Taming your indicator consumption pipeline

Presented by:
Ryan Stillions – Vigilant LLC.

http://www.vigilantnow.com
Ryan Stillions
rstillions@vigilantnow.com
@ryanstillions
ryanstillions.blogspot.com

Incident Detection & Response

Operationalizing threat intel …at scale.

faith, family, horses, camping, fishing

Vigilant’s charity partners:

New Oaks Community

Back2Back Ministries
I’ve got 99 problems and a lack of indicator feeds ain’t one of ‘em

- Intel
- Prevent
- Detect
- Respond

Era of Prevention
Era of Response
Era of Increased Visibility
Era of Intelligence
Era of Clarity & Focus
The cost of context (re)construction

Construction of context

Risk

Intel

Response

Deconstruction of context

Threat Intelligence Platform

Reconstruction of context & compare

Tool A

Tool B

Tool C

Alerts

Detect Ops

$$>=$$
WHAT THE ADVERSARY WANTS

HOW THE ADVERSARY PLANS TO GET IT

TTPs

EVIDENCE LEFT DURING OR AFTER THE ACT

GOALS

STRATEGY

TACTICS

TECHNIQUES

PROCEDURES

TOOLS

HOST & NETWORK ARTIFACTS

ATOMIC INDICATORS
Only consume the right stuff

Get good at deploying it

So gear doesn’t blow up & Analysts won’t kill us
1. Raw Data

All tactical indicators
- Internal sources
- External providers

“disseminated” intel

IT’S JUST RAW DATA
Can you act on this if you wanted to?

Know your tech stacks.

How they consume TI.

API? UI?

Identify consumption gaps & close them
What must you detect?
vs. what you’d like to?
vs. why bother?

Forces you to prioritize what’s important

Aligned to your Detection Objectives?
Shelf life matters!

Standing order…

Keep until…

Was good between…

Forces you to evaluate temporal accuracy
Capture your Go / No-Go consumption choice

Decide to take action

Keep track of who/when/why decisions

From here forward things get operationally costly
Only consume the right stuff
Raw Data becomes detection logic

One – to – Many transformation

Network controls & NSM
Host controls & LR
Event Log - SIEMs
Other stuff

Ensures deployment to all possible places
The point of no return...

These are your indicators

This is your detection logic

Don’t consume detection logic as source intel
Content Management

Develop draft detection logic for each platform

Input Lists
JSON data structures
Detection Signatures

Source Controlled with revision tracking

Document it all till you puke, then do it again!
Stop looking for everything everywhere

Deploy based on host & network placement.

Ingress/egress, DMZ, Internal, VPN, 3rd Party

Only put the right stuff, in the right places
2. Fielded

Ready, FIRE, aim!

< 15 minute burn in under realistic load

Avoid DOS’ing yourself

Detection Brownouts

Testing reduces the chances of disruption
Ship it… Danno!

Track *where* and *when* detection logic hits

Varying stages of ‘deployed’

Know your deploy times for all systems

This captures your Go / No-Go deployment choice
Get good at deploying it
So we’re done, right?

This represents everything you have ever deployed to production… ever

When was the last time you tuned it?

You can’t just keep deploying stuff forever…
3. Maintained

How hot do your systems run?

Detection technology has upper limits, find them
Detection Efficacy

Shift focus to the end customer…

The analyst

TP/FP Ratio & “Precision”

Chris Sanders’ Blog on “Precision”

Only detect what we intended to, while balancing detection efficacy
3. Maintained

0

1

Performant

2

Efficient

3

Relevant

Only alert on what’s absolutely necessary

Analysts’ time is precious
Don’t waste it

Good analysts will hunt

Reduce the Cost of Context Reconstruction!
Final Product

Performant systems

Efficient detection logic

Relevant & actionable alerts

more signal, less noise
So gear doesn’t blow up & Analysts won’t kill us
Building the pipeline...

What systems manage these tasks in your org?
The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency.

(Bill Gates)
Build out the capability equally across all three phases
Mature them in parallel

Be mindful of your sourcing model

Hybrid Sourcing

Raw Data

Fielded

Maintained

1. Actionable
2. Prepared
3. Performant
4. Accurate
5. Localized
6. Efficient
7. Timely
8. Tested
9. Relevant

Inherently unique to your organization
What most people think it looks like
Ryan Stillions
rstillions@vigilantnow.com
@ryanstillions