Skill Sharpening @ the Cyber Range: Developing the next generation Blue Team

Don Murdoch, GSE #99, MSISE, MBA

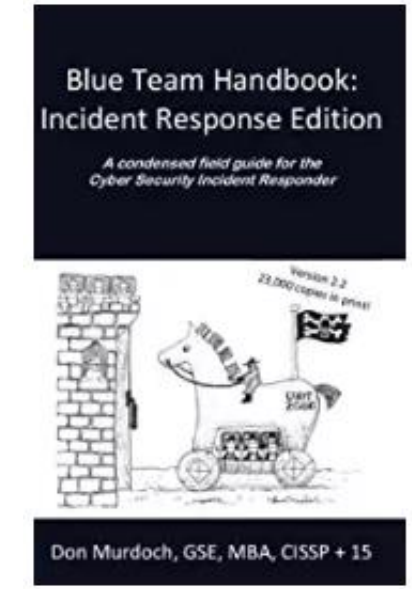
(and quite a bit more alphabet soup)

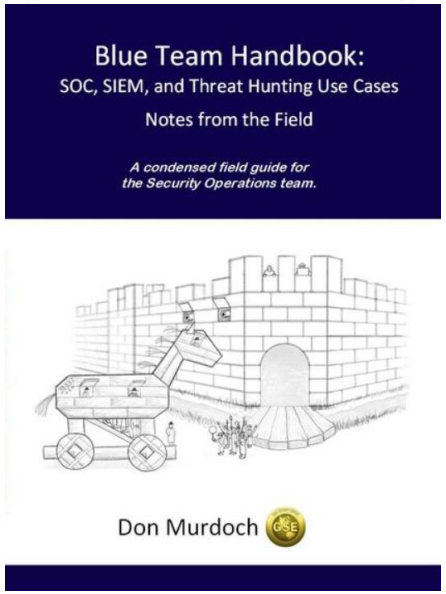
Asst. Director, Regent Cyber Range Virginia Beach, VA

Jan 9, 2019 Virginia Beach ISC2 Chapter Meeting

REGENT UNIVERSITY

whoami





Sapere Aude
"Dare to be Wise"

- There are three types of people on the Internet:
  - Sheep
  - Wolves
  - **Shepherds**

- Shepherd
  - 27+ years in IT, 17 InfoSec (gosh I feel old…)
  - Boat loads of alphabet soup, including EMT/A
  - Author BTHb Series
  - Scenario Designer and Instructor at Regent U. Cyber Range
    - Come flex your muscles!

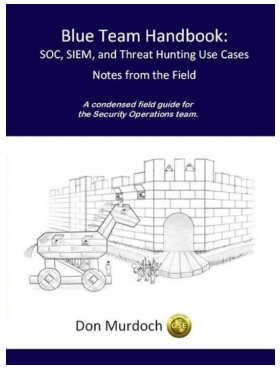
Regent Range - In a Nutshell
Blue Team Focused Adversary Emulation

- Four class groups in 2x3 arrangement
  - Five students
  - One trainer station
  - Each class is isolated from each other
  - Live, re-runnable scenarios
- Instrumentation
  - SIEM's, Firewall's, Sec Onion, email, DNS, ICS hardware, 15 segments, 40+ OS's….
  - Rinse, Wash, Repeat (4 min) as needed
- Students go through
  - Tools Orientation
  - SIEM Instrumentation
  - Intrusion analysis and IR
- Practice Incident Response
  - Working as a team of two
  - Investigate and Document
  - Reconstruct investigative attack timeline
  - Strive for an exec summary
- After action
  - Share tools, techniques, write ups
  - Formal Certification req's a Don-Cu-Ment grade write up
- **Students** ***can actually change the environment and achieve different outcomes, which we encourage***

REGENT UNIVERSITY

Blue Team Ed. Must Answer Critical Questions for Success

- Why do you need to test internal staff?
- Why is AdSim going to improve internal security over establishing and maturing the "next best thing"?
  - Mature the threat hunting program.
  - Reduce overall elevated account exposure.
- How will internal staff respond to being tested?
  - Hawthorne Effect
  - What will this do to their morale?
  - AdSim generally depends on "assumed compromise".
  - What are your breach vectors so that AdSim works properly in your environment?



REGENT UNIVERSITY

Even more questions

- How are info systems *actually instrumented?*
  - Avoid building scenario dev with a capability you don't actually use!
- How do we prioritize?
  - This answer must be **BUSINESS RELAVENT** and tied to the **Value Chain.**

- How do we safely build scenarios?
  - What happens if some nastiness "escapes"?
  - Ans: MITRE ATT&CK & Adversary TTP, MISP
- Can we use production? (that might be a RGM…)

REGENT UNIVERSITY

Hawthorne Effect

(because everyone needs some industrial psychology…)

- Research has found that the novelty of being research subjects and the increased attention from such leads to ***temporary*** increases in workers' productivity; result tin short term gain; improvements are not sustainable from direct observation and measurement. For the observer, too….
- BT Application:
  - Personal Observation found that trainees follow the "outline" more when facilitator routinely checks in on them, certain people have more attention applied to them, and professed skill affects the amount of coaching given.
  - Compensator: Develop ***and use*** timing, process, and output analysis objective criteria
- Originated at Hawthorne Works in Cicero, Illinois, in 1958 by Henry A. Landsberger

REGENT UNIVERSITY

BT Training Needs a Plan!

- A training outline has a purpose: its about a learning outcome (KSA's)
  - Title, Learning Objectives, outline, and written learning outcomes
  - OBJECTIVE Scoring vehicle
  - Completion Tool Activity list (did you do X,Y, and Z?)
  - NICE / NICCS INRE and CDA are usable starting points
- A training program needs to include:
  - Initial KSAl assessment, entry points, and progression model
  - Time commitments outlined with a tie in to the organization IDP
  - Charge code::
    - Professional educational development with a scenario costs between 23 to 143 hours per hour of delivery time , based on complexity and delivery method (Assoc for Talent Dev2018 study)
  - Reusable resources (more on that later....)
- Ref: https://www.td.org/insights/how-long-does-it-take-to-develop-one-hour-of-training-updated-for-2017

REGENT UNIVERSITY

BT Range Requirements

- Platform management
  - Virtualization is a must – Local VMware, AWS, Azure, ...
  - Cloud = set your VPC to allow to/from your own network to prevent spillage
- Scenarios
  - Static, Dynamic, multiple levels, different duration, ...
  - Training scenario generation and execution for repeatability through scripted ed.
- Modeled Networks
  - Server, Client, ICS, DMZ, Internet, Partner, VPN, ...
- Hosts – after all, you need something to attack and defend!
- After action analysis and reporting process and measurement

REGENT UNIVERSITY

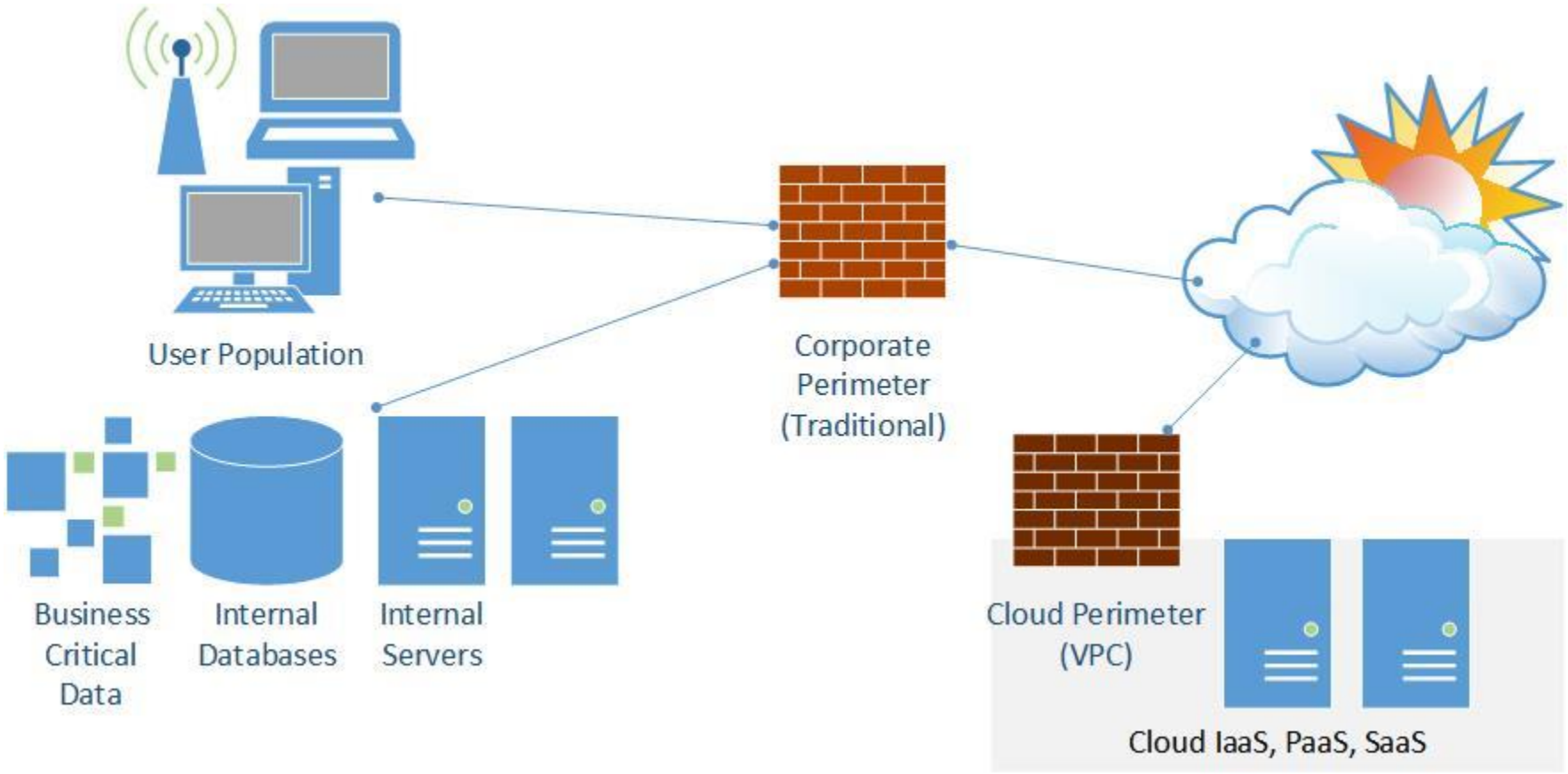
Cyber Range Scenario Information Flow

Range info flow *impacts attendee* progress!

- Setup, initiate session using a reusable/repeatable attack generation
- Observation/recording of the trainee
  - Merely observing staff *will change their behavior*
- Record keeping for meeting objective(s)
  - Did the trainee use the desired technique? Was an alternate suitable?
- Defense tools observe, trainee react and engage, INVESTIGATE
- Confirm the trainee "Solves the case"
  - Implement a change to contain the breach/attack (Remediate)
  - Perform root cause analysis
- Write up at the level required by the organization, using org specific tools

REGENT UNIVERSITY

Range Network Layout and Components



How do you select tools?

- What do you own?
  - Is there a "lab" model
    - For example, Palo Alto has a PA-220 Lab Skew w/ a < $1k price point
- Or better yet – do you actually need "tools"?
- Requirements?
- Will FOSS get you there?
  - Remember – many AdSim tools assume the attacker gains at least end user access, and takes it form there. Several FOSS packages support this.

REGENT UNIVERSITY

What FOSS tools are out there?

- APT Simulator (batch)***
- Atomic Red Team ***
- AutoTTP
- Blue Team Training Toolkit (BT3) ***
- Caldera
- dumpsterfire
- Infection Monkey
- Invoke-adversary
- Kali – build purpose drive scripts with MetaSploit – Tons of Packt type books!
- Metta
- NSA unfetter
- Endgame's Red Team Automation
- Unicorn for Pshell Encoding

- Other Blue Tools
  - SiLK
  - BHIS RITA – but Zeek needs TSV
  - QRader @ 50 EPS or less
  - Relkci – whitenoiselist
  - Windows Forensic Toolchest
  - Log MD – Free or Pro ***
- Platforms
  - OpenSOC.io
  - Security Onion ***

REGENT UNIVERSITY

Artificial Domain Build Tools

- AutoLab
- AutomatedLab
- Boxstarter
  - Targets Hyper V
- DetectionLab ***
  - Targets VirtualBox, somewhat finicky, but when it works!
- LAN/WAN Specific emulation tools
  - GNS3
  - Cisco VIRL

- DetectionLab
  - Multistage extendable build process
  - Downloads Win2016, Win10, Linux
    - Uses native MSFT build tools
  - Windows AD, DNS Server
    - Strong Windows audit posture
  - Windows Event Forwarding Server
    - Collector & Subscriptions
  - Windows 10 Workstation
    - Highly instrumented sysmon and WEF
  - Logger
    - Splunk, OSQuery, and MITRE Caldera

apt simulator

- Start here
  - Snapshot the VM….
- Solid "stand alone" batch tool
  - Triggers AV, NIDS, HIDS, …
- Cases – highlights
  - Local file collation
  - C2 connection w/WMI
  - Malware RAT, Mimikatz
  - Guest Admin
  - NBTscan, other local Recon
  - Persistence – AT, Run, Sch Tasks
- https://github.com/NextronSystems/APTSimulator

Administrator: Command Prompt - APTSimulator.bat

```
================================================================================
DNS CACHE

Creating DNS Cache entries for well-known malicious C2 servers
C2: msupdater.com
Non-authoritative answer:
C2: twitterdocs.com
Non-authoritative answer:
C2: freenow.chickenkiller.com
Non-authoritative answer:
C2: www.googleaccountsservices.com
Non-authoritative answer:

================================================================================
EVENTLOG

Creating Eventlog Entries indicating the use of password dumpers

SUCCESS: An event of type 'Success' was created with 'System' as the log.

SUCCESS: An event of type 'Success' was created with 'System' as the log.

================================================================================
HOSTS

Modifying the hosts file
Adding update.microsoft.com mapping to private IP address

================================================================================
SETHC BACKDOOR
Two methods: Replacement of sethc.exe / Debugger registration

Backing up old sethc.exe
        1 file(s) copied.

Trying to replace the real sethc.exe - administrator rights needed
Instead registering cmd.exe as debugger for sethc.exe
```

REGENT UNIVERSITY

Integrate an Open Source / Inexpensive Option – BT3

BT3 – Encryptio.IO

Several N/C modules in each category

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

- Easy implementation
  - Get Kali, 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
- 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

REGENT UNIVERSITY

BT3

- Server side setup – set LHOST, sample profile, and gen the py 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...
```

REGEN UNIVERSITY

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

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs

☑ 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	URG	ACK	PSH	RST	SYN	FIN	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
61 20 68 74 74 70 2D 65 71 75 69 76 3D 27 43 41
43 48 45 2D 43 4F 4E 54 52 4F 4C 27 20 63 6F 6E
74 65 6E 74 3D 27 4E 4F 2D 43 41 43 48 45 27 3E
3C 2F 68 65 61 64 3E 3C 62 6F 64 79 3E 4E 6F 20
64 61 74 61 21 3C 21 2D 2D 68 61 76 65 78 68 61
76 65 78 2D 2D 3E 3C 2F 62 6F 64 79 3E 3C 2F 68
74 6D 6C 3E
```

```
<html><head><meg
a http-equiv='CA
CHE-CONTROL' con
tent='NO-CACHE'>
</head><body>No
data!<!--havexha
vex--></body></h
tml>
```

REGENT UNIVERSITY

Pivot to Kibana in Sec Onion

Dashboard / Indicator

Full screen Share

"192.168.1.55"af

Add a filter +

Navigation

Home
Help

Alert Data
Bro Notices
ElastAlert
HIDS
NIDS

Bro Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos

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

Export: Raw Formatted

Sensors

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")

Options

Add a filter +

Navigation

Home
Help

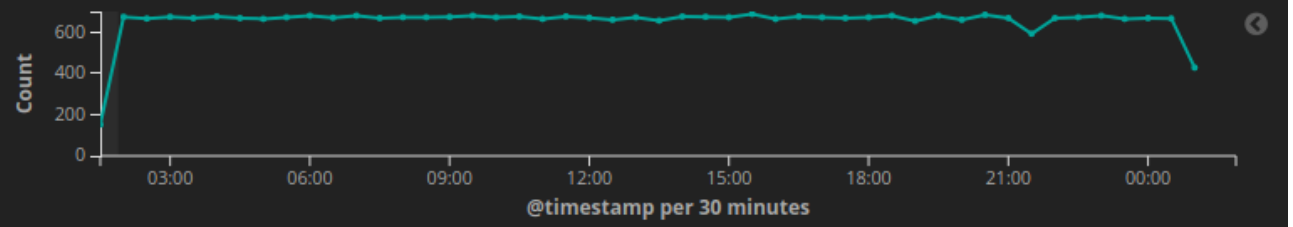
Alert Data
Bro Notices
ElastAlert
HIDS
NIDS

Bro Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel

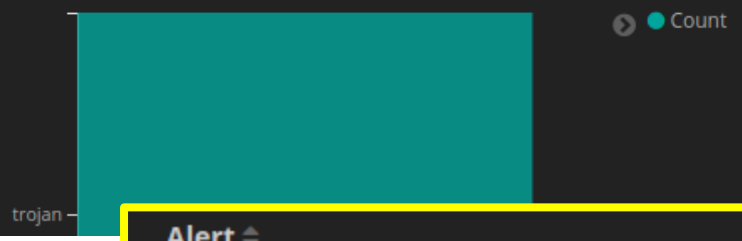
NIDS - Alert Count

31,382

NIDS - Alerts Over Time



NIDS Alerts - Category



NIDS - Classification

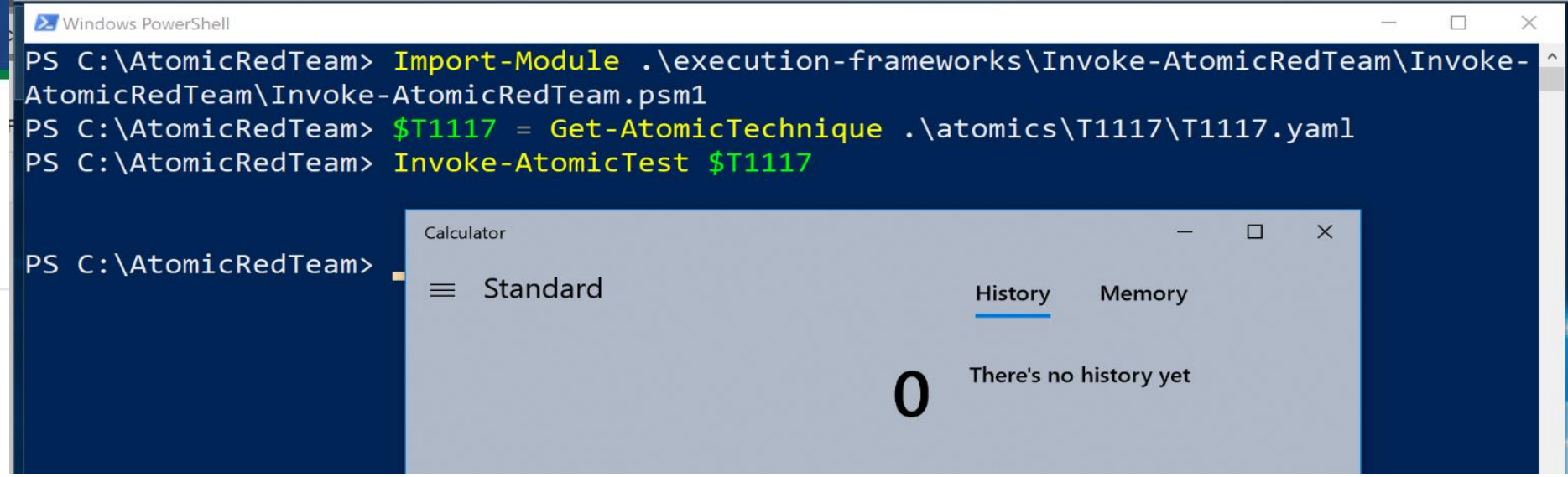
Classification	Count
A Network Trojan was detected	30,248
Potentially Bad Traffic	1,108
Potential Corporate Privacy Violation	26

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

REGENT UNIVERSITY

Atomic Red Team

- Simple Atomic Tests
- Mapped To MITRE ATT&CK
- Easy To Use
  - Execute in either PowerShell or Python
- Demystify The Attacks
- Open Source
- Test Multiple Products




```yaml
---
attack_technique: T1117
display_name: Regsvr32
atomic_tests:
- name: Regsvr32 local COM scriptlet execution
  description: |
    Regsvr32.exe is a command-line program used to register and unregister OLE controls
  supported_platforms:
  - windows
  input_arguments:
   filename:
    description: Name of the local file, include path.
    type: Path
    default: Regsvr32.sct
  executor:
   name: command_prompt
   command: |
    regsvr32.exe /s /u /i:#{filename} scrobj.dll
```

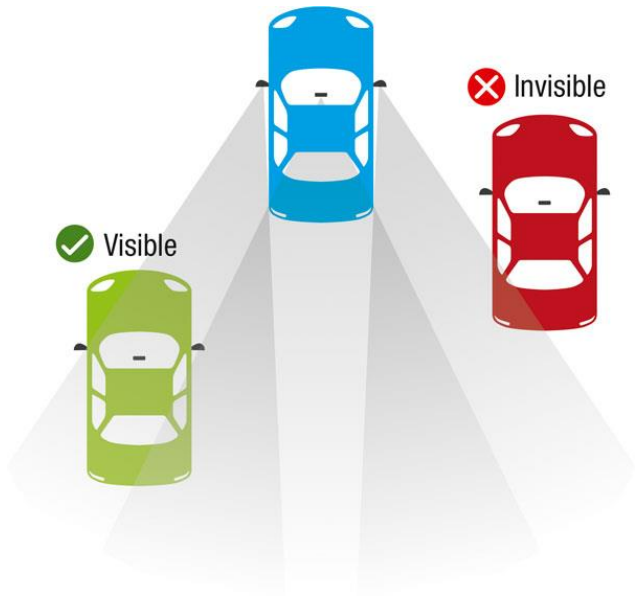
Commercial BAS Products

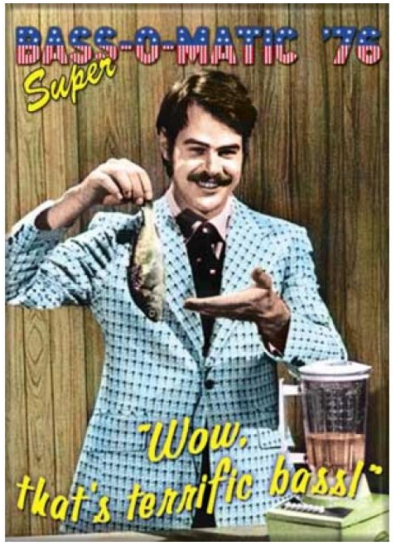
(Breach and Attack Simulation)

- BAS tools
  - AttackIQ
  - Safe Breach
  - Immunity Adversary Simulation
  - Cymulate
  - Immunity Adversary Simulation
  - Office 365 - Attack Simulator
  - Spectre Ops
  - On the horizon
    - randori.com
- Tools that can be leveraged
  - SCYTHE (by Grimm) ***
  - Cobalt Strike
- BreakingPoint by IXIA
  - > 500 malicious traffic patterns
  - >2300 (?) application traffic patterns
- And others…

BAS: What Benefits should you hope to find?

- How well do your security focused tools "Work"?
  - Inform, Prevent, Alarm
  - Do they really perform deep packet inspection?
    - Can you validate your $spend?
- How well have you instrumented your tools?
  - Do you perform protocol enforcement?
  - Just how many systems and users can ignore the proxy?
  - When you *know* what happened, can you find multiple supporting artifacts and traces?
- How porous is your perimeter?
  - What about that internal segmentation project?
  - How easy is it for you to data exfiltrate a 1 GB payload with SSNs?





REGENT UNIVERSITY

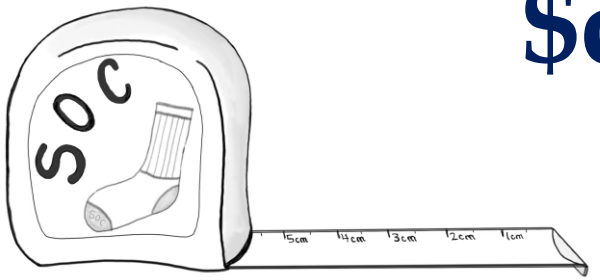
Commercial Product Approaches

- Operate in Isolation
  - Virtualized Company Work A Like Platform using VMware / AWS
- Artificial agent deployment
  - Similar to what a network trojan would do, but under InfoSec control
  - Scan for local vulnerabilities & stays "local"
  - Maps out pathways
- Malicious Network Traffic Generation
  - Virtualized systems, net to net traffic, needs to pass in front of a sensor
- Black Box Multi Vector
  - Agent to cloud service – intends to function as close to a real trojan or persistence tool as possible

Beware: Range-Isms Abound!

- Artificial constructs *are not attackers.*
  - They do not pivot
  - They do not adjust
  - They go after one thing – Domain Admin
  - They don't read your email … because they got your C Ring account creds
- Network activity without a "On System Trace" is only half the puzzle.
- Tools that depend on an "agent" aren't all that "real"
  - Attackers establish persistence that should be removed
  - Agents that need to run and can't be removed b/c that breaks other things
- Artificially high or low auditing
  - Do not train in a way where you cannot fight

REGENT UNIVERSITY



$o how will you mea$sure your training program $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 Zimmermans "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

REGENT UNIVERSITY

BTHb:SOCTH's Metrics

- 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

Focus in on Timeline Reconstruction

- Mean Time To Decision (MTTD)
  - Is the observable event True or False? (hint – range alarms are usually True!)
- 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 privilege on the target

Log MD – Need this in the toolbox

MalwareArchaeology.com

- Audit Policy compliance, Winows IR, Malware Discovery, Forensics
- Check Windows Advanced Audit Policies against Logging Cheat Sheet
- Harvest both Event Logs and non-log events
  - AutoRuns including all WMI namespaces
  - Large Registry keys (hidden payloads and scripts)
  - Full filesystem hash compare against known good image of hashes
  - List of Locked Files malware often uses to prevent cleanup
  - Full registry compare against known good registry snapshot
  - WhoIs lookups of single IP or a list of IPs
- Feed LOG-MD reports (CSVs) to your Log Management/SIEM if available

REGENT UNIVERSITY

Reports

- Focus on what happened
- Empty report?
  - Got Nutthin!
- CSV reports enable downstream processing with a variety of tools
- Create a "baseline", and then run the scenario, students should be able to compre/contrast

```
Report Summary:

  NumRows  Report
  -------  ------
    62840  Report.csv
        3  Report_BITS.csv
       35  Report_FW_Modifications.csv
      696  Report_File_Reg_Auditing.csv
    60124  Report_IP_Connections_All.csv
    20682  Report_IP_Connections_Browsers.csv
    39442  Report_IP_Connections_No_Browsers.csv
      839  Report_Process_Started.csv
       96  Report_Share_Accessed.csv
      858  Report_Task_Scheduler.csv
      141  Report_User_Activity.csv
    44864  Report_Whitelisted_out.csv

        0  Report_Process_Started_Users.csv
        0  Report_User_Privileges.csv
        0  Report_Windows_Defender.csv
        0  Report_Wrong_OS_Type_Errors.csv
```

REGENT UNIVERSITY

Upgrade to the Pro Version

- Parent / Child Process Tree
- MS Word calling CMD.EXE is not generally a good thing …

Parent_PID	Parent_Path	Child1	Child2	Child3	C
2140	C:\Windows\explorer.exe	C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE			
5140		|---------->	C:\Windows\SysWOW64\cmd.exe		
7784			|---------->	C:\Windows\System32\conhost.exe	
7784			|---------->	C:\Windows\SysWOW64\cmd.exe	

- Especially if there is a PowerShell call later on in the process tree

Child4	Child5	Child6	Child7	Child8
xe				
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe				
|---------->	C:\Users\HACKME\AppData\Local\Temp\986.exe			
	|---------->	C:\Users\HACKME\AppData\Local\Temp\986.exe		
		|---------->	C:\Users\HACKME\AppData\Local\Microsoft\Windows\slskey.exe	
			|---------->	C:\Users\HACKME\AppData\Local\Microsoft\Windo

After Action Reporting and Analysis

- Each "team" discusses their findings and how they got there
- 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

REGENT UNIVERSITY

Incident Response Report

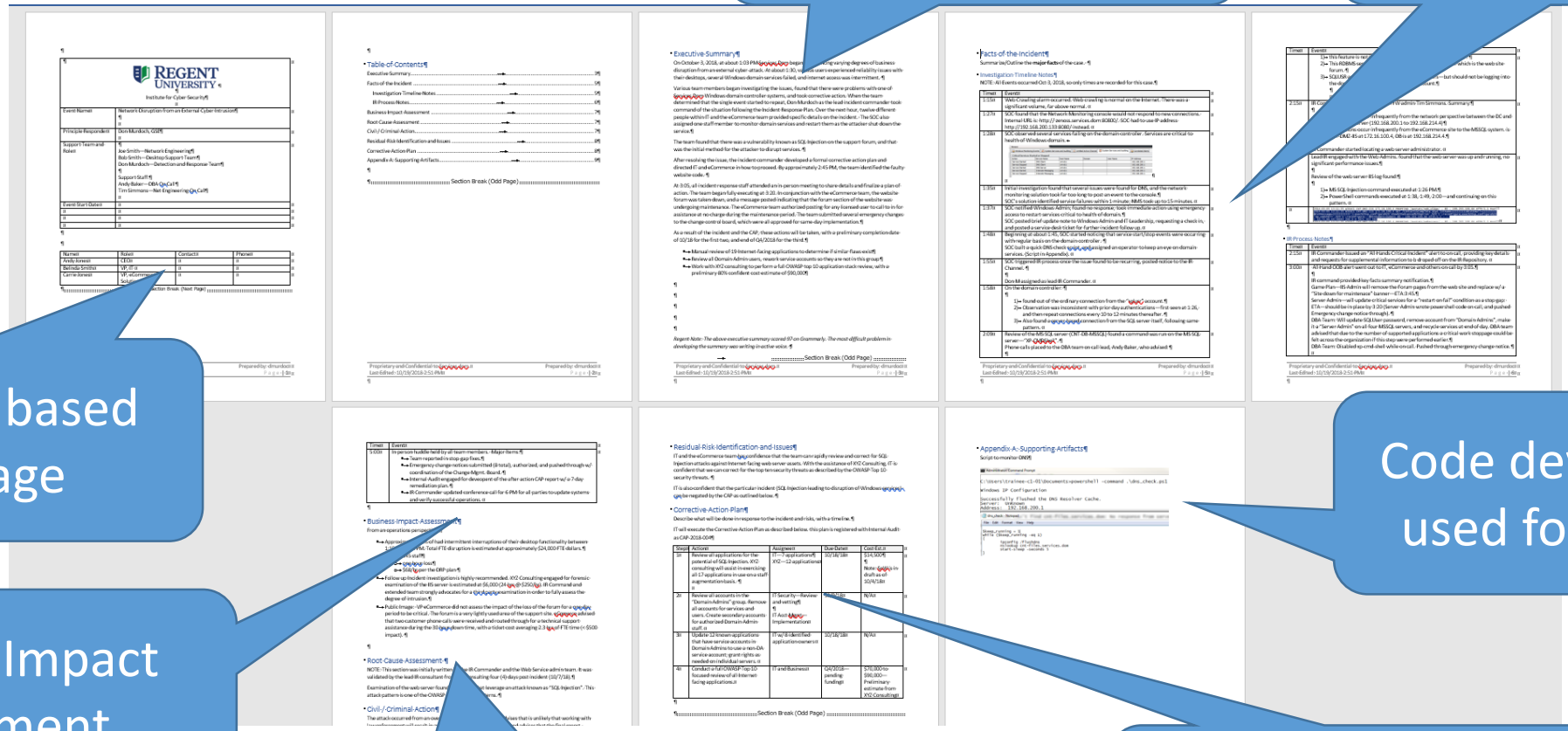
- Incident Response is a *team sport*
  - *Document* as you go
  - *Screen shots* really help
  - *IR Template* is a professional learning experience – you will use each template throughout the week
    - *PICERL format and an Executive Summary/Timeline format*
    - *Write Ups and the Template are yours to keep*
- During After Action Review
  - Go over each team's IR document and executive summary
  - Everybody is asked to contribute, talk through and take notes
  - Emphasis on Timeline Reconstruction – this is one of the *hardest skills to master* when it comes to Incident Response

REGENT UNIVERSITY

IR Report

Executive Summary with a Grammarly Score of 95

Timeline with fact data and artifacts



Participant based cover page

Code developed or used for the case

Business Impact Assessment

Blameless Root Cause Analysis

Corrective Action Plan (ISACA)

REGENT UNIVERSITY

Thank you!

Questions and Possible Answers for the balance of our time.

REGENT UNIVERSITY

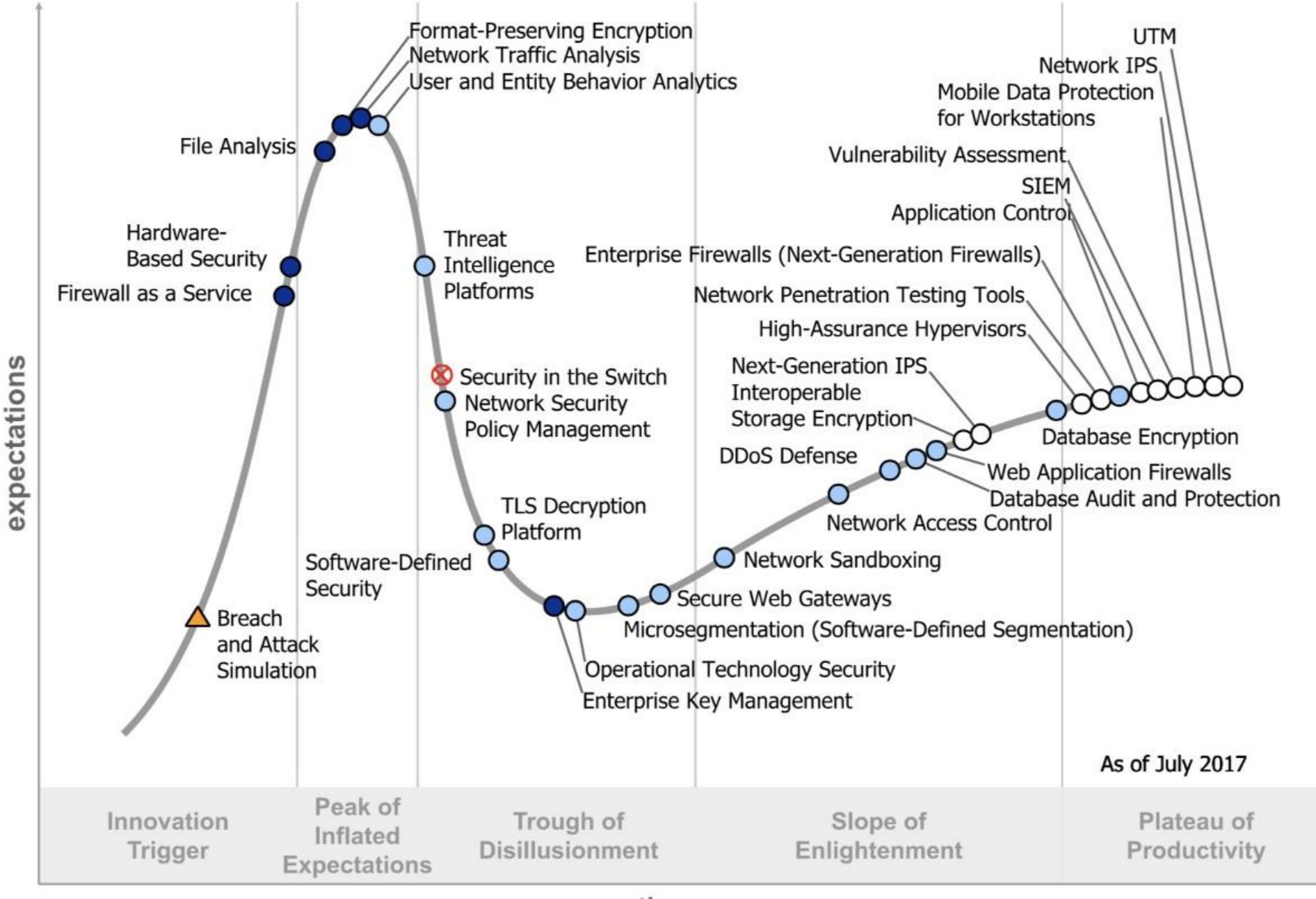
Other Slides that may be used

Level Set on the AdSim Lingo

- Gartner's BAS term – next slide!
- Red Team
  - Generally: externally hired to test physical, psychological, and technical defenses while they avoid detection and "find the crown jewels"
  - Should make every effort to use APT type attack patterns (A'la MISP)
- Blue Team (DART) – This is our focus area
  - Quite simply, YOU, the internal defender – the maintainer of the security posture
  - Detect, analyze, respond, weaken, and thwart the Red team
  - Focus on log analysis, network pattern analysis, and persistence detection and response
- Purple, White, Green
  - Conceptual, Transient – oversee and optimize RvB exercise, staffed with senior staff

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

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



REGENT UNIVERSITY

Leveraging the Gartner Model

Breach & Attack Simulation (BAS) Technologies

- Gartner Definition
  - Tools that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means
- Search Terms
  - Breach and Adversary Simulation will be a search term
  - Vendors will ensure that SEO works here (**Marketecture**^{TM})
- Beginning process of feature comparison
  - CIO/CISO's on the edge will start paying attention to this tech category
  - Posture testing – just starting to be a "purchased" item, as benefit is "high"

REGENT UNIVERSITY

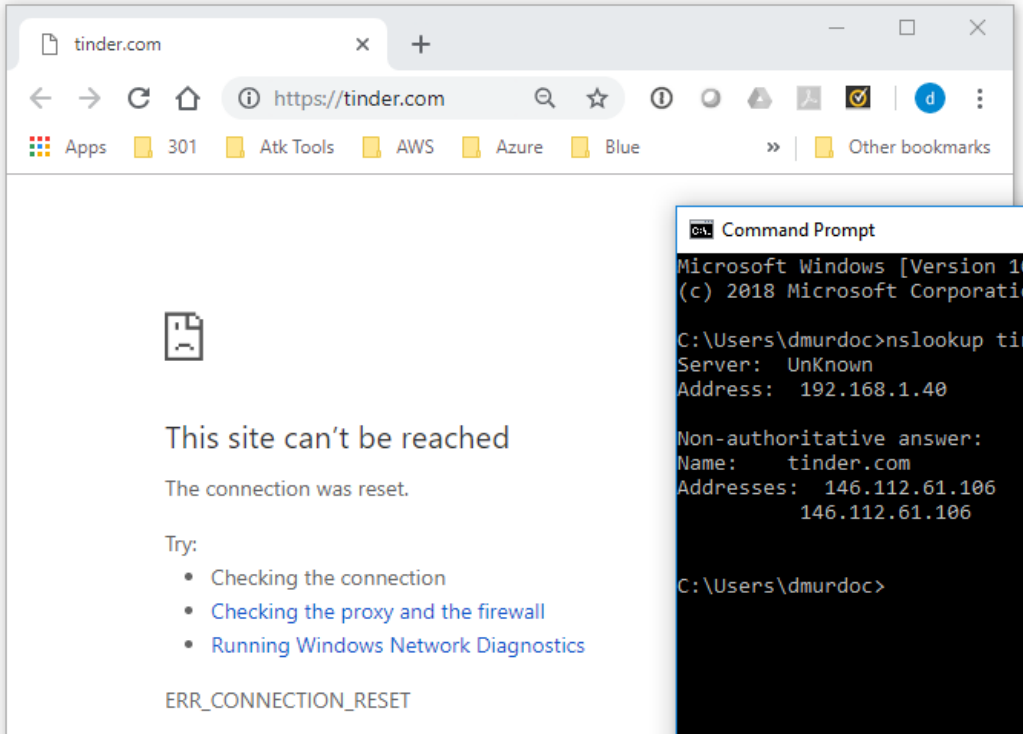
You do not need to actually $pend much to te$st your infra$tructure…

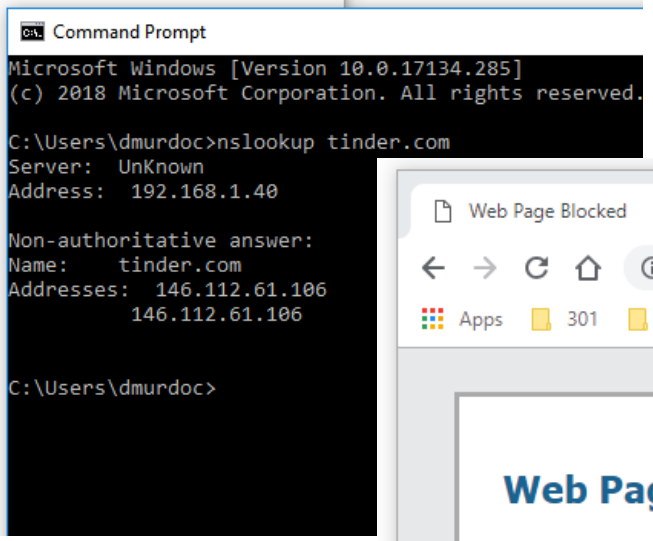
- Create an isolated segment
  - Install workstation with your golden image and common application
    - Amp it up a bit … sysmon, check the stance with LogMD
    - Install a "rollback" app
  - Install a copy of Sec Onion on the same segment
    - Must mirror LAN traffic for this to be effective
  - Limit connectivity to internal segments
  - Build scripts to:
    - Retrieve "recent" malware lists (MDL, RBL, ISC)
    - Reach out, retrieve, curl, etc.
- Technique used for several years (by me) to demo security products for clients

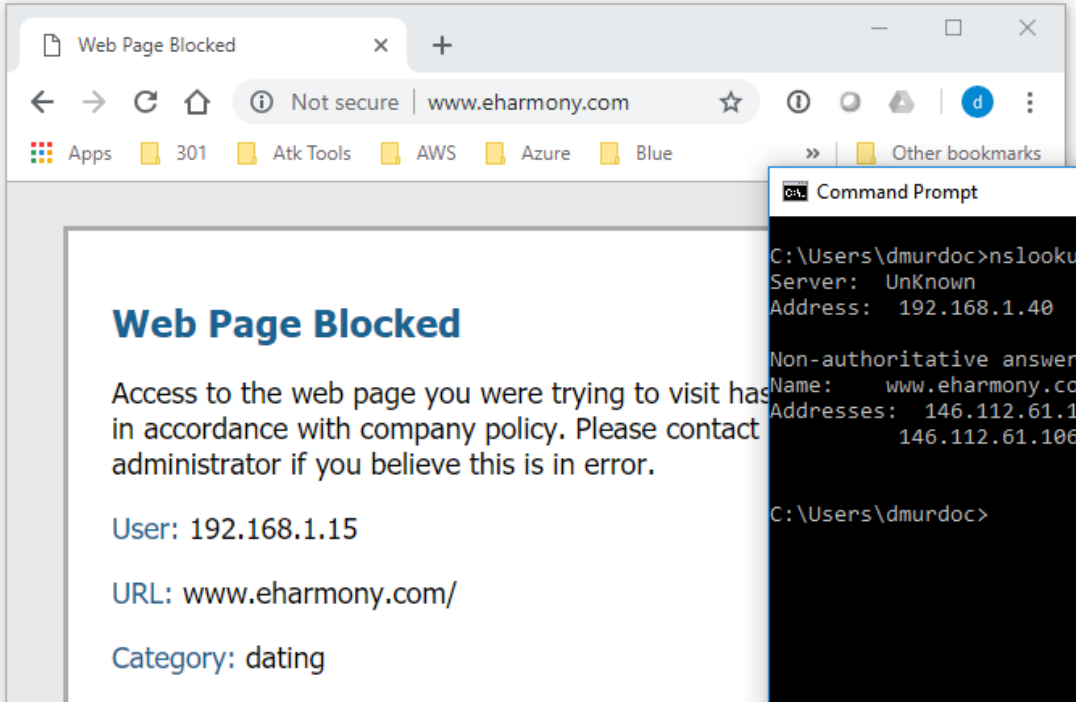
REGENT UNIVERSITY

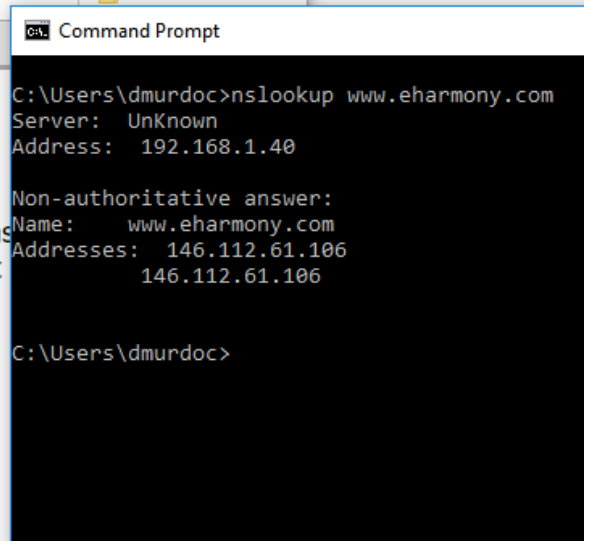
Example Test

Why does the Palo Alto treat these differently?









REGENT UNIVERSITY

Note that the protective system behaved differently…

(addr.src in 192.168.1.15)

Receive Time	Category	URL	From Zone	To Zone	Source	...	Destination	Application	Action
10/09 23:34:52	dating	tinder.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url
10/09 23:34:52	dating	tinder.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url
10/09 23:34:47	dating	tinder.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url
10/09 23:34:47	dating	tinder.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url
10/09 23:34:47	dating	tinder.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url
10/09 23:34:47	dating	tinder.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url
10/09 23:34:38	dating	www.eharmony.com/favicon.ico	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	web-browsing	block-url
10/09 23:34:38	dating	www.eharmony.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	web-browsing	block-url
10/09 23:34:32	dating	www.okcupid.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url
10/09 23:34:32	dating	www.okcupid.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url
10/09 23:34:32	dating	www.okcupid.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url
10/09 23:34:32	dating	www.okcupid.com/	LocalLAN	Internet	Dons_Window...		hit-adult.opendns.com	ssl	block-url

Detailed Log View

General

Session ID	185773
Action	block-url
Application	web-browsing
Rule	dons_computers
Virtual System	
Device SN	
IP Protocol	tcp
Log Action	siem
Category	dating
Generated Time	2018/10/09 23:34:38
Receive Time	2018/10/09 23:34:38
Tunnel Type	N/A

HTTP Headers

User-Agent	
Referrer	
X-Forwarded-For	

Source

User	
Address	192.168.1.15
Country	192.168.0.0-192.168.255.255
Port	6058
Zone	LocalLAN
Interface	ethernet1/2

Details

Severity	informational
Repeat Count	1
URL	www.eharmony.com/
	Request Categorization Change
HTTP Method	get

Destination

User	
Address	146.112.61.106
Country	Austria
Port	80
Zone	Internet
Interface	ethernet1/1

Flags

- Captive Portal ☐
- Proxy Transaction ☐
- Decrypted ☐
- Packet Capture ☐
- Client to Server ☑
- Server to Client ☐
- Tunnel Inspected ☐
- Credential Detected ☐

PCAP	Receive Time ▲	Type	Application	Action	Rule	Bytes	Severity	Category	Verdict	URL	File Name
	2018/10/09 23:34:52	end	web-browsing	allow	dons_com...	4857		dating			
	2018/10/09 23:34:38	url	web-browsing	block-url	dons_com...		informational	dating		www.ehar...	

REGENT UNIVERSITY

How about another application?

```
dmurdoch@seconion500gb:~$ date
Wed Oct 10 03:53:00 UTC 2018
dmurdoch@seconion500gb:~$ curl https://www.okcupid.com
curl: (35) gnutls_handshake() failed: Error in the pull function.
dmurdoch@seconion500gb:~$ curl https://www.eharmony.com
curl: (35) gnutls_handshake() failed: Error in the pull function.
dmurdoch@seconion500gb:~$
```

	Receive Time	Category	URL	From Zone	To Zone	Source	...	Destination	Application	Action
	10/09 23:56:18	shopping	www.amazon.com/	LocalLAN	Internet	192.168.1.34		a23-211-128-116.deploy.static.akamaitechno...	ssl	alert
	10/09 23:53:53	dating	www.eharmony.com/	LocalLAN	Internet	192.168.1.34		hit-adult.opendns.com	ssl	block-url
	10/09 23:53:37	dating	www.okcupid.com/	LocalLAN	Internet	192.168.1.34		hit-adult.opendns.com	ssl	block-url
	10/09 03:32:07	computer-and-internet-info	rules.emergingthreats.net/	LocalLAN	Internet	192.168.1.34		96.43.137.99	ssl	alert
	10/09 03:32:07	computer-and-internet-info	rules.emergingthreats.net/	LocalLAN	Internet	192.168.1.34		204.12.217.19	ssl	alert

REGENT UNIVERSITY

Ideas… There are MANY!

- Study each phase of the ATT&CK framework
  - Find / deploy a tool / tech for each phase grouping
  - Red needs to learn how, Blue needs to learn to find
- Build out a persistence lab, starting w/ an infected NBK that walks back in
  - Get some lateral movement going on
  - then use the JPCert LogonTracer to go find ‘em
- Build out an OWASP Top 10 lab
  - Red: perform attacks using MetaSploit, CobaltStrike, etc.
  - Blue: active monitor using SecOnion, bro (now zeek)
- Grab some Kali books, see what is a current attack technique, and detect it
- Review MetaSploit attacks against your deployed technology stack, spin up a P2V copy, defang the data, attack and defend

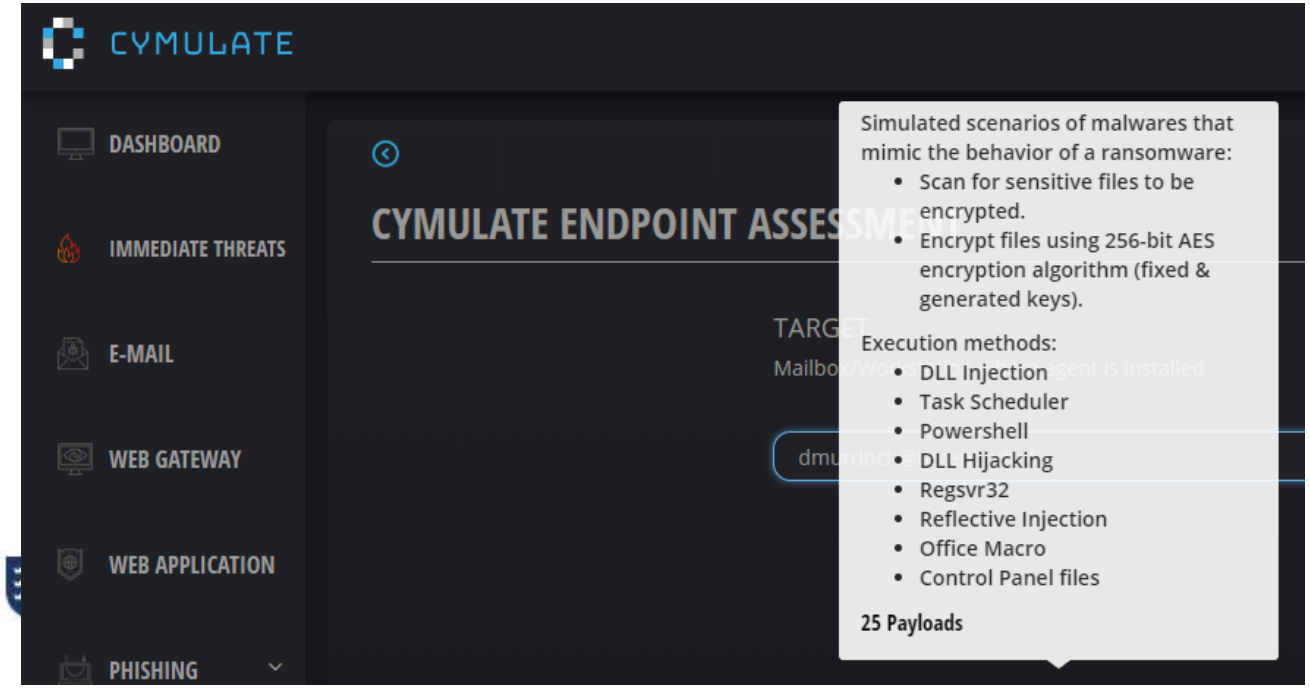
REGENT UNIVERSITY

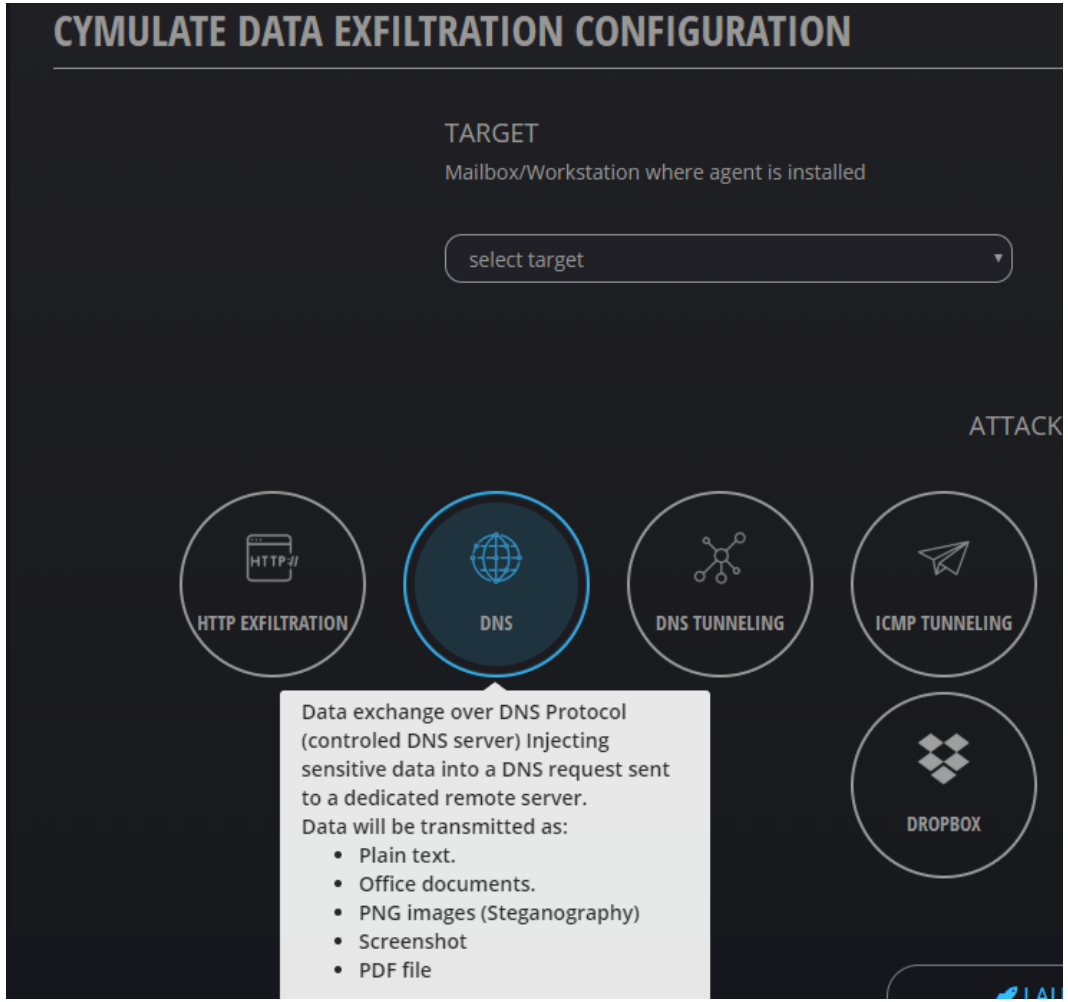
Attack IQ

- 1,500+ distinct attacks built into the tool
  - Active user community
- Designed to support tool, team, and process testing
- Staff can create (build) scenario steps
- Cannot change the deployed EXE name
- Significant remediation assistance and advice

Cymulate – Instrument Agents, Local ENV

- Mimic myriad of attack strategies and tools that malicious hackers and cyber criminals deploy
- Test all phases of an attack, from pre-exploitation to post-exploitation

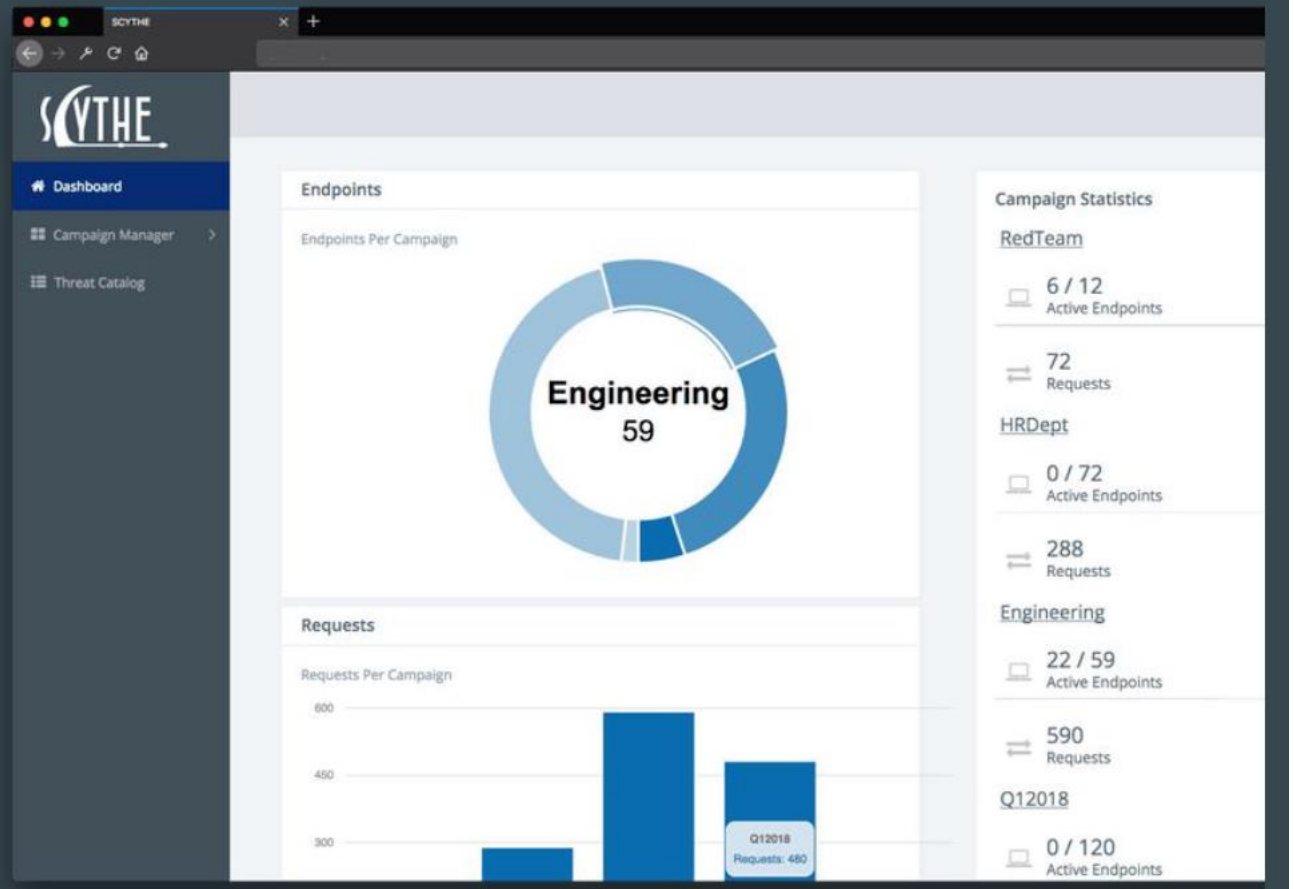




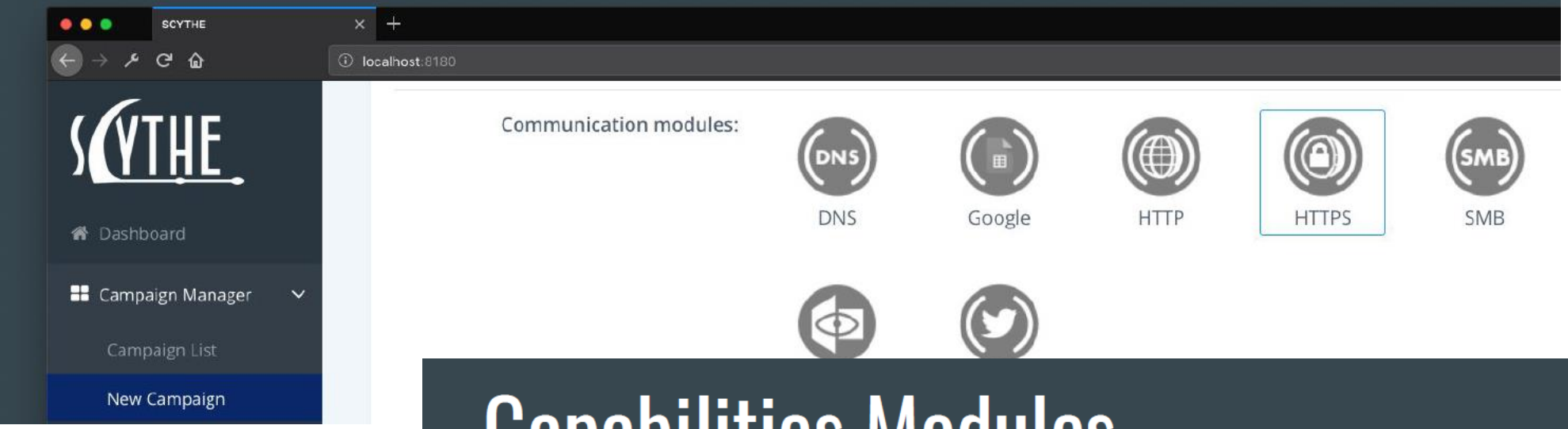
Overview

Scythe

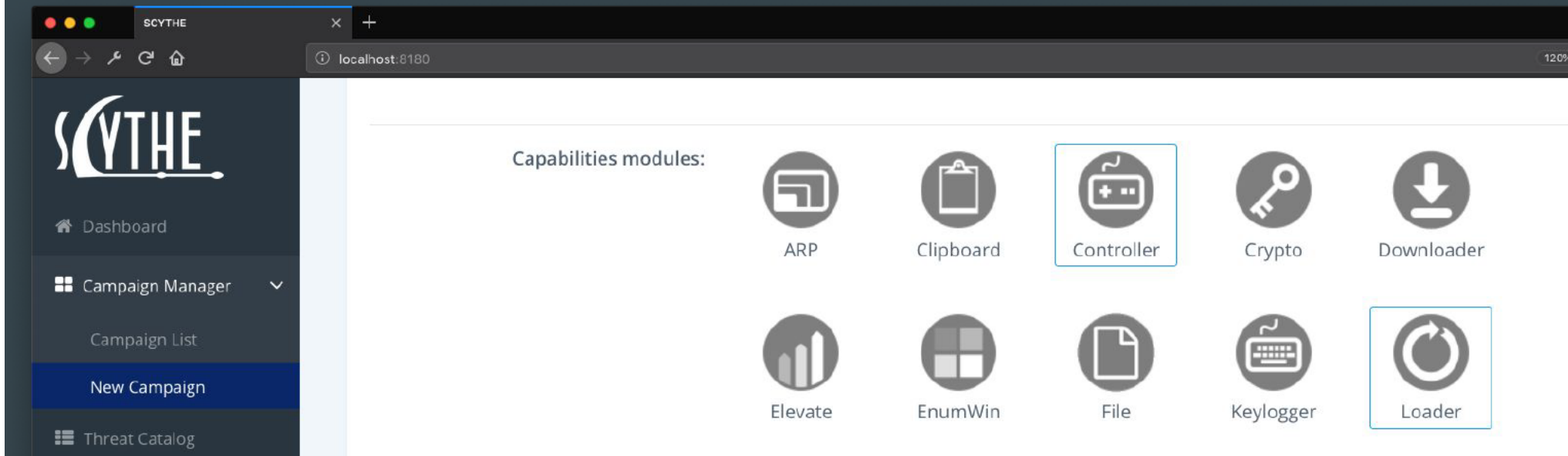
- Complex Adversary Simulation
- Modular Framework
  - Communication
  - Capabilities
- Flexible Implant Delivery
  - EXE & DLL
  - Phishing & Web
- Variable Reporting
  - Executive Summary
  - Detailed Exports
- Industry Aligned
  - MITRE ATT&CK & LM Kill Chain
- Module Development Guide



Communication Modules



Capabilities Modules



REGENT UNIVERSITY

Campaign Automation

SCYTHE

localhost:8180

SCYTHE

- Dashboard
- Campaign Manager
  - Campaign List
  - New Campaign
- Threat Catalog
- MITRE ATT&CK
- Users
- Settings

Automate Campaign

Actions

Search

Load a module

Elevate	EnumWin
File	Keylogger
Mimikatz	Persist
Processes	Search
Services	SMB Relay
SysInfo	Terminate

0 Start (with https , loader, and controller)

1 loader --load printscr

2 loader --load run

3 loader --load uploader

4 run cmd /c dir %USERPROFILE%\Documents

5 printscr --window Desktop