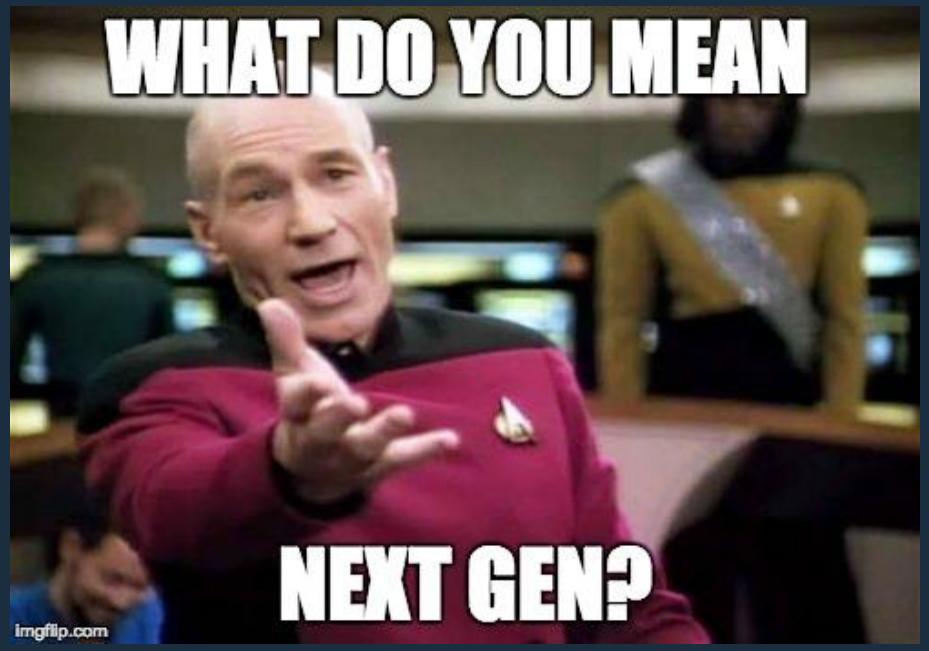


XDR – THE HIDDEN PITFALLS OF EVALUATION AND DEPLOYMENT

Who am I

Steve Turner

Director, Security Architecture @ Prudential

LinkedIn: in/beingageek/

Twitter: beingageek

IT Infrastructure – 6 years

Infosec – 6 years

Who am I

Ben Tyminski

Senior Security Specialist @ Prudential

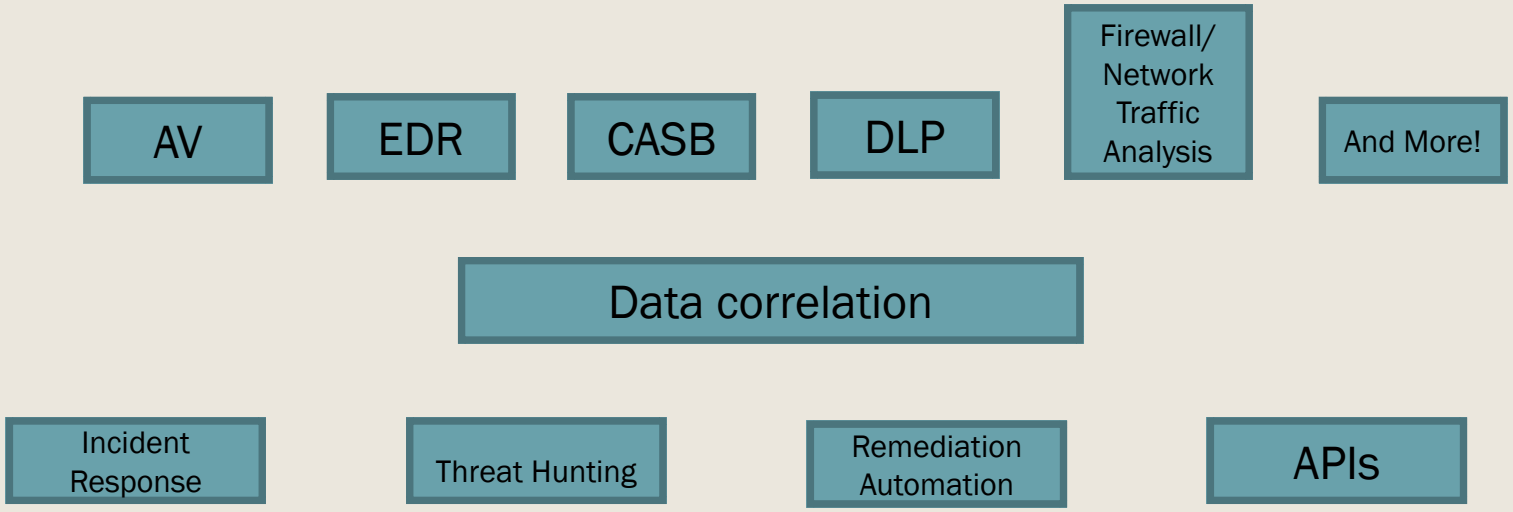
LinkedIn: In/benjamintyminski

IT Infrastructure – 2 years

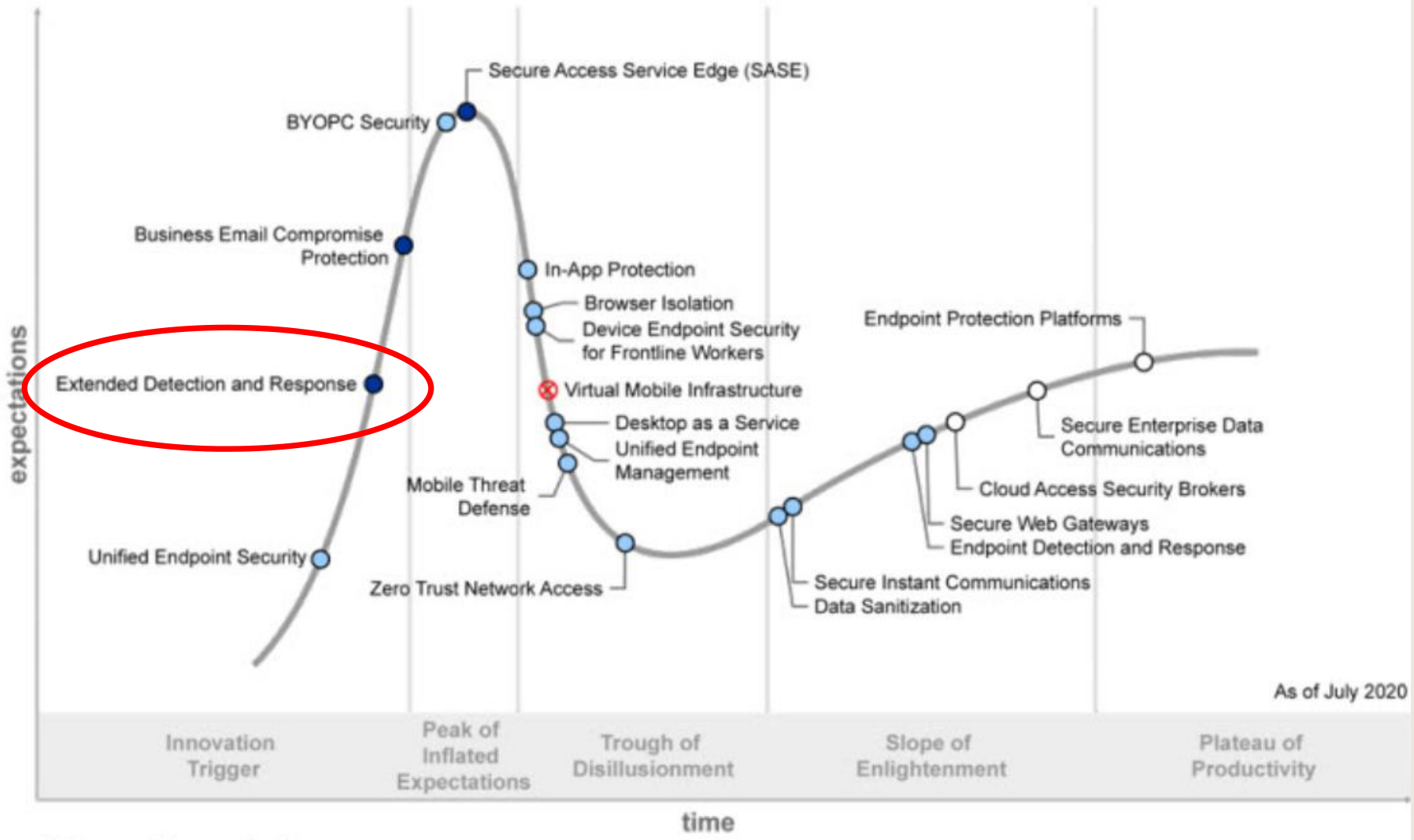
Infosec – 4 years

XDR?!? BUT we just got to EDR ☹

- What is XDR?
  - *Extended Detection and Response*
  - *Integrated suite of security products across entire computing stack (endpoint, network, cloud, identity, SIEM, and more!)*
  - *Assumes compromise (fits in with the model of Zero Trust)*
  - *Continuously evolving, generally fits in with Secure Access Service Edge (SASE)*



Hype Cycle for Endpoint Security, 2020



Plateau will be reached:

○ less than 2 years ● 2 to 5 years ● 5 to 10 years ▲ more than 10 years ⊗ obsolete before plateau

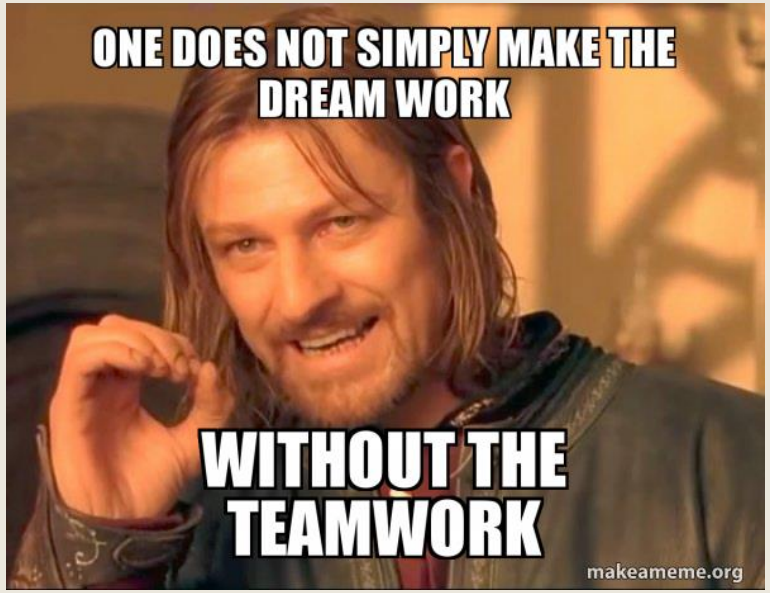
Source: Gartner
ID: 450232

Why do it now?

- Legacy security tools in a growing/evolving threat environment
- Point solution security placed around the environment to fill gaps quickly
- Multiple sensors/vendors on the network and endpoint
- Multiple consoles to manage and view
- No correlation/integration between different solutions
- Massive overhead with trying to manually correlate telemetry in your SIEM
- Carried over configurations someone made a long time ago that haven't been adjusted
- Poor end user experience, "Security is just getting in the way"
- Tools implemented with no input from other technology/business teams

What to look out for (DO THIS FIRST)?

- **Things you need to do (and will save your butt later)**
  - *Map out your existing security tools and capabilities*
    - Make sure to include existing gaps you may have whether it's not having an EDR tool, missing endpoint logging, really dive into the details
  - *Map your existing security tools to the capabilities that they provide to you, you will probably find lots of overlap*
    - Why did you buy a specific tool? Can the tool functionality be moved into something else you have?
  - *Take the data you collected above and create a very detailed requirements and rating matrix*
    - Not all XDR solutions are created equal, you need to research what's out there
      - *Leverage your typical research firms (Gartner, Forester, IANS), presentations and networking with other security folks (SANS, Twitter, etc)*
    - Don't be shy, put in all your wishlist items as well! Remember, you want to drive your security posture forward. If that means getting things like Cloud Posture Management, Threat/Vulnerability Manager, OS Configuration Compliance, etc, go for it!



Coordination and Working with Other Groups (One Team, One Dream)

- Assign a Project manager
- Don’t wear too many hats!
- Avoid too many cooks in the kitchen
- Reach out to other teams early and often
- Define tasks and roles for each team
- Utilize a task management and tracking solution such as JIRA or some other type of Kanban/Agile task tracking system

POC’s and Testing

- Prepare a sample set of machines, cloud environments, and users that represent your environment
  - Use newly imaged machines and existing machines
  - Reimage machines between tests
  - Use sandbox cloud environments, do not test in production!
- Documentation, Documentation, Documentation
  - Document everyyyyyyything
  - Vendor documentation will have a wealth of knowledge, you may need to reread it multiple times
- Make sure to continuously update your ratings for each vendor that you test as your testing
- Have a solid test plan for each business/technology area
  - Partner with the business/technology teams to help build this out, there will always be something that you didn't think of or planned for

Planning and Deployment Gotchas

- Communicate, Communicate, Communicate!
  - And when you think you've done enough communicating, communicate some more!
  - Make sure the technology community understands the benefits!
- Ensure policies are consistent between environments
  - Adjust where necessary (different cloud environments, email, VDI vs Traditional Endpoint)
- Don't just move over legacy policies (if moving from an existing solution), start fresh and build from the ground up
- Train help desk and various technology teams and business partners in new procedures
  - *Make sure they clearly understand the types of calls that they may have come in so that they're routed appropriately (Email, Endpoint, Cloud, etc)*

Other Gotchas and Troubleshooting (Wow that snuck up on me)

- Errors that didn’t come up in POC
- The hidden process of a business group that was not brought up
  - *Worked on the old product doesn’t now.*
- Be ready to deal with False Positives
  - Especially because now you're dealing with telemetry across the security stack
  - Utilize your internal resources/teams to determine bad from good
  - Most XDR solutions have a baselining period of about a week, so that also may have not completed
- Each cloud environment is unique, you may spend more time than you planned for connecting your XDR solution to them
  - Evaluate Inline vs API integrations and what makes sense for your org

Evolve your process

- Work with your SOC to update their knowledgebase and workflows.
  - Their concept of alerts and incidents may change drastically based on the correlation logic within your XDR platform
- Adjust your exception process as needed
  - How will you handle exclusions?
- Operationalize new features and update/create any processes as needed
  - Don't just expect "we slammed in this new platform, why aren't you using *insert new feature here*"
- Move ownership of processes that belong in a different technology tower/department

Preparing to be successful

- Update all documentation for security standards that your XDR solution is replacing, integrating into, etc

- Be prepared to continuously evaluate new functionality as XDR evolves (it currently evolves very quickly compared to traditional security tools)
  - Keep security features/capability list updated to identify any new capabilities and potential gaps
  - Create an intake process for potential new features

- Create a dynamic security culture around XDR
  - Refresh training sessions of solution
  - Talk to peer teams on what is working for them and what isn't, can it be change through process or a block within the solution.

- Automate as much as possible!

- Ensure all team are in sync during and after deployment