CARDINALOPS

Detection Posture Management

Detection Engineering Maturity: Helping SIEMs Find Their Adulting Skills

Dr. Anton Chuvakin, Google Office of the CISO

with Jay Lillie, VP Customer Success

7 Nov 2024

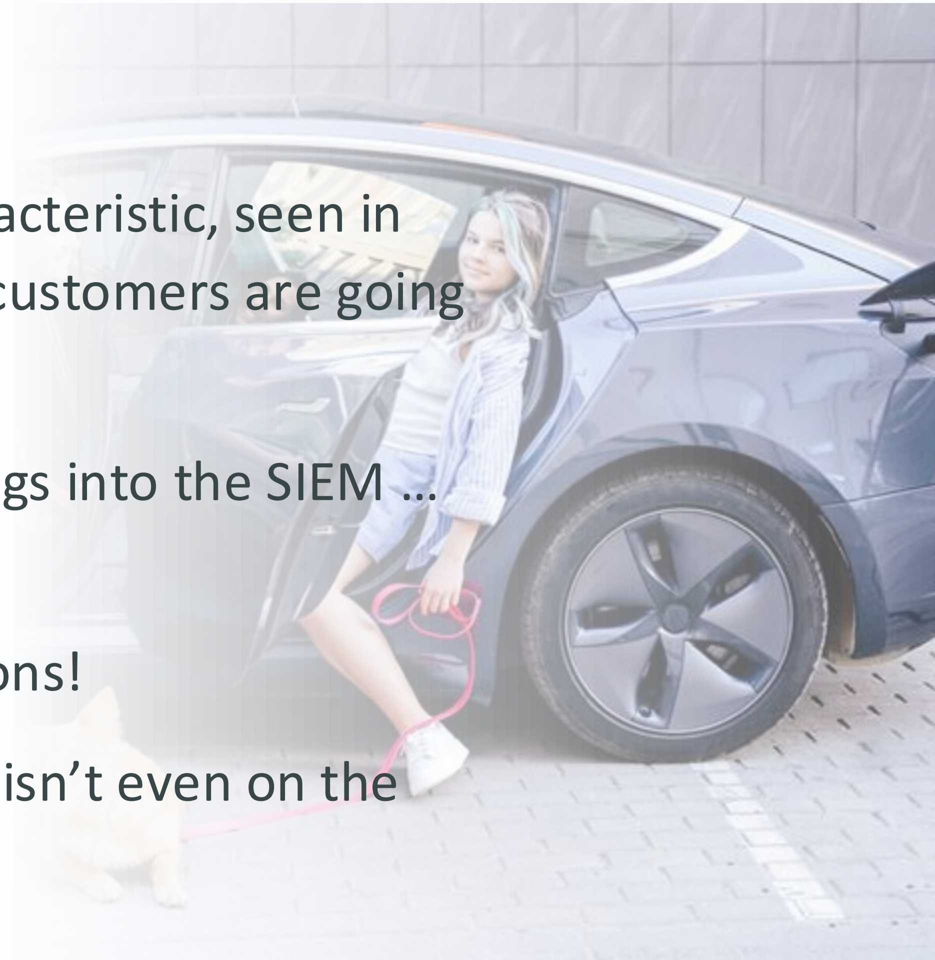
Agenda

- SIEM journey to adulthood
- Stages of development
- Free advice (with help from mom!)

Onward toward adulthood…

Stage	0. Dependent	1. Early stage	2. Maturing	3. Advanced
	“Mom, can I have a ride?”	“I got a job!”	“Living away from home!”	“My own place… by myself!”
Identity	I have a new SIEM… either my first one or I’m starting a green-field change-over to a new vendor. I’m relying exclusively on other defensive measures (e.g., EDR) to protect me while I’m getting things off the ground.	I have a SIEM up and running but there are so many alerts! My initial excitement that it was operational has been blunted by the fact that I’m now starting to ignore signals from the very detections I worked so hard to get into place.	We’ve finally reached a balance of sorts – detection coverage without too much noise. What worries me, however, is a new concern: where have I overlooked false negatives that provide opportunities for attackers? What am I missing?	My organization has finally matured around our SIEM. Detection (yes, and entire team!) and response are partnering. Threat information is actionable and MITRE ATT&CK® coverage is broad. However, I’m concerned I may not be fast enough!
Pros	Lots of time to spend with friends	Money to spend!	No curfew!	I make my own rules
Cons	Somebody else makes the rules	Where did my free time go?	Room-mates are awful	Adulting is expensive!

Stage 0: Dependent



Profile

“Mom, can I have a ride?”

I have a new SIEM… either my first one or I’m starting a green-field change-over to a new vendor. I’m relying exclusively on other defensive measures (e.g., EDR) to protect me while I’m getting things off the ground.

Lots of time to spend with friends

Somebody else makes the rules

- Besides a “first SIEM” characteristic, seen in specific migrations where customers are going “green field.”
- The focus here is getting logs into the SIEM … so that we can…
- …we can get more detections!
- Measuring SIEM efficiency isn’t even on the table.
- **FOCUS: GET IT TO WORK…**

Stage 0: Dependent

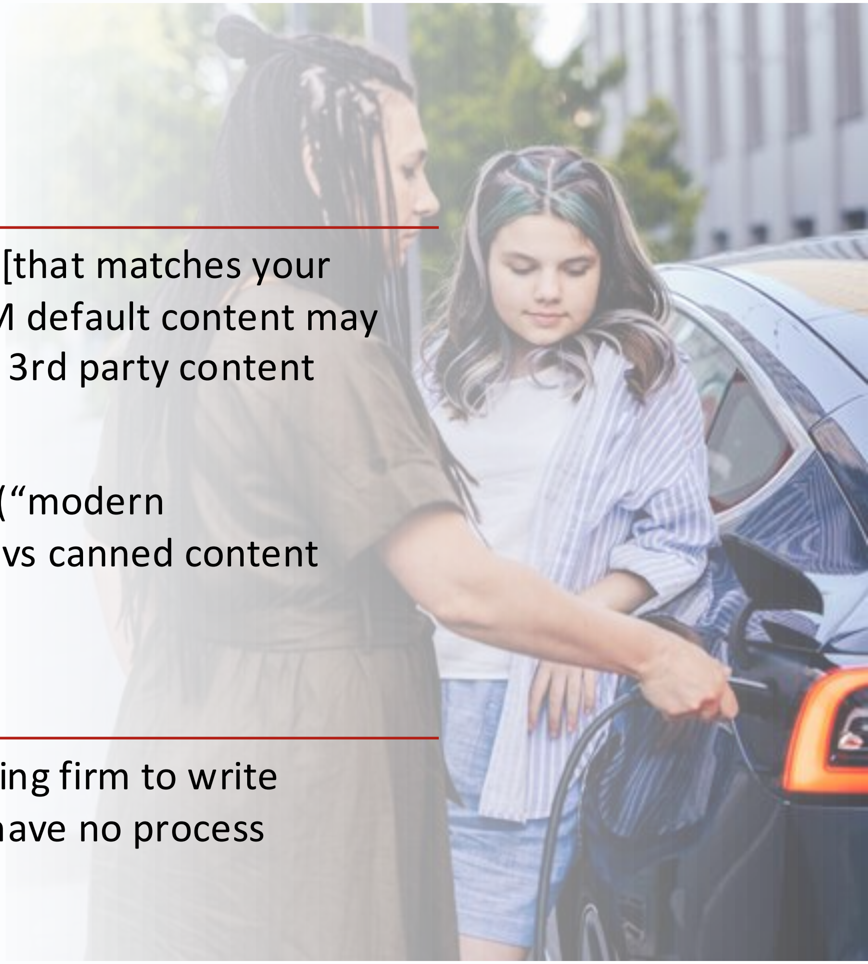
Profile

“Mom, can I have a ride?”

I have a new SIEM… either my first one or I’m starting a green-field change-over to a new vendor. I’m relying exclusively on other defensive measures (e.g., EDR) to protect me while I’m getting things off the ground.

Lots of time to spend with friends

Somebody else makes the rules



DO

- Get content pack and feed [that matches your threats / realities] Your SIEM default content may be fine for that, or get basic 3rd party content (CardinalOps can help!)
- Know your default content (“modern curated/managed content” vs canned content written 20 years ago)

Do NOT

- Hire a big team or a consulting firm to write detections ONCE and then have no process

Stage 1: Early Stage

Profile

“I got a job!”

I have a SIEM up and running but there are so many alerts! My initial excitement that it was operational has been blunted by the fact that I’m now starting to ignore signals from the very detections I worked so hard to get into place.
Money to spend!

Where did my free time go?

- Get a solid detection feed(s)
- Detect / tune
- No detection team; at best somebody who decided what detections end up being enabled..
- Metrics and reporting focus on noise, toil, time wasted, and burnout prevention?
- **FOCUS: REDUCE NOISE**

Stage 1: Early Stage

Profile

"I got a job!"

I have a SIEM up and running but there are so many alerts! My initial excitement that it was operational has been blunted by the fact that I'm now starting to ignore signals from the very detections I worked so hard to get into place.
Money to spend!

Where did my free time go?

DO

- Turn it off, create a list of use cases you need, enable content that maps to them … then tune
  - Popular use case list is: malware, compromised systems, data theft, etc
  - Look at risks (and threats, such as using TI) and environments you have/assets, do asset discovery / ASM

Do NOT

- Immediately buy a SOAR to filter
- Try to tune all content at once, use cases before tuning

Stage 2: Maturing

Profile

“Living away from home!”

We’ve finally reached a balance of sorts – detection coverage without too much noise. What worries me, however, is a new concern: where have I overlooked false negatives that provide opportunities for attackers? What am I missing?

No curfew

Room-mates are awful

- Noise is managed well or manageable
- False negatives and gaps become a bigger issues than noise
- Broken rules appear and have an impact!
- Metrics and reporting focus in gaps, coverage, etc
- Detection coverage discussions start en masse
- **FOCUS: REDUCE GAPS**

Stage 2: Maturing

Profile

"Living away from home!"

We've finally reached a balance of sorts – detection coverage without too much noise. What worries me, however, is a new concern: where have I overlooked false negatives that provide opportunities for attackers? What am I missing?

No curfew

Room-mates are awful

DO

- Evaluate the gaps, start filling them
- Start detection engineering team
- Create your detection lifecycle
- Use MITRE ATT&CK® to plan

Do NOT

- Rely on naïve ATT&CK coverage as the answer on what to do
- Don't jump to filling all gaps at once, this means stress

Stage 3: Advanced

Profile

“My own place… by myself!”

My organization has finally matured around our SIEM. Detection (yes, and entire team!) and response are partnering. Threat information is actionable and MITRE ATT&CK coverage is broad. However, I’m concerned I may not be fast enough!
No rules!

Adulting is expensive!

- Have good coverage, reasonable visibility into gaps, gaps are shrinking
- Noise is still manageable, detection quality is a thing
- You have a detection lifecycle, etc - TODO
- There a detection team here
- But are we fast enough? Do we have detection content before the attacker shows up?
- Do we not accidentally creating noise by keeping detections for too long; detection lifecycle ongoing work
- Metrics and reporting focus on speed of detection creation, detection in depth (multiple opportunities to detect) and TBD

Stage 3: Advanced

Profile

“My own place… by myself!”

My organization has finally matured around our SIEM. Detection (yes, and entire team!) and response are partnering. Threat information is actionable and MITRE ATT&CK coverage is broad. However, I’m concerned I may not be fast enough!
No rules!

Adulting is expensive!

DO

- Consider that this is a good place – there may be diminishing returns from overengineering the SIEM from this point onward
- Testing and refinement; from OK detections now to good detections forever
- Continuously evaluate and improve the efficiency of your detection lifecycle management process
- Relentless pursuit of automation
- Cover environments where you are weaker

Do NOT

- Rest on your laurels
- Don’t lose people to burnout

Mom? Help me!!!!

- **“Mom? Help, I ran out of money!”** Budget overruns on the SIEM project, or realizing that ongoing maintenance costs are higher than anticipated.
- **“Mom? I think I'm getting evicted!”** Logs are not being collected or log retention is not long enough, log data is lost/gone
- **“Mom? I crashed the car!”** Despite all your work, SIEM failed to detect the attack, leading to significant damage.
- **“Mom? This adult life is hard!”** Alert triage work still overpowers detection engineering work and the model that works for you fails to emerge…

Conclusions

- The maturity journey is ongoing: **SIEM and threat detection optimization are continuous processes.** Even at the advanced stage, you never stop (because threats don’t).

- (for most) Don't over-engineer: **There's a point where excessive SIEM engineering yields diminishing returns.** Focus on core use cases and detection lifecycle management.
- **Prioritize based on your stage:** Early stages should focus on noise reduction, while mature organizations can shift to proactive gap assessment and threat hunting.
- **People and processes are key:** Building a skilled detection team and fostering collaboration with response teams is essential for success.

Thank you!