

Empowering a Small Security Team

October 26, 2016

Meet Your Panelists



Kelly Brazil
VP of Systems Engineering
ProtectWise



Richie Field
IT Infrastructure and
Security Coordinator
Hoosier Energy

It's Interactive



Please submit your questions through the control panel to get answers LIVE from our panelists.



It's Hip to Chat

EnergySec is hosting an online chat to accompany this webinar which is open to all registered EnergySec Community participants.

To join the chat as a guest, visit:

<https://hipchat.energysec.org/g0kGNyQRW>

If you have a HipChat account already, join us in the room titled, EVENT: EnergySec Webinar Chat. Note: Registered users have access to the chat history, file attachments, and links.

Agenda

Challenges
Small Teams
Face

ProtectWise
Demo

Q&A









PROACTIVE

REACTIVE

Security Analytics Goals

Goal 1: Warp Time

Goal 2: Cut the noise

Goal 3: Focus



Scale The Advanced Humans!

The Analytics Kill Chain



Reconnaissance

Attacker locates a security gap



Delivery

Attacker delivers malicious payload



Exploit

Victim executes malicious payload



Beaconing

Infected host phones home



Command & Control

Attacker takes control of victim host



Fortification

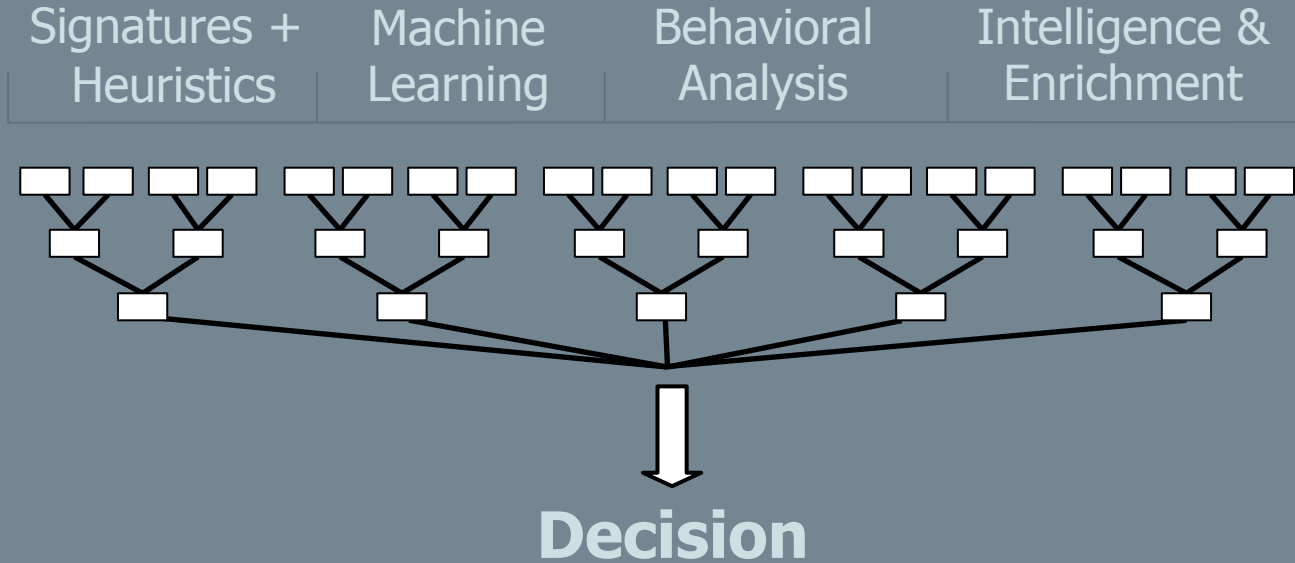
Lateral movement and entrenchment



Actions on Objectives

Data Theft

Analytics Framework



Signatures

Example: Bedep

IDS Signature:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"Bedep HTTP POST CnC Beacon";  
flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri;  
fast_pattern:only; content:! "Content-Type|3a|"; http_header; content:"Accept|3a 20|text/html,  
application/xhtml+xml, */*|0d 0a|"; http_header; pcre:"/\\.php(?:\\?[a-zA-Z0-9=&]+)?$/U"; pcre:"/^[a-  
z]+\\d*=(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}=|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4})(?:&[a-z]+  
\\d*=(?:[A-Za-z0-9+/]{4})*(?:[A-Za-z0-9+/]{2}=|[A-Za-z0-9+/]{3}=|[A-Za-z0-9+/]{4})){2,}$/P";  
pcre:"/^(?:Connection\\x3a[^\\r\\n]+\\r\\n)?Accept\\x3a[^\\r\\n]+\\r\\n(?:Accept-Encoding\\x3a[^\\r\\n]+\\r\\n)?  
Accept-Language\\x3a[^\\r\\n]+\\r\\n(?:Referer\\x3a[^\\r\\n]+\\.php[^\\r\\n]*?\\r\\n)?User-Agent\\x3a[^\\r\\n]+(?:  
MSIE |rv\\x3a11)/Hi"; classtype:trojan-activity; sid:2021418; rev:8;)
```








File Signature (hash):

ef0503a22a0a359bcb82ff2ef57907a0b2cabf3a145b661d053d42fba712a073



Signatures in Real Life

Kill Chain Coverage

Recon	Delivery	Exploitation	Beacon	C2	Fortification	Theft
						

Very good at detecting known exploits

Very bad at detecting 0 days – ***Unless you save PCAP***

Prone to false positives

Not so good with encrypted traffic

Tired, but not dead

Heuristics

... any approach to problem solving, learning, or discovery that employs a practical method not guaranteed to be optimal or perfect, but sufficient for the immediate goals ...

Host Based Heuristics

Combination of Signatures / Detonation / Static Analysis

Prone to False Positives

Can be slow

Simple Network Heuristic: port scanning



TTPs

Tactics Techniques and Procedures

Phishing Sigs + Malware Used + Infrastructure Cues








Create a behavioral profile and code as analytics logic

Often Implemented by SIEM as heuristics on logs

Can cover the entire killchain

Heuristics in Real Life

Kill Chain Coverage

Recon	Delivery	Exploitation	Beacon	C2	Fortification	Theft
						

Effective at reducing noise – SIEM

Helped security products move past signature based AV

Limited by their design and predetermined logic

Require constant update

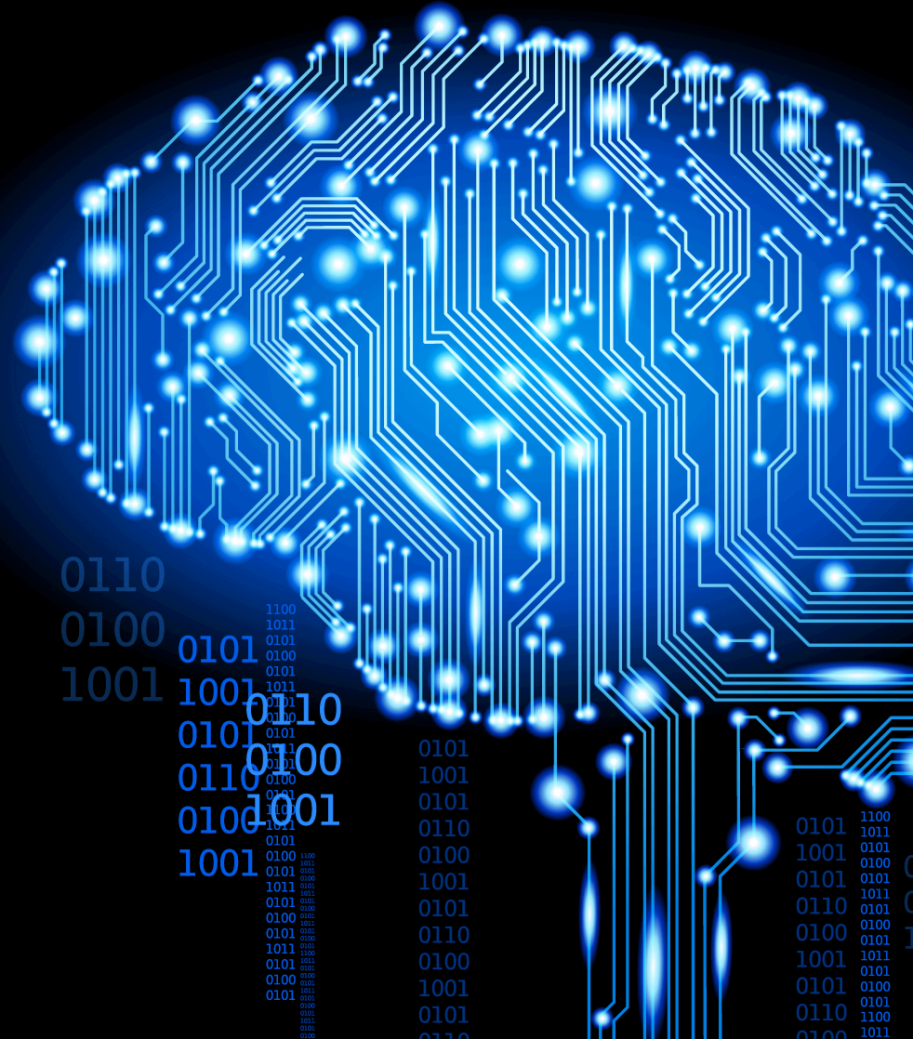
ML Example: DGA

Distinguish Legit domain from
Algorithmically Generated domain

facebook.com





vs.

bysxkmhxikr2.com



ML in Real Life

Kill Chain Coverage

Recon	Delivery	Exploitation	Beacon	C2	Fortification	Theft
						

Resilient to zero days

Does not require white list, black list or notary service to be effective



Shines a light on encrypted traffic

Require retraining

Can be “falsey”

Behavioral Analysis in Summary

Kill Chain Coverage

Recon	Delivery	Exploitation	Beacon	C2	Fortification	Theft
						

Able to detect zero days

Provides clues to data theft

Must account for periodicity

Requires burn in period

Over sensitive to change

Often suffers from false negatives



Intelligence and Context

Intel Sources Abound

Commercial




Open Source

All require active curation



Intelligence In The Real World

Kill Chain Coverage

Recon	Delivery	Exploitation	Beacon	C2	Fortification	Theft
						


Good at highlighting known compromised hosts and known infrastructure

Subject to rapid change

Targeted Intel is labor intensive

Sharing still ... not so good

Prone to false positives due to becoming stale



PROTECTWISE

13:16:06

Wed 02:17:2016

ADMIN

EVENTS

OBSERVATIONS

New

Priority

Assigned to me

Resolved

All

TIMEFRAME: ALL

PRIORITY

TAG

IP ADDRESS

EVENT NAME

KILLCHAIN STAGE

THREAT CATEGORY

ASSIGNED TO: None

EVENT STATE: Open

RESOLUTION

EVENT TYPE

THREAT LEVEL

THREAT SCORE RANGE

FOUND RETROSPECTIVELY

SENSOR

Jim Treinen

(as threat)

02:08:38

HUD

KILLBOX

126 EVENTS

OCURRED · NEWEST FIRST

NOW 15	55 JS/Nemucod requesting EXE payload 2015-12-01	Malicious Conversation	Yesterday at 11:41:21	4
SAT 13	55 Pommocup HTTP Request (generic) M8	Malicious Conversation	Yesterday at 11:41:14	2
TUE 11	55 Connection to Suspicious Domain 'bysxkmhikr2.co...	Malicious Conversation	Yesterday at 11:41:08	15
TUE 08	55 Bedep HTTP POST CnC Beacon	Malicious Conversation	Yesterday at 11:41:08	3
FRI 07	55 Bedep HTTP POST CnC Beacon	Malicious Conversation	Yesterday at 11:41:08	2
FRI 05	55 Bedep HTTP POST CnC Beacon	Malicious Conversation	Yesterday at 11:41:08	3
WED 03	55 Beaconsing Host: 10.52.95.56	Compromised Host	Yesterday at 11:41:08	7
WED 03	55 Connection to Suspicious Domain 'elqzbhkwptcunb...	Malicious Conversation	Yesterday at 11:41:08	4
FRI 31	48 Angler encrypted payload Nov 23 (4)	Malicious Conversation	Yesterday at 11:41:08	6
FRI 29	45 Targeted Host: 10.52.95.56, Repeat Exploit Attempts	Compromised Host	Yesterday at 11:41:08	6
WED 27	60 Alphacrypt/TeslaCrypt Ransomware CnC Beacon R...	Malicious Flow	Yesterday at 11:40:58	3
NOW 23	60 Attack Progression on Host: 10.240.66.37	Killchain Escalation	Yesterday at 11:40:58	4
SAT 23	45 Angler EK Landing Dec 10 2015 M1	Malicious Conversation	Yesterday at 11:40:58	7
TUE 21	40 Malicious Redirect Leading to EK Apr 03 2015	Malicious Conversation	Yesterday at 11:40:58	2
TUE 18	45 Targeted Host: 10.240.66.37, Repeat Exploit Attem...	Compromised Host	Yesterday at 11:40:58	6
	55 Pommocup HTTP Request (generic) M8	Malicious Conversation		

EXPLORER BETA

SITREP

SETTINGS

PCAP DOWNLOAD

55 Connection to Suspicious Domain 'bysxkmhikr2.com' by Host: 10.52.95.56

Malicious Conversation

START / END TUE 02/16/2016 11:41:08 - TUE 02/16/2016 11:41:08

OBSERVED TUE 02/16/2016 11:41:24

02/16/16 11:41:08

DNS 168 B Sensor 2

Malicious Domain: bysxkmhikr2.com DNS REP

Machine Generated Domain Name: ... DNS REP

HTTP 51B Sensor 2

Malicious URL: bysxkmhikr2.com/al... URL REP

Bedep HTTP POST CnC Beacon PAYLOAD

Bedep HTTP POST CnC Beacon PAYLOAD

Malicious URL: bysxkmhikr2.com/inc... URL REP

HTTP 171 kB Sensor 2

Malicious URL: bysxkmhikr2.com/wl... URL REP

Malicious URL: bysxkmhikr2.com/inc... URL REP

Bedep HTTP POST CnC Beacon PAYLOAD

DNS 168 B Sensor 2

Malicious Domain: bysxkmhikr2.com DNS REP

Machine Generated Domain Name: ... DNS REP

DNS 168 B Sensor 2

Malicious Domain: bysxkmhikr2.com DNS REP

Machine Generated Domain Name: ... DNS REP

HTTP 21B Sensor 2

Bedep HTTP POST CnC Beacon PAYLOAD

Malicious URL: bysxkmhikr2.com/for... URL REP

10.52.95.56

8.8.8.8

95.211.205.229

C2 via Intel

Beacon via Sig

Beacon via ML

Recon via Intel

Jim Treinen

(as threat)

02:08:38

Bending Time



Punch Above Your Weight



-Demo -

Q&A



Thank You

Kelly Brazil
kelly.brazil@protectwise.com

