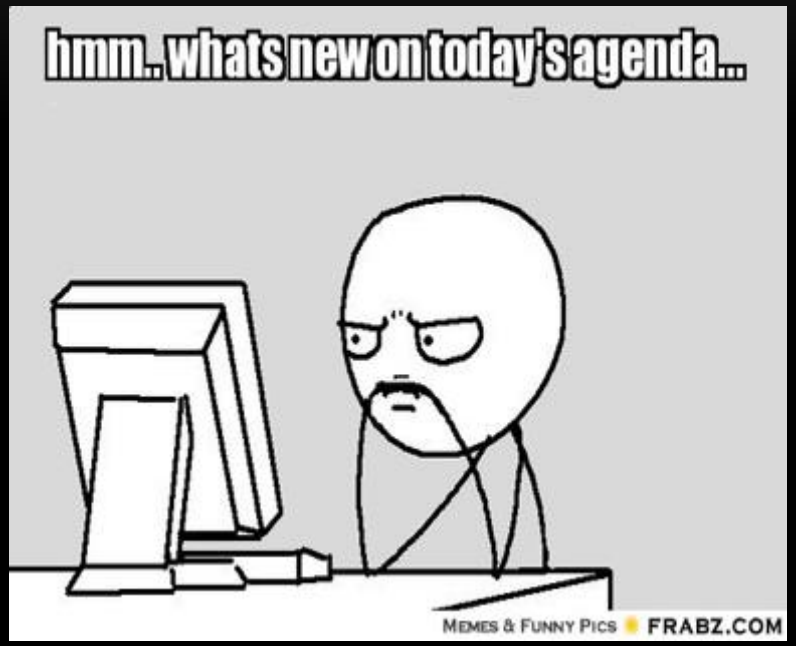
ADAPTIVE MONITORING AND DETECTION FOR TODAYS LANDSCAPE

BIO

- CISO at Binary Defense Systems
- 15+ years experience, specializing in security operations, threat intelligence, and incident response
- Created SOC's and threat intelligence programs for Fortune 500's
- Assisted 3 letter agencies in profiling foreign cyber criminals
- U.S. Marine
- Twitter: @b0dach

AGENDA

- Overview of monitoring and detection
- Overview of incident response
- True incident response planning
- Adaptive monitoring and detection
- Tying it all together



I HAVE MONITORING AND DETECTION, WHY THE BREACH?

- All the major companies that have been breached had some kind of monitoring and detection program.
- You need to monitor more than just what you see as critical infrastructure
- What about upstream and downstream partners?

OVERVIEW OF MONITORING AND DETECTION: OLD PRACTICES

- Buy a SIEM
- ????
- Detection
- SO?
  - WAY too much is not seen
  - Waiting for a daily report != monitoring
  - Phase 2 is what is critical

OVERVIEW OF MONITORING AND DETECTION: OLD PRACTICES

- A SIEM as a checkbox tool

OVERVIEW OF MONITORING AND DETECTION: OLD PRACTICES

- SIEM Content:
  - Default content that isn't tuned
  - Old content that is broken
  - Alerting not working correctly

OVERVIEW OF MONITORING AND DETECTION: THE RIGHT WAY

- Buy a SIEM
- ????
- Detection

- ??? = Tune, Tune, TUNE!

OVERVIEW OF MONITORING AND DETECTION: THE RIGHT WAY

- SIEM Content:
  - Default Content; make sure it is configured properly
  - Clear stale content for better performance
  - Test all content, rules, alerts, etc.

OVERVIEW OF INCIDENT RESPONSE

- Typical incident response plans
  - Contains regularly updated escalation points and contacts; internal AND external
  - Trigger points are included
  - Reviewed and practiced with key players/units
  - Guidelines of typical scenarios that are flexible for atypical situations

OVERVIEW OF INCIDENT RESPONSE

- Typical incident response plans
  - High level overview of outdated types of incidents
  - Plans that haven't been updated regularly
  - Although plans may be "recertified" annually, typically they are still stale.

OVERVIEW OF INCIDENT RESPONSE

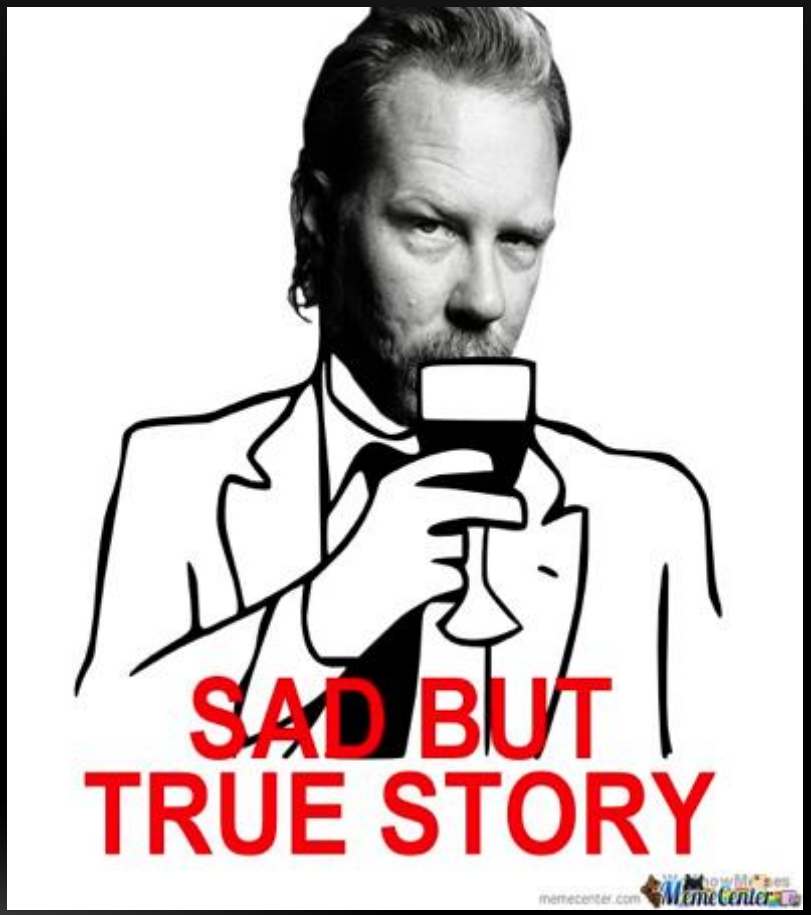
- Typical incident response plans
  - A couple of pages of outdated contact info
  - Based loosely off of disaster recovery plans
  - Do not offer any real value in an incident

INCIDENT RESPONSE PLAN FAILURES

- Either too stringent to be effective or not info information/planning to be effective
- Key players/organizations aren't involved in the plan or don't know their roles in an incident
- NOT UPDATED OR PRACTICED

INCIDENT RESPONSE? THE STORY OF LACK OF INVOLVEMENT

There once was a company in a far away land that thought they had an incident response plan for the ages. While they slumber in their beds, the evil APT'z from China snuck in and tried to steal their IP. When they awoke to the alarms of intrusion and despair, they reached for the IR plan of gold. When they blew the dust off of the plan and opened the tome, prepared for battle, no one knew where to start. The plan had grown old, it's power no more. All the knights of the fair company began to scurry and scamper. Communication broke down, help could not be raised, they castle was falling. While they scampered, the evil APT'z from China scurried away with all they held dear. The End.



INCIDENT RESPONSE? THE STORY OF LACK OF INVOLVEMENT

- Incident response plans MUST have buy in AND involvement from key players
- When an incident happens is not the time to figure out wat do.
- The plan should at minimum be review, preferably rehearsed regularly

TRUE INCIDENT RESPONSE PLANNING

- Creating/updating a plan based on real threats you are monitoring, what's going on in the wild, and situations that can affect your company
- Identify and include the key players from ALL the appropriate areas
- What kind of data do you need in case of a breach in order to even start the investigation?
- How are you going to communicate internally and externally (email? NO)
- How are you going to prevent data from leaving?
  - When you have that identified, how are you going to do that across the organization synced up and not alert the attackers?
- Think about what would happen if you got a call saying you were breached
- Regularly test and evaluate your plan

ADAPTIVE MONITORING AND DETECTION

- Proper utilization of monitoring technologies
  - If you have a product that is important enough to use, why would you not make sure it is being used properly?
  - IDS/IPS/HIDS/Next Gen product X are good tools (and not cheap). If you are going to spend the time and money on them, why would you not configure them properly?
  - Is it configured to send the right logs?
  - Is your SIEM or MSSP set up correctly to take in, correlate, and alert to these devices?

ADAPTIVE MONITORING AND DETECTION

- Incorporating penetration testing into monitoring
  - The results are based on REAL examples in your company
  - Focus on the technical findings; start creating monitoring content, rules, etc. to look for these avenues of approach
  - Test and retest this content

ADAPTIVE MONITORING AND DETECTION

- Incorporating threat intelligence into your monitoring
  - By proactively utilizing threat intelligence, you can increase the monitoring capabilities of an organization and decrease response time.
  - Taking information you gather, you can monitor threats to your company and industry
  - If you have a SIEM, you can create rules based on the intel you gather

ADAPTIVE MONITORING AND DETECTION

- Tuning and alerting on new threat vectors and IOC
  - Look at what's going on in the wild, use that knowledge
  - Adapt your monitoring to include these new threats. You should always be updating monitoring content on what's out there

TYING IT ALL TOGETHER

- Don’t make the mistakes that historically have led to missing a breach
- Whatever you use for monitoring and detection, you need to make sure you have the right content
- Never stop tuning that content
- Make sure you have a good foundation for your incident response plan
- You need to think outside the box when you start adapting your monitoring content utilizing everything at your disposal including pen test, threat intelligence, and what’s going on in the wild

TL;DR WHAT DID WE LEARN?


THANK YOU FOR YOUR COOPERATION
YOU ARE THE BEST
memecrunch.com

QUESTIONS?