Exit Night, Enter Light

A case study

About the Presenter

- David Mashburn
  - Blue Teamer
  - GSE #157
  - Instructor
  - Coach

Overview of the case study

- How do we achieve tactical security visibility?
- How quickly can actionable data be gathered?
- What guidance can be leveraged to achieve these goals?
- How much of that guidance is achievable given the environment?

Tactical Security Visibility

- What defines security visibility?
  - The capture of security relevant events in our environment
  - Focus on detection rather than prevention
- Visibility provided by the collection and effective use of two forms of data
  - Network data (NSM)
    - Data in motion
    - Examples: Firewall logs, flow data
  - Endpoint data (CSM)
    - Data at rest
    - Examples: Log files, registry keys

The Environment

- Non-profit organization
  - Science-driven public health mission
  - Global presence
- Initial conditions
  - No existing security program
  - Resource constraints (people and skills)
- Opportunities vs obstacles

Constraints and Considerations

- Immediate security needs
  - Recent high-visibility security incidents
- Organizational inertia
  - The way that things are done
  - Security sounds like a great idea, but…
- Limited appetite for change
  - Focus on evolution rather than revolution
  - Control over security infrastructure, but otherwise limited authority

Constraints and Considerations (2)

- State of the Union
  - No significant organizational policies
  - Generally lacking formal IT governance
- Policy for monitoring was first task
  - Address relevant Legal/HR issues for monitoring
  - Operating internationally, so define scope of what we are able to do in certain localities
- Now have authority for technical implementation

Setup for Success

- Art of the possible
  - Security needs to build trust and establish credibility within IT
  - Initial actions need to have minimal impact on user community
- 'Living off the Land' from a defensive perspective (LOL Defense)
  - Focus on native features in deployed systems
  - Prioritize actions that have minimal impact on user community
- Critical Security Controls implementation

National Cyber Hygiene Campaign

- Do we know what is connected to our systems and networks? (CSC 1)
- Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
- Are we continuously managing our systems using "known good" configurations? (CSC 3)
- Are we continuously looking for and managing "known bad" software? (CSC 4)
- Do we limit and track the people who have the administrative privileges to change, bypass, or over-ride our security settings? (CSC 5)

Mapping a Plan

Control	Brief Description	Resistance	Applicability	Timeline
CSC 1	Device inventory	Low	Direct	Short
CSC 2	Software inventory	Low	Direct	Medium
CSC 3	Secure configurations	Medium	Indirect	Long
CSC 4	Vulnerability assessment	Low	Direct	Medium
CSC 5	Admin privilege management	High	Indirect	Long
CSC 6	Audit logs	Low	Direct	Short

Security Rectangle of Sorcery

Increasing User Impact

Increasing IT Effort

Firewall Flow data* IDS*	Web filters Vulnerability scanning Endpoint security suite
DNS logging DHCP logging Windows event collection Application whitelisting (auditing)	Application whitelisting (enforced) Secure configurations Privileged user management

Beyond the Network Focus

- Network centric view lacks full endpoint visibility
  - Looking only at inbound/outbound
  - Missing lateral movement
  - No visibility into encrypted traffic

- Leverage the Windows environment
  - Windows Active Directory, Windows desktops (enterprise edition)
  - Enable available OS features (no software deployment required)
  - Configuration changes via GPO

Windows Group Policy

- Audit settings
  - By default, endpoints are not logging important events
  - Critical Windows Servers already configured in some areas via GPO
  - Need visibility at endpoints to detect lateral movement and post-exploitation actions
- Windows Group Policy to the rescue
  - Increase maximum log sizes
  - Specify event categories to be audited
  - Enable fine-grained audit categories and process logging

Windows Group Policy (2)

- Application Whitelisting with AppLocker
  - Not full whitelist, just audit mode
  - Capture execution of items that would have been blocked
  - Can easily separate out executables and scripts
  - Can focus on execution of unsigned code
- Logs to the local system
  - Need to collect these logs centrally
  - Would like to filter out low value events
  - Keeping with low touch approach, can achieve without additional software

Leveraging Windows Capabilities

- Windows Event Forwarding
  - Method to collect logs without an agent
  - Rollup to servers controlled by security
  - Filtering on endpoint prior to forwarding
- Simple configuration for rapid deployment
  - Windows domain and a Windows server to collect events
  - Group Policy settings to govern WEF
  - Endpoints configured to push events to collector

Security: AppLocker unsigned scripts redacted

timestamp	hash	files	client	count
2017-11-22 09:41:00	EE454D43D799F1851EFF2DFE29CFD72DE6A5A2453AC718CF03E9546440CD61CC	%OSDRIVE%\ORACLE\PRODUCT\10.2.0\CLIENT_1\BIN\OEMAPP.BAT	56300ffe	1
2017-11-22 08:58:38	D7C4E6C74B88E0F1CBC360855C87B9247AEA072CF961AA9701B04DFB0E52BB40	%OSDRIVE% .APPDATA\LOCAL\TEMP\I4J465054996344113606.BAT	95ec7700	1
2017-11-21 16:21:33	4120A510DEA4D4A442F9433B2666539882411E5D2F51B82386564D4B84E3EFB2	%OSDRIVE% .OCUMENTS\SHOW1.BAT	c09567ab	1
2017-11-21 12:29:49	37B9BDFEA860FAE8F4802D5C3FF96C666DE78D1E34A420A7664A97F543D32357	%OSDRIVE% .DOCUMENTS\CZYRS.BAT	c09567ab	1
2017-11-21 11:56:05	AC49920E8063EF2A0BFE6C96A00C4D6480F1B90730927A7DC16A4EC52F887097	%OSDRIVE%\PROGRAMDATA\WATERS\ELN EMPOWER INTERFACE\ELN-EMPOWER INTERFACE - TEST.BAT	f518d94d	1
2017-11-21 11:55:59	AFD61CCF87ECA120A9D321CC0CC7F2E1B129A8B1DE16CD9AA4D5B4E5D296391A	%OSDRIVE%\PROGRAMDATA\WATERS\ELN EMPOWER INTERFACE\ELN-EMPOWER INTERFACE - PRODUCTION.BAT	f518d94d	1
2017-11-21 10:21:06	FBE5B229955CEF86CA8D66FDC8105073218B12B7FB3F14FADF3578AC97D6CFE9	%OSDRIVE% .\DOCUMENTS\SENT.BAT	c09567ab	1
2017-11-21 03:16:31	EE32351103DFD4A431125E05ADACEF4DD4147B263D2D945CE6F69F291331137F	%OSDRIVE% .DESKTOP\MARSAPI_PROXY BRANCHES\DEV\TESTS\RUNTESTS.CMD	39186a1d	1

Security: AppLocker unsigned executables redacted

timestamp	hash	files	client	count
2017-11-21 15:53:02	19ED48980C188F7A1A2A70903EBE71763C9905F8ABDDEE066F4F87B0E138BE05	%OSDRIVE%\ ' PPDATA\LOCAL\TEMP\IS-H41AD.TMP\CONSOLEPLUSSETUP.TMP	5c607e97	1
2017-11-21 15:53:01	E24B2067CC8946BE3A6C5178DBC3735EB79DB2E0E7FD06BDED99F545EE4D5C5B	%OSDRIVE%\ DOWNLOADS\CONSOLEPLUSSETUP\CONSOLEPLUSSETUP.EXE	5c607e97	1
2017-11-21 07:47:38	C2A4472BCC510CC624C0D100304A4520E49A79E87EB9327AEB32AB86655AD82E	%OSDRIVE%\EAGER FOR FLASH\EAGER 300 FOR EA1112.EXE	5e3c84b8	1
2017-11-21 07:47:36	FA70B976898E4BE596095CDA72868A978D6C6C36D17D38FEB27B6FCE971DD1F2	%OSDRIVE%\EAGER FOR FLASH\EA1112.EXE	5e3c84b8	1
2017-11-20 15:14:00	28FA38F092AC7A26E26E49FD0D157AADF0783B6CEF1A2125B8F42FDFEA63777C	%OSDRIVE%\BRUKER\TOPSPIN3.5PL6\PROG\MOD\DECON.EXE	1a0e721c	1
2017-11-19 20:22:45	6976BEF0720C7DC4C584963B7D3D45EE06ED641D4D495D2FC9D4670A929A20B5	%OSDRIVE% \DOWNLOADS\FREEMIND-WINDOWS-INSTALLER-1.0.0-MAX-JAVA-INSTALLER-EMBEDDED.EXE	1dbd24d8	1
2017-11-19 12:41:33	102168237B386299152AD10AFEB4ECC20579A59B713ABABB2C1C73A717E673C7	%OSDRIVE% .SABRE RED WORKSPACE\SETTINGS\J34I_1234\JDIC_FILES\IEEMBED.EXE	045b4ca8	1
2017-11-16 15:22:15	2A6BF35D7025F677720B566759CF0A72BAE79D61FC719F42AD8FA247424DD355	%OSDRIVE%' .\PPDATA\LOCAL\MICROSOFT\WINDOWS\TEMPORARY INTERNET FILES\CONTENT.IE5\NAEE85JD\WINFFSETUP.EXE	cc07eb0d	1

AppLocker detected signed execution

filename	name	product	imagename	version	hash
CHROME.EXE	GOOGLE INC	GOOGLE CHROME	CHROME.EXE	61.0.3163.100	733F158FDA371E04E649CCB4A695190140B6B3F59C99AC72B79A9CB6557C4A53
CONCENTR.EXE	CITRIX SYSTEMS, INC.	CITRIX ICA CLIENT	CONCENTR.EXE	13.1.0.89	C1F08A97860E0F9146DECD6899AAD1DA0CB94A299619392CD0EF894757B1F261
SELFSERVICEPLUGIN.EXE	CITRIX SYSTEMS, INC.	CITRIX RECEIVER	SELFSERVICEPLUGIN.EXE	3.1.0.21744	D88E1260B597F246A9C3D27CDC15EA6E35923C949282791FC77CCC4C662E9512
G2MUPLOAD.EXE	LOGMEIN, INC.	GOTOMEETING	G2M.EXE	8.16.0.7856	AB1DB4436C9B5A433EC45D49BE4978F9D5230082F18FBE219988259DCF3C4C91
GOOGLEUPDATE.EXE	GOOGLE INC	GOOGLE UPDATE	GOOGLEUPDATE.EXE	1.3.33.05	7BDA8C4B183E75D2822E51050BBA92EBE22F4A1B3219B01ED9BA86D1F8831FFC
UTILITYFUNCTIONS.PS1	MICROSOFT CORPORATION		UTILITYFUNCTIONS.PS1	0.0.0.00	886A625F71E0C35E5722423ED3AA0F5BFF8D120356578AB81A64DE2AB73D47F3
TS_BROKENSHORTCUTS.PS1	MICROSOFT CORPORATION		TS_BROKENSHORTCUTS.PS1	0.0.0.00	354F7D8D44FC598F469343CF64458F477C561E4E47580FF4AA85C9D2AE501110
TS_UNUSEDDESKTOPICONS.PS1	MICROSOFT CORPORATION		TS_UNUSEDDESKTOPICONS.PS1	0.0.0.00	6A199A65B6165B3683AFA060E225A4E972379CD4F11ACF0BE6B21B931983637F

Windows account lockouts

Account	Source	Lockouts	Last occurrence
TM	L-J0000021	14	2017-11-22 07:57:44
WV	DESKTOP-RO2Y01R	14	2017-11-22 05:42:20
HAL	JOHNATHON	19	2017-11-22 04:21:48
EVE	\\INA	5	2017-11-21 15:31:44
inge.clare	L-10WS0P1	2	2017-11-21 14:24:39
YUK	KELI-0002	1	2017-11-21 12:50:44
hee	HWA	7	2017-11-21 11:24:19
LIZ	\\INA	1	2017-11-21 11:07:05
janee.johnnie	DUBMN2	2	2017-11-21 10:55:02
SON	OUVXRZ0	1	2017-11-21 09:48:10

Windows group membership changes

Change Date	Changed By	Action	Username	Group Name
2017-11-21 19:35:26	MAE_AD\jarod	Added [Universal]	Lorna O'Erlene	TZ_FIN-RONA
2017-11-21 19:35:26	MAE_AD\jarod	Added [Universal]	Lorna O'Erlene	TZ_GALA
2017-11-21 19:35:26	MAE_AD\jarod	Added [Universal]	Lorna O'Erlene	TZ_SALES
2017-11-21 16:51:03	MAE_AD\jarod	Added [Universal]	Verna B. Danica	MQ_JONA
2017-11-21 16:51:03	MAE_AD\jarod	Added [Universal]	Chante Madonna	MQ_JONA
2017-11-21 16:51:03	MAE_AD\jarod	Added [Universal]	Rosalyn Alejandro	MQ_JONA
2017-11-21 14:05:37	ME\SAM	Added [Universal]	Omega Trzql0	G_SU
2017-11-21 13:34:09	ME\dud.lakendra	Added [Universal]	OyyqqKmfds	TI_OLINDA
2017-11-21 10:55:48	ME\OXFBA1$	Added [Universal]	Tosha Isidro	MARLON
2017-11-21 09:04:30	ME\howard.latina	Added [Universal]	Solange K. Kelli	ZSDSaduo

Windows account creation

Created	Created By	Login ID	UPN	Display Name
2017-11-17 11:49:50	AU\TZSAS0$	AU\tessa.kurt	tessa.kurt@IDA.org	Tessa Kurt
2017-11-17 11:48:39	AU\TZSAS0$	AU\kieth.octavio	kieth.octavio@IDA.org	Kieth Octavio
2017-11-15 12:54:38	AU\TZSAS0$	AU\inge.duxggoqgwcyc	inge.duxggoqgwcyc@IDA.org	Inge Duxggoqgwcyc
2017-11-14 17:08:33	AU\TZSAS0$	AU\melba.zvcoteouifet	melba.zvcoteouifet@IDA.org	Melba Zvcoteouifet
2017-11-14 16:53:49	AU\TZSAS0$	AU\isa	isa@IDA.org	Jesse Alex
2017-11-14 16:50:38	AU\TZSAS0$	AU\phebe.lasonya	phebe.lasonya@IDA.org	Phebe O'Janise
2017-11-14 16:49:30	AU\TZSAS0$	AU\vanna.ud	vanna.ud@IDA.org	Vanna Ud
2017-11-13 15:19:19	AU\TZSAS0$	AU\earnestine.jacquie	earnestine.jacquie@IDA.org	Earnestine C. Jacquie
2017-11-13 13:23:22	AU\TZSAS0$	AU\sally.natalie	sally.natalie@IDA.org	Sally Natalie
2017-11-13 12:22:29	AU\TZSAS0$	AU\leonardo.tiera	leonardo.tiera@IDA.org	Leonardo Tiera

Windows account deletion

Deleted	Deleted By	Login ID
2017-11-20 14:28:51	BA\ISA	maurine.willette
2017-11-20 14:28:47	BA\ISA	troy.jacques
2017-11-20 14:28:43	BA\ISA	alysa.dionne
2017-11-20 14:28:37	BA\ISA	judy.couch
2017-11-20 14:28:31	BA\ISA	nerissa.maira
2017-11-20 14:28:28	BA\ISA	isidra.clementine
2017-11-20 14:28:21	BA\ISA	ela.deandrea
2017-11-20 14:28:17	BA\ISA	santo.julieann
2017-11-20 14:28:13	BA\ISA	julius.lashonda
2017-11-20 14:28:08	BA\ISA	lekisha.eugenio

Windows password resets

Reset	Reset By	Login ID
2017-11-21 16:08:05	VZ\JEN	VZ\TXWFVPRDIPSYFR
2017-11-20 16:35:43	VZ\lavone.norris	VZ\NM
2017-11-20 15:48:26	VZ\ALI	VZ\TED
2017-11-20 13:57:08	VZ\ALI	VZ\ENA
2017-11-20 13:55:36	VZ\ALI	VZ\LIN
2017-11-20 13:22:12	VZ\ALI	VZ\CUC
2017-11-20 11:35:55	VZ\JEN	VZ\EUN
2017-11-20 07:32:27	VZ\HUI	VZ\KIT
2017-11-19 17:22:39	VZ\XXQRJ0$	VZ\melany_0d2jn3eol2104
2017-11-18 17:53:59	VZ\KATELYNN$	VZ\EgkklmLsqhcfb1v8um03

Minimally Invasive Logging

- DNS logging
  - Performance concerns regarding debug logging in Windows DNS server
  - DNS audit and analytic event logging available if debug logging an issue
- DHCP logging
  - Need to change the default log size of 70 MB total (10 MB/day)
  - DhcpLogFilesMaxSize registry key needs to be modified
    - HKLM\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters
- Unable to collect DHCP or DNS debug logs via WEF
  - Logging agent required, but only on a few hosts

DNS: Long query names

length	type	query
227	A	f5rk3hvwcvoah6gincwldux2mih52tcbejeryj335nh6im7s.n2djovcdti2chtyxk2f5mjdtlmy6hltxk6aj2nswj4gw5w37.2hyq7t5t3epkhag2
227	A	f25eiz7eozbyj4uhtts3ld2yi4y5vvz67virb25gfjkglgki.wwrav7oyb5ycga6fcillb74rwxfua5ke5ieprp4ytkywgzdy.p3tk6ggogcdfijstcpmoo
82	A	andr-c2356069e9-968e2d5b08687bf4-acd02e8ea2c861f00d-1131470.na.api.amazonvideo.com
82	A	andr-c2356069e9-968e2d5b08687bf4-c5841ef24d99462e85-1131470.na.api.amazonvideo.com
80	A	dualstack.awseb-e-d-awsebloa-1a537iy2fffgy-238588516.us-east-1.elb.amazonaws.com
80	A	dualstack.awseb-e-j-awsebloa-yfxnb5rgajcj-2076400972.us-west-2.elb.amazonaws.com
77	A	p4-bns7mflymzya4-d6ikppcvql3vogkx-231436-i2-bogus-dnssec-vd.gexperiments2.com
77	A	p4-bns7mflymzya4-d6ikppcvql3vogkx-231436-i1-bogus-dnssec-bd.gexperiments3.com
77	A	user-platform-infinityid-prod01.us-east-1--production.containers.aws.conde.io
76	A	j8ck72di-a5b649176b1db383b05c5dd3c761c7d793ef982d-sac.d.aa.online-metrix.net

tld	count
agency	2
bj	2
caixa	2
comoffers	2
date	2
dhl	2
dog	2
ir	2
lat	2
market	2

tld	count
io	6704
tv	3522
co	1720
home	1314
uk	918
local	670
us	468
jp	432
fi	414
to	378

DHCP redacted

Edit | Export | ...

DHCP client count

2,336

DHCP first seen today

Timestamp	client	MAC
11/22/17 07:30:53	redacted.domain.tld	F8CAB85B240E
11/22/17 03:46:43	redacted.domain.tld	94D4690A1D6A
11/22/17 00:44:34	redacted.domain.tld	34F64B9F32A1
11/21/17 13:12:08	redacted.domain.tld	34F64B7E6B6B
11/21/17 11:37:02	redacted.domain.tld	A434D9FBCBEC
11/21/17 11:01:00	redacted.domain.tld	F0D5BF60448D
11/21/17 10:08:50	redacted.domain.tld	184F32F14E73
11/21/17 10:03:59	redacted.domain.tld	F48C50A13542
11/21/17 10:02:55	redacted.domain.tld	4845208FB33A
11/21/17 09:14:00	redacted.domain.tld	4851B719113A

Increased Insight vs Increased Impact

- Options for more intrusive actions
  - New software rather than a configuration change to capture specific data
  - Prioritize domain controllers, critical Windows servers, high-value endpoints/users
- Sysmon
  - Detailed tracking of processes, network connections, and file ops
  - Install driver and install XML configuration file, events sent to local Operational log
- Feature updates required to get new functionality
  - PowerShell logging features in version 5

Gap Acknowledgement

- Missing some things
  - Remember constraints from earlier
- No endpoint security logs
  - Centralized solution needed some maintenance
- No proxy logs
  - Coincidentally, not using a web proxy
- No IDS logs
  - No solution deployed at the time

Sad But True

Alignment to Critical Security Controls

CSC	Description	System feature/setting
1.2	DHCP logging	Windows DHCP logging
2.3	Software inventory tool	Windows AppLocker
3.7	System configuration management	Windows Group Policy
5.4	Logging of changes to privileged groups	Windows Auditing
5.5	Logging of unsuccessful logins to administrative accounts	Windows Auditing
6.3	Adequate space for logs	Windows Group Policy
6.4	Reports to identify anomalies	SIEM / Analytics
6.5	Configure network devices to log	Device specific

Case Study Conclusions

- The organizational objectives were achieved using the CSC
  - Achieved the short-term tactical goal of security visibility
  - High-value, actionable data collected
  - Minimal requirement for non-security IT resources
  - Minimal impact on the user community
  - Provides a framework for current and future security initiatives

Fade to Black

The End of the Line

Questions?