Taking Your Detection Program To The Next Level

CARSON ZIMMERMAN

SANS VIRTUAL EVENT OCTOBER 2020

About Carson

- Worked in Security Operations for >15 years
- SOC investigations team lead @ Microsoft
- Previously SOC engineer, analyst & consultant @ MITRE
- Check out my book if you haven't already: https://www.mitre.org/publications/all/ten-strategies-of-a-world-class-cybersecurity-operations-center

Not speaking on behalf of my employer, past or present; any opinions expressed are my own.

What Customers Think

Data collected by SOC == Totally Monitored

Our Reality

	Generation	Collection	Storage	Detection	Analysis & Response
Host OS	✓	✓	✓	✓	✓
Services & Applications	✓	✓	✓	✓	✓
Network	✓	✓	✓	✓	✓

It takes a lot more than just collecting some data for a customer to be monitored!

There's too much to do

Too many types of systems

- Cloud
- IoT
- Mobile
- Non-Windows

Too many detections

- Across kill chain
- Across device types
- Generic vs customer-specific

On Prem	IaaS	PaaS	SaaS
App	**App**	**App**	App
Data	Data	Data	Data
Runtime & Middleware	Runtime & Middleware	Runtime & Middleware	Runtime & Middleware
OS	**OS**	OS	OS
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

The ways we lie …and the outcome

- Collecting data without setting expectations
- Thinking you will create detections for all the things
- Running detections without testing them
- Putting one sensor in one location and calling a customer "monitored"

- Customers think monitoring is happening when it isn't
- Never enough time & resources -> never gets done
- Detections don't work
- Major blind spots remain

TL; DR:

Don’t lie

Don’t reinvent the wheel

Outline

- **Engage** the customer
  - Formulate a shared sense of situational awareness
  - Perform purposeful planning for monitoring, detection, analytic investments
- **Leverage** everything you can, especially commodity solutions
- **Create** and **maintain** detections and analytics using consistent, accurate methodology
  - Test them to make sure they're working
- **Measure** coverage along four dimensions

Routine Customer Engagement

From the customer:

- Changes in the business
  - New/expanded/changed services
- Business context, criticality, risk
- Input on investments: scanning, monitoring, hygiene, detections

From the SOC & security org

- "what have you done for me lately"
  - New sensor deployments
  - New detections/use cases
  - Threat/campaign/incident insights
- Hygiene/compliance status
- New metrics and asks

“Standard” customers get:

- Low cost network perimeter protections
- EDR
- Standard set of SIEM analytics & detections
- Semi-annual engagement
- Standard set of hygiene controls

“Special” customers get:

- Everything standard customers have, plus…
- >= Quarterly engagement
- EDR “low fi” detections turned on
- Handful of environment specific detections
- Potential “deputization” of detection & analytic creation
- Direct access to their slice of data

https://fr-en.openfoodfacts.org/product/0037600106252/peanut-butter-skippy
https://creazilla.com/nodes/28411-simple-snowflake-clipart

Building Situational Awareness & Differentiated Value

Detections & Analytics

Instrumentation Strategy & Data Collected

Technological Environment

IT
OT
Mobile
Cloud

Data

On prem
In cloud
Mainframe
Endpoint

Mission

Risks
Threats
Owners
Priorities
Consequences

Regulatory Environment

Laws
Compliance

Threat

Internal
External

SOC & Customers

Plan

- Routine planning: quarter, semester, annual
- Work tracking: Azure DevOps, JIRA, etc.
  - Stack priority/rank: make this live data shared with the customer
  - New ask? New work item. Make a list and keep it.
  - Don’t get randomized!
- Consider Agile scrum, DevOps or something like it

Leveraging Others' Work

- **Host**: use an EDR
  - Collect OS data "by hand" only when necessary
  - More on following slides
- **Network**: Zeek scripts, Suricata detections
- **SIEM/big data**: CAR, Sigma, vendor marketplace/ github
  - Customers' data in place without backhauling it
- **Cloud**: demand customers enable built-in detections & log collection
  - Dozens of different cloud resource types & growing fast
  - Broad use of DIY detections completely infeasible

Example

You need rich host telemetry:

- Process creation events
- Network connection events
- Auth/directory/login/logout
- Service/kernel/driver/OS/ device changes
- Storage & USB events
- User/group changes
- RPC, scripting actions

You could…

- Deploy WEC/ETW/sysmon/ auditd collection for > 200 event types
- Tune audit policies and WEC subs
- Stand up & tune log management / SIEM
- Write & tune >500 detections

https://www.needpix.com/photo/1316340/snow-shoveling-man-shovel

Oooor…

- Buy an EDR
- And Deploy it
- …
- Profit!

- *Might* cost less $$$, when accounting for labor
- Gets most of the important telemetry ”manual” collection gets
- Huge detection library
- Possibly a better user experience

https://www.needpix.com/photo/1308810/snow-winter-blower-machine-clearing

Focus

- Don't write generic detections
  - Leverage an existing platform & detection library!
- Spend your cycles for what's specific to your environment
  - Custom apps
  - Specific customers
  - Known scenarios that should never occur
  - Specific incidents from your past & partners/competitors
  - Inspired by hunt: hypotheses, traps, findings

Detection Metadata

- Title
- ID
- Created by
- Created on
- Last modified by
- Last modified on
- Status (not started, dev, prod/active, retired, prod/deactivated)
- Required source telemetry
- Customer scope: global, specific named services
- Asset scope: Windows, Linux, Mac, Cloud, OT
- Intent
- Known false positives
- What to do next
- Kill chain
- ATT&CK framework tile ID and tile name
- Notes/discussion

Keeping Detection Tracking Accurate

Observation: detection metadata, tracking drift from what's in prod

Consider:

- Parent/child relationships to overall detection work tracking (epic/feature/user story/etc.)
- Surface detection IDs in alerts that fire
  - Join alert IDs against detection metadata, look for discrepancies
  - Enrich fired alerts with detection metadata: analysts will miss it when it's not there, drive closing gaps that pop up
- Use CI/CD to push detection code from repo to production, where possible (think: functions in big data "query on a timer" and NRT detection systems)

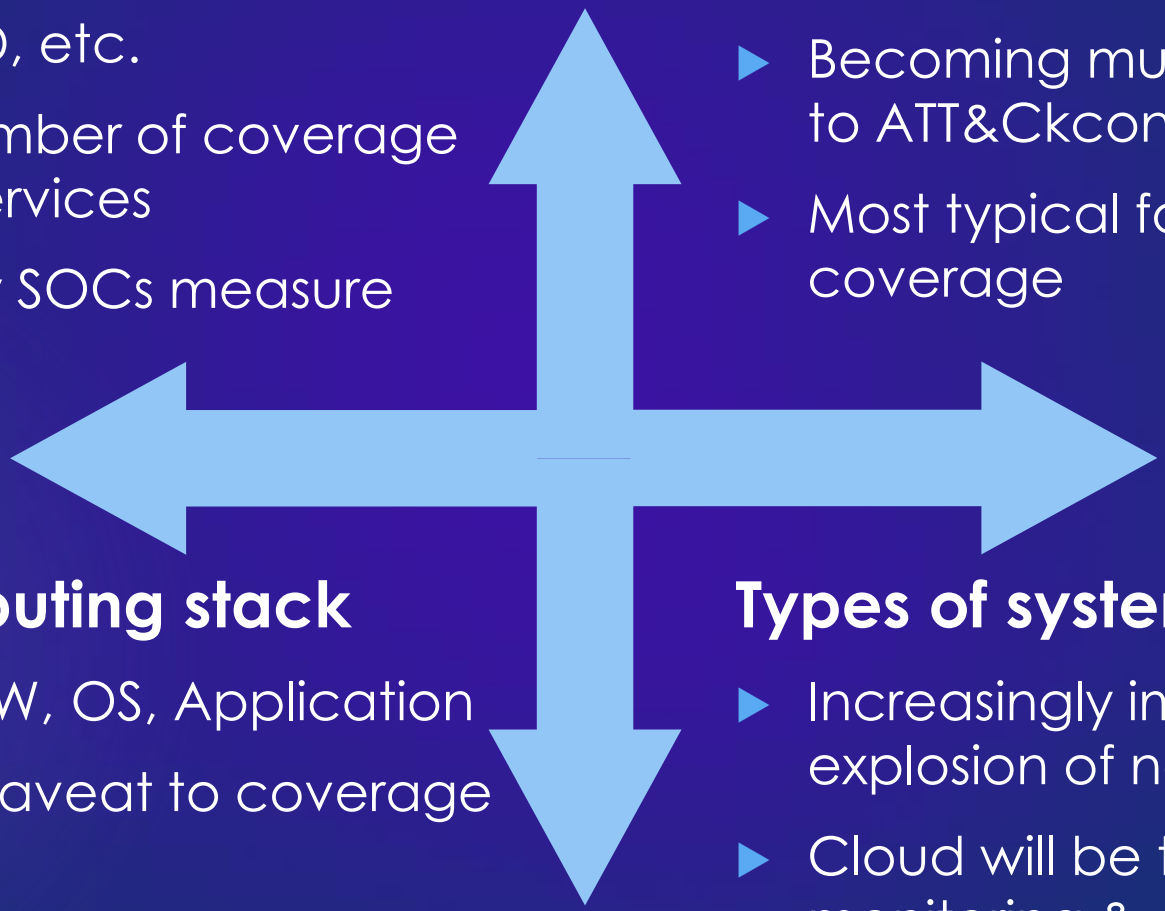
Measuring Coverage

Breadth of systems and enclaves

- Customer A, B, C, D, etc.
- % and absolute number of coverage by known assets, services
- Most common way SOCs measure coverage

ATT&CK & kill chain coverage

- Becoming much more common thanks to ATT&Ckcon, EDR evaluations
- Most typical for mapping detection coverage



Height of the computing stack

- Network, host HW/FW, OS, Application
- Can be used as a caveat to coverage breadth
- Maybe only measure for high criticality customers, systems

Types of systems & resources

- Increasingly important given explosion of non-Windows & Cloud
- Cloud will be true tipping point: monitoring & detection coverage will soon spread across >50 categories

Test Your Detections

Breach as a Service

"BaaS"

- Evaluates more than just detections
- Repeatable & automatable
- Cheaper than frequent pen tests

Unit Tests

Stimulate detections using synthetic data

- Appropriate when the SOC wants a custom testing "harness"
- Can be used as gating factor in detection build for CI/CD
- Repetition ensures detections never stop working

Red & Purple Team

- You should be doing this anyway; keeps SOC humble
- Illuminates blind spots
- Limited capacity

Conclusion

- **Be true to yourself, your analysts and your customers**
  - When you collect a set of data, be clear about what you will do wit it
  - Collected "just in case" with no detection or monitoring?
  - Routine "vanilla" detections, analysis and response
  - Specialized, customer-specific scenarios
- **Leverage everything that you can: don't reinvent the wheel**
  - The old "slap a sensor on it and call it good" strategy no longer works
  - Exploding variety of monitoring scenarios: leverage commodity solutions

Thank You

- Resources
  - https://attackevals.mitre-engenuity.org/
  - https://car.mitre.org/
  - https://github.com/Neo23x0/sigma
  - https://github.com/OTRF/OSSEM
  - https://packages.zeek.org/packages
- Past presentations
  - https://summit.fireeye.com/learn/tracks.html#executive-soc-metrics
  - https://www.youtube.com/watch?v=KRH9bbQLq0Y
  - https://www.youtube.com/watch?v=dmrSVXgMoeY