test evolving techniques and improve detection, reduce threat plane and attack surface
- Objectives: Mutual learning, shorten the cycle, build the team

- Implement Technical Controls
- Security Monitoring
- Incident Triage
- Incident Response
- Outsourcing is marginally effective

Blue Team

Defense

Key Definitions From an Industry Expert

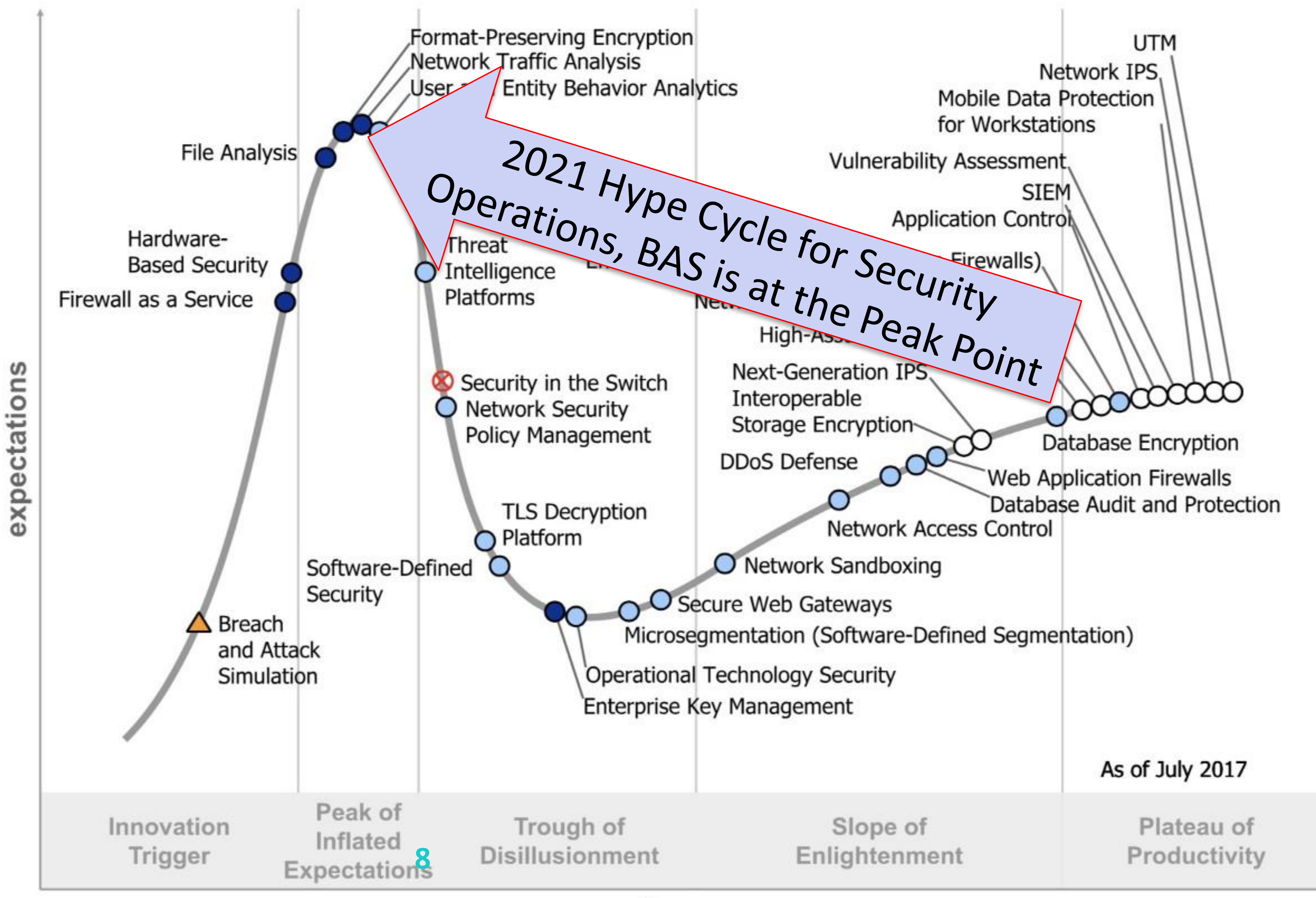
Jake Williams, Rendition InfoSec

- **Adversary emulation** and **purple teaming** are fundamentally different activities.
  - In adversary emulation, a red team member conducts an assessment using only the techniques and tool types used by a specific adversary.
  - This differs from the more generic "threat emulation" red team where assessors use any tool or technique available to them.
- In **purple teaming**, the red team works hand in hand with the blue team to validate that their actions are detected.
  - If a particular action is not detected by the blue team, red team should repeat the action after the blue team adjusts instrumentation. Then lather, rinse, repeat.
- Therefore:
  - Think Red, Test Blue, as if you were simultaneously attacking and defending the network. Skill mastery through practice. Aim to improve blue using well structured attack methodology.
  - Testing network resilience against an advanced attacker in a disciplined and controlled manner

Origin Story: BAS is Related: But not a Pure Play AdSim Offering

Breach and Attack Simulation and its position on the Gartner Hype Cycle

Figure 1. Hype Cycle for Threat-Facing Technologies, 2017



2021 Hype Cycle for Security Operations, BAS is at the Peak Point

Adversary Simulation Needs a Plan

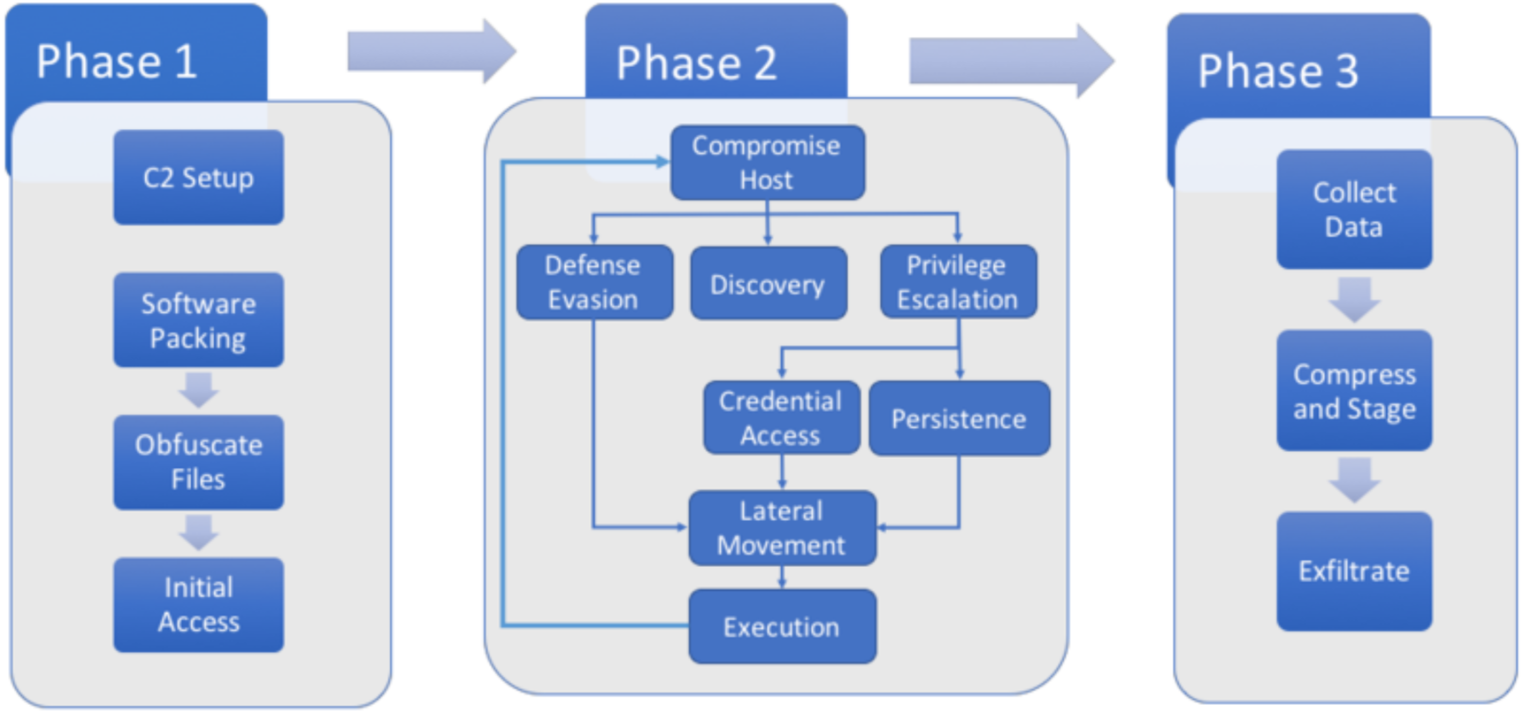
- Event: Your outline must have a purpose
  - Learning outcome. Think Knowledge, Skill, and Abilities (KSA’s).
  - Title, Scenario Objectives, Outline, Control testing, and Written Outcomes
  - Devise objective event scoring vehicle
    - Did the red team **perform all 20 steps**, in order, and get expected results?
    - How did the red team **overcome** an issue?
    - How long did the blue team take to detect? React? Respond? Contain? Activate the IRP?
- Simulation **program** needs to include:
  - Initial KSA assessment, entry points, and progression model
  - Fearless people, process, and technology assessment. Start small (Elephant theory)
  - Time commitments outlined tie into the organization Individual Development Plan (IDP)
  - Charge code(s):
    - Professional educational development with a scenario costs between 23 to 143 hours per hour
    - Utilize as many reusable resources as you can (more on that later....)

How and Where do you start to protect the value chain?

- Learn the MITRE ATT&CK Framework. Start with the APT3 Emulation Plan

Prework:

- Gain internal Mgmt.
- Red / Blue support
- Instrument
- Plan X3!
- Start small
- Understand staff impact



Approved for Public Release; Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved MITRE

Post Event

- Activate the lessons learned from the IRP
- Improve detection
- Repeat

Exercise every aspect of your technical and incident security apparatus.

Source: The MITRE Corporation: https://attack.mitre.org/resources/adversary-emulation-plans/

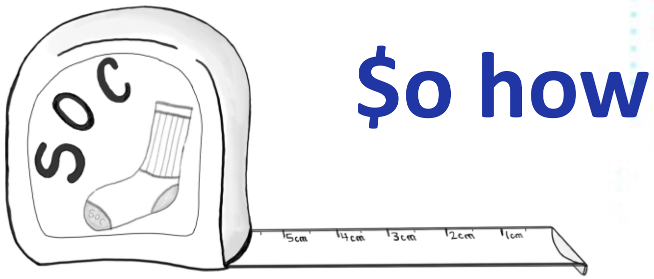
Gaining Support for Adversary Simulation

- Maximizes the $ecurity $pend
  - Well structured event should exercise most of the security and technology stack
  - Stakeholders are brought together
- Ensures effectiveness of procedural, technical, and operational controls
  - Are toolsets working, current, and configured well?
  - Reduce reaction time, cross training, career variety
- Find errors, weaknesses before “they” do, especially if “they” are an insider
- MITRE ATT&CK provides a solid framework
- Create documented “audit support artifacts”: Go the extra 5-7%
- Internal training and process improves staff skills
- Simulating TTP’s can be difficult

$o you want to run AdSim project, eh?

- Define roles
  - System, scenario, Red/White/Blue
  - Willing Partner(s)
- Define Use Cases -> ATT&CK
  - What skill do you need to develop?
  - Tool to test, validate, retire?
  - Rerun a prior red / pentest?
  - Proof of technical controls, auditing in place, policy/compliance?
- Outcomes
  - How will you use the UC finding?
  - BAS will reveal risk, blind spots
  - Establish cadence

- Guidance
  - Determine where your program needs help/support
  - SWOT analysis of the Sec Arch
    - identify strengths, weaknesses, opportunities, and threats
  - Refer to MITRE ATT&CK
  - Isolated lab – build a DetectionLab test bed, and add Sec Onion w/ a commercial rule set
  - Deploy “capability”, let it simmer
  - Only whitelist if you must



$o how will you mea$ure your project $ucce$$?

“What cannot be measured, cannot be managed.” - W. Edwards Deming.	“Not everything that counts can be counted, and not everything that can be counted counts.”’ - William Bruce Cameron

- Resources
  - Don Murdoch, “Blue Team Handbook: SOC, SIEM, and Threat Hunting”
  - Carson Zimmerman, “Measure Yo Bad Self” @ SANS SOC Summit 2018 https://www.sans.org/summit-archives/file/summit-archive-1532960745.pdf
  - Pragmatic Security Metrics, W. Krag Brotby and Gary Hinson

BTHb:SOCTH: Metrics Adapted to Adversary Simulation

- Time to sweep the enterprise (Test Net)
- MTT Close an alarm by Close Category
- MTT Forward an alarm up Tier
- MTT Open a formal Incident
- MTT Implement a use case
- # of Events Received / Analyzed in scope for a given exercise
- # of Alarms by Severity in scope for the given exercise
- ATT&CK Coverage by Exercise

- Impact and Cost per incident – trainees can be asked to assess the impact
- MTT to Detect a Security Incident
- MTT for Detect to Contain
- MTT to expel an intruder
- Incidents opened and closed
- Avoidability of an Incident
- Thoroughness of eradication practices
- MTT Notify Principle, System Owner, or Custodian

Key Timeline Measures and Event Reconstruction

- Mean Time To Decision (MTTD)
  - Is the observable event True or False?
- Mean Time to Compromise (MTTC)
  - This starts counting from the minute that the Red Team initiated the attack to the moment that they were able to successfully compromise the target
- Mean Time to Privilege Escalation (MTTP)
  - This starts at the same point as the previous metric, but goes all the way to full compromise, which is the moment that the Red Team has administrative/elevated privilege on the target

Prerequisites

- Central Logging
  - No “coffee break SIEM’s here”
- Endpoint visibility
  - Minimum Standard: Windows sysmon coupled with WEC/WEF
- Network device logs
  - Carefully instrumented Zeek, NIDS, Internal switch, Perimeter NIDS
- Person Power
  - Natural curiosity, patience, ability to question oneself, low ego
  - Attention to Detail – John Hubbard's best blue teamer is a librarian!
  - Solid IT background very helpful

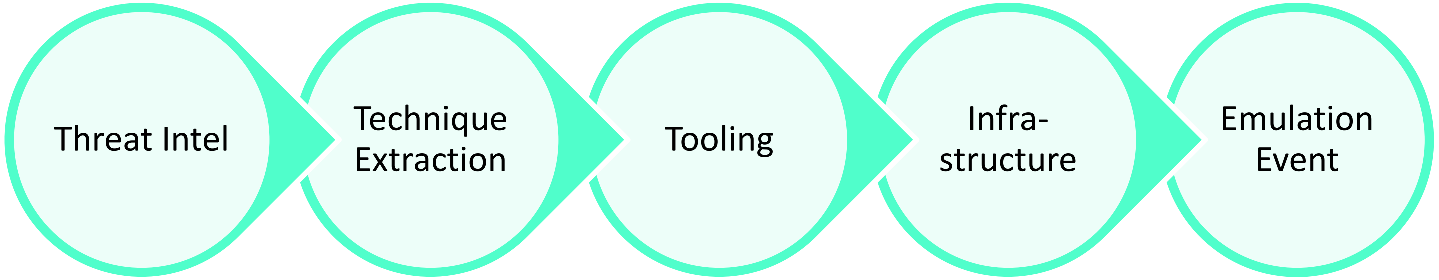
Which SOC Security Service will you test?

From BlueTeam Handbook:SOC, SIEM, Threat Hunting

Reactive Services	**Proactive Services**
Monitor Security Posture (Alerts)	Network Security Monitoring
Command Function (IR/Analysis)	Threat Hunting
Initiate & Manage Incident Response	Platform Health Monitoring & Support
Vulnerability Management	Cyber Threat Intel
Forensics/eDiscovery	Threat Intel Integration
Reporting	
Malware Analysis	**Other Services**
Intrusion Detection	Policy Procedure Support
Audit/Assessment	Internal Training and Support
Notification Refinement	

As the Program Matures, Maximize Each Event and Team Performance

- Utilize industry specific
  - Threat intelligence
  - Exercise Adversary Group patterns (https://attack.mitre.org/groups/)
- Map effectiveness of technique against MITRE ATT&CK



- Acquisition
- Research
- Vendor Intel
- OTX
- Threat Connect
- ....

- Technique
- Analyze M.O.
- JPCert Common Tools Pattern

- Develop
- Test

- C2
- Deployment
- Phish

- Launch
- Monitor
- Test
- Remove
- Operational Window

Candidates for your Tool Inventory

- Nearly no cost (OpEx only)
  - ***APT Simulator, MITRE Caldera***
  - Red Team Automation (RTA)
  - alphasc flightsim
  - uber-common/metta (endpoint)
  - DumpsterFire Toolset
  - Red Canary Atomic Red Team
  - Invoke-UserSimulator PS script
  - OSquery, ELK, Security Onion
- Low Cost
  - ***BT3,*** Cobalt Strike
  - Office 365 Attack Sim
  - Silent Break Slingshot
- Not so low cost: Scythe (CapEx)

- Build Environments for V2V, P2V staging (OpEx)
  - DetectionLab
    - AD, Splunk, Clients, Caldera, OSQuery
  - Cliffe SecGen
  - AutoLab
  - TechNet AutomatedLab
- People really are the best asset in this game

- Breach and Attack Tools really aren’t in this space because they are for continuous posture assessment
  - Cymulate, attack-IQ, SafeBreach, etc.

FOSS Compared by PenTestIT

TACTIC NAME	CALDERA	METTA	APTSIMULATOR	RED TEAM AUTOMATION	INFECTION MONKEY	ATOMIC RED TEAM
Initial Access	No	No	No	No	Yes	Yes
Execution	Yes	Yes	Yes	Yes	Yes	Yes
Persistence	Yes	Yes	Yes	Yes	No	Yes
Privilege Escalation	Yes	Yes	No	Yes	No	Yes
Defense Evasion	Yes	Yes	Yes	Yes	No	Yes
Credential Access	Yes	Yes	Yes	Yes	Yes	Yes
Discovery	Yes	Yes	Yes	Yes	Yes	Yes
Lateral Movement	Yes	Yes	No	Yes	Yes	Yes
Collection	No	Yes	Yes	No	No	Yes
Exfiltration	Yes	Yes	No	No	No	Yes
Command & Control	No	Yes	No	Yes	Yes	Yes

Game Day: Make Sure you have Air Cover!

Red Team

- **Rehearsed**, Run your steps
- Willing **partner**
- Record Results with timeline events

Green Team

- Active listening / observing
- Protects integrity of event
- Grades both teams and produces outcome briefing

Blue Team

- (Un) announced?
- Normal Monitoring processes
- Detection Event (we hope!)
- Be aware of observer bias, Hawthorne Effect
- Avoid IR Command being tipped off for best experience
- Writes incident report

After Action Reporting with Info Exchange

- Have an objective grading criteria
  - Write your own discovery timeline
- Request each participant or team list observation in writing
  - Put each person’s observations up on the screen
  - Open discussion promotes “What they said” responses
- IR can look like a tree
  - Many branches – encourage different approaches
- IR skills will develop over time
  - Build up a KB!

Incident Response Report

- Incident Response is a team sport
  - Document as you go, timestamped screen shots really help
  - IR Template is a professional learning experience (PICERL)
- During After Action Review
  - Leverage DevOps: Culture, Automation, Lean, Measurement, and Sharing
  - Everybody is asked to contribute, talk through and take notes by reviewing the IR Doc and Executive Summary
  - Emphasize on Timeline Reconstruction

Success Story: Impact Analysis Operations

Ref: Farzan Karimi Electronic Arts, PenTestMag 09/19

- Most often when a Cyber Incident is *declared*
  - Red team function stops to ensure deconfliction while Blue checks technical solutions and the IR lead coordinates business process
- Instead, bring Red in as a core contributor
  - Emulate the live attacker for controlled assessment impact
  - Evaluate for potential reach based on the attack path
  - IRL: Red scanned, found a weakness, Blue coordinated an ACL fix, and … within the hour the Adversary was attempting the very same thing
- Red
  - Highly skilled, think like the attacker, well armed with attack tools

Takeaways, Actions, and Next Steps

- 30 days
  - Identify your Value Chain
  - Perform a threat analysis which should inform your simulation plan
- 60 Day
  - Build out enough of an environment to stage and test both Red/Blue tooling
  - Plan each event, rehearse the steps, and practice for repeatability, air cover
- Every 90 Days is Game Day!
  - Run your simulation, observe blue team response, grade both teams against respective plan and operational capabilities, processes
- Remember: You Move the Needle when you focus in on making measured improvement in every engagement

BT3: Example of an Inexpensive Tool

Following slides are one of two possible demos. Really depends on which works better given the target 35 minute time limit.

Option One: Run a variety of end user workstation tools, see what you can see.

Option Two: Use a low cost tool that behaves like a modern adversary – BT3 – and a well known FOSS detection platform

Integrate an Open Source / Inexpensive Option – BT3

BT3 – Encryptio.IO

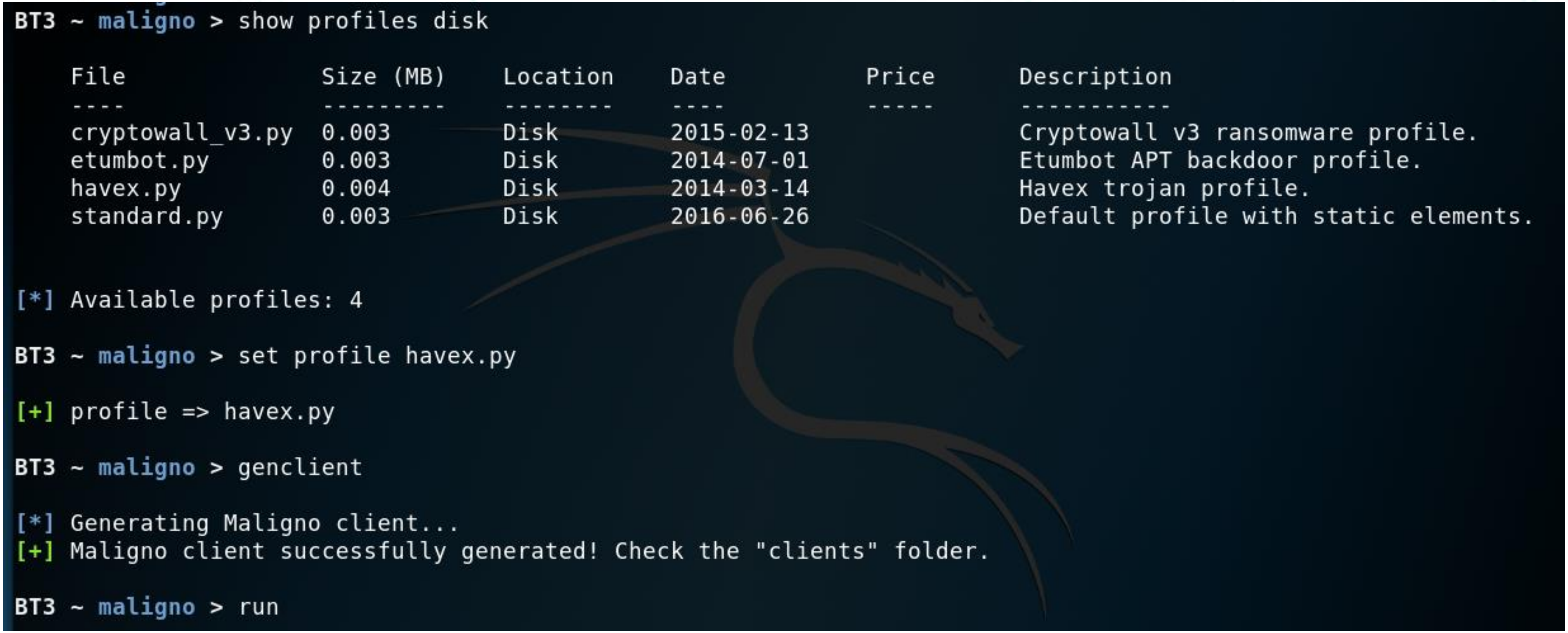
Several no cost modules in each category

BT3 - https://www.bt3.no/

- Easy implementation
  - Get Kali Linux, install BT3, register for an API key
  - Leverages Maligno – client/server, simulates C2, 4 examples free, others
  - Includes pcapteller for packet capture replay
  - Has files that pass md5sum analysis for malware samples (hash collisions)
  - Download agents, pcaps, and run
- Very low risk – White team is in control of the VMs and script code
  - Can install script code, drop off, we know where the bits go
- Inexpensive content update subscription available

- URL: https://www.encripto.no/forskning/whitepapers/BT3_User_Guide.pdf

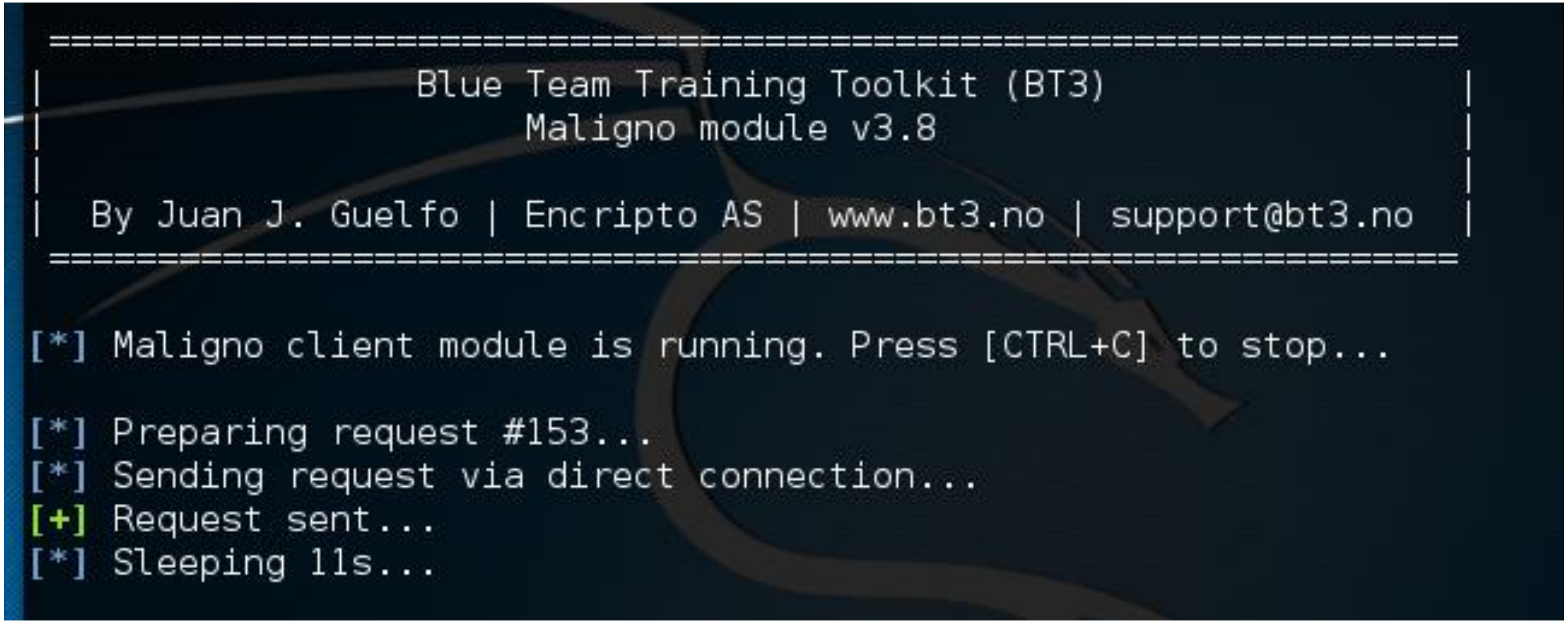
BT3: Adversary Server side setup is similar to Metasploit. set LHOST, sample profile, and gen the Python client code



```
BT3 ~ maligno > show profiles disk

    File              Size (MB)    Location    Date          Price     Description
    ----              ---------    --------    ----          -----     -----------
    cryptowall_v3.py  0.003        Disk        2015-02-13              Cryptowall v3 ransomware profile.
    etumbot.py        0.003        Disk        2014-07-01              Etumbot APT backdoor profile.
    havex.py          0.004        Disk        2014-03-14              Havex trojan profile.
    standard.py       0.003        Disk        2016-06-26              Default profile with static elements.


[*] Available profiles: 4

BT3 ~ maligno > set profile havex.py

[+] profile => havex.py

BT3 ~ maligno > genclient

[*] Generating Maligno client...
[+] Maligno client successfully generated! Check the "clients" folder.

BT3 ~ maligno > run
```

BT3 Client Side

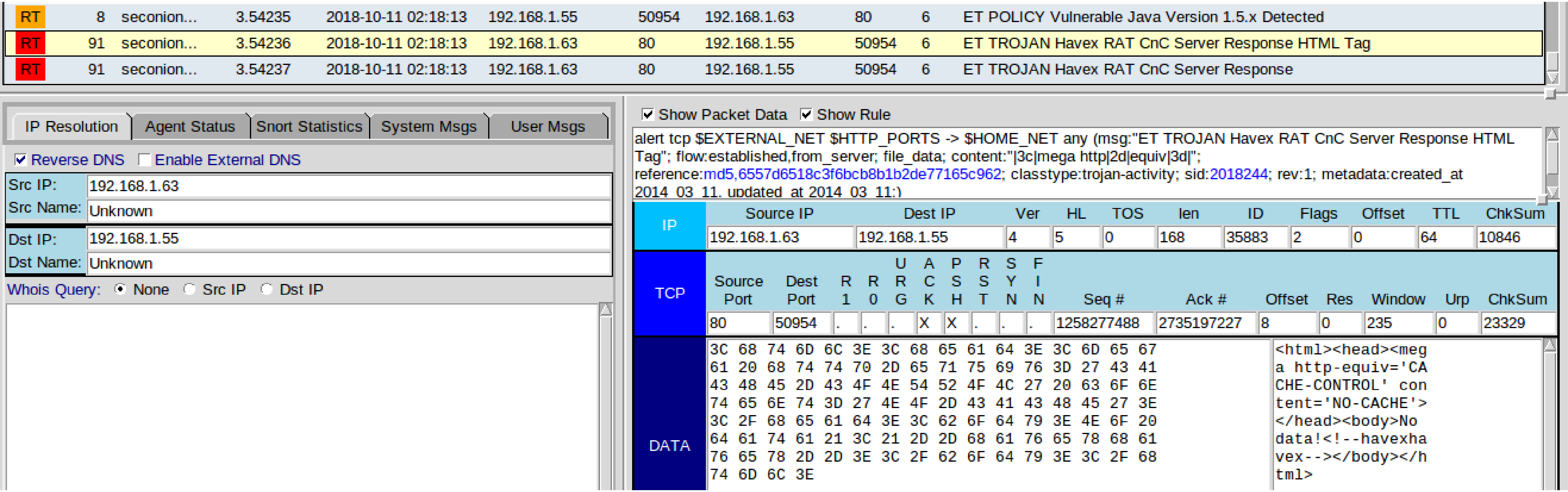
- Client needs the “maligno_client_havex.py” file onboard – just run it!
- python maligno_client_havex.py # options abound here....



```
 ==========================================================================
|                      Blue Team Training Toolkit (BT3)                    |
|                            Maligno module v3.8                           |
|                                                                          |
|  By Juan J. Guelfo | Encripto AS | www.bt3.no | support@bt3.no          |
 ==========================================================================

[*] Maligno client module is running. Press [CTRL+C] to stop...

[*] Preparing request #153...
[*] Sending request via direct connection...
[+] Request sent...
[*] Sleeping 11s...
```

NETWITNESS
Internal Use - Confidential An RSA Business

Snort Picks up the Trojan Behavior
Havex is an espionage focused tool



RT	8	seconion...	3.54235	2018-10-11 02:18:13	192.168.1.55	50954	192.168.1.63	80	6	ET POLICY Vulnerable Java Version 1.5.x Detected
RT	91	seconion...	3.54236	2018-10-11 02:18:13	192.168.1.63	80	192.168.1.55	50954	6	ET TROJAN Havex RAT CnC Server Response HTML Tag
RT	91	seconion...	3.54237	2018-10-11 02:18:13	192.168.1.63	80	192.168.1.55	50954	6	ET TROJAN Havex RAT CnC Server Response

☑ Reverse DNS ☐ Enable External DNS

Src IP: 192.168.1.63
Src Name: Unknown
Dst IP: 192.168.1.55
Dst Name: Unknown

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET TROJAN Havex RAT CnC Server Response HTML
Tag"; flow:established,from_server; file_data; content:"|3c|mega http|2d|equiv|3d|";
reference:md5,6557d6518c3f6bcb8b1b2de77165c962; classtype:trojan-activity; sid:2018244; rev:1; metadata:created_at
2014_03_11, updated_at 2014_03_11;)
```

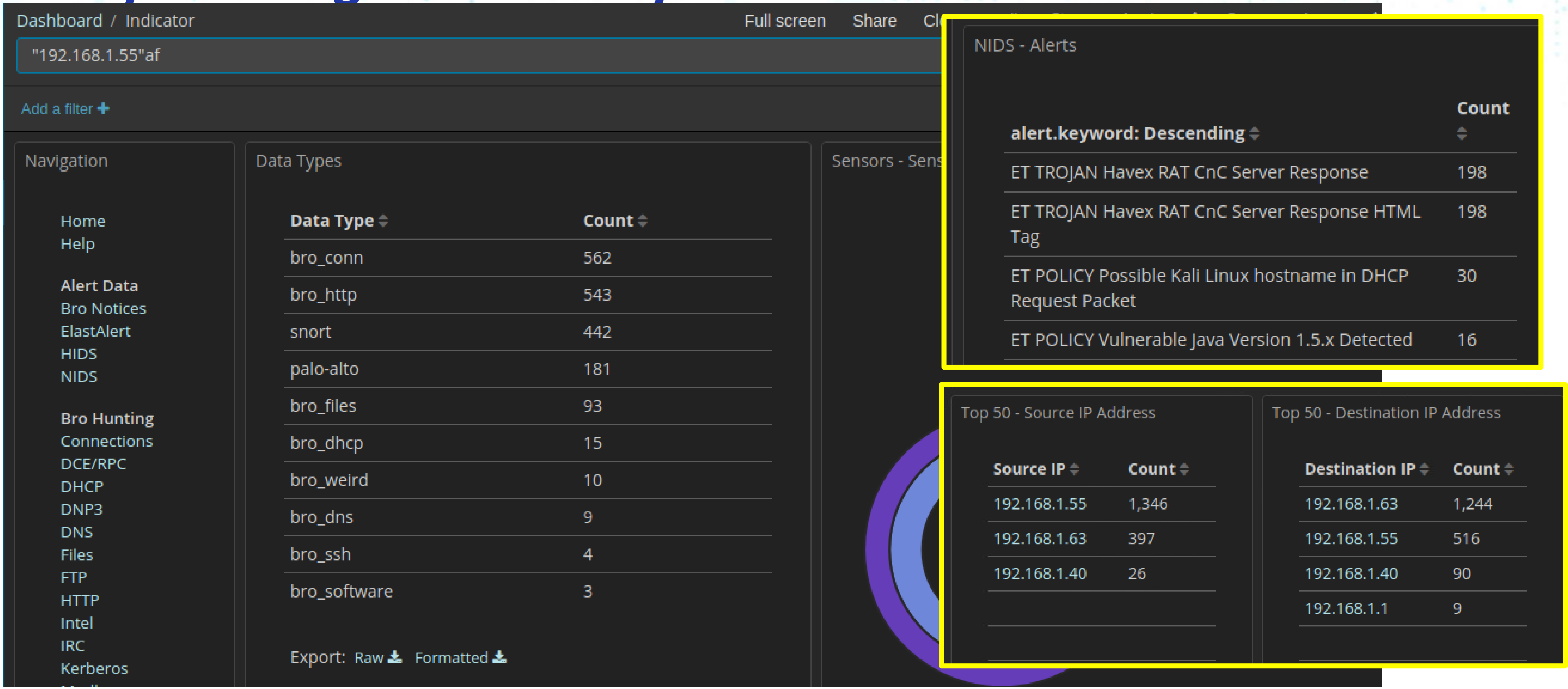
IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	192.168.1.63	192.168.1.55	4	5	0	168	35883	2	0	64	10846

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	80	50954	.	.	.	X	X	.	.	.	1258277488	2735197227	8	0	235	0	23329

DATA

```
3C 68 74 6D 6C 3E 3C 68 65 61 64 3E 3C 6D 65 67   <html><head><meg
61 20 68 74 74 70 2D 65 71 75 69 76 3D 27 43 41   a http-equiv='CA
43 48 45 2D 43 4F 4E 54 52 4F 4C 27 20 63 6F 6E   CHE-CONTROL' con
74 65 6E 74 3D 27 4E 4F 2D 43 41 43 48 45 27 3E   tent='NO-CACHE'>
3C 2F 68 65 61 64 3E 3C 62 6F 64 79 3E 4E 6F 20   </head><body>No
64 61 74 61 21 3C 21 2D 2D 68 61 76 65 78 68 61   data!<!--havexha
76 65 78 2D 2D 3E 3C 2F 62 6F 64 79 3E 3C 2F 68   vex--></body></h
74 6D 6C 3E                                       tml>
```

Analysis Using the Security Onion Solution



Data Types

Data Type	Count
bro_conn	562
bro_http	543
snort	442
palo-alto	181
bro_files	93
bro_dhcp	15
bro_weird	10
bro_dns	9
bro_ssh	4
bro_software	3

NIDS - Alerts

alert.keyword: Descending	Count
ET TROJAN Havex RAT CnC Server Response	198
ET TROJAN Havex RAT CnC Server Response HTML Tag	198
ET POLICY Possible Kali Linux hostname in DHCP Request Packet	30
ET POLICY Vulnerable Java Version 1.5.x Detected	16

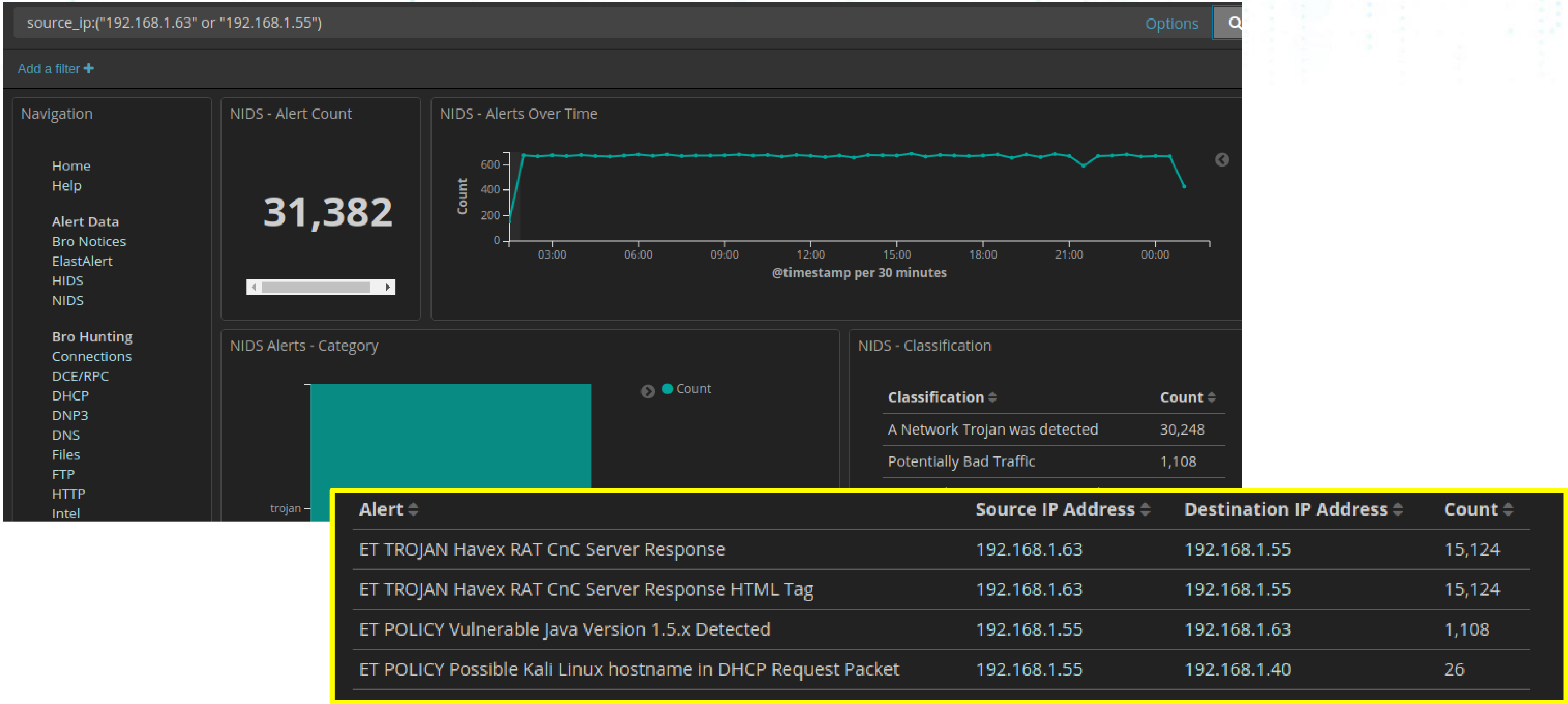
Top 50 - Source IP Address

Source IP	Count
192.168.1.55	1,346
192.168.1.63	397
192.168.1.40	26

Top 50 - Destination IP Address

Destination IP	Count
192.168.1.63	1,244
192.168.1.55	516
192.168.1.40	90
192.168.1.1	9

If you let it run for a day …



```
source_ip:("192.168.1.63" or "192.168.1.55")
```

NIDS - Classification

Classification	Count
A Network Trojan was detected	30,248
Potentially Bad Traffic	1,108

Alert	Source IP Address	Destination IP Address	Count
ET TROJAN Havex RAT CnC Server Response	192.168.1.63	192.168.1.55	15,124
ET TROJAN Havex RAT CnC Server Response HTML Tag	192.168.1.63	192.168.1.55	15,124
ET POLICY Vulnerable Java Version 1.5.x Detected	192.168.1.55	192.168.1.63	1,108
ET POLICY Possible Kali Linux hostname in DHCP Request Packet	192.168.1.55	192.168.1.40	26

Thank you!