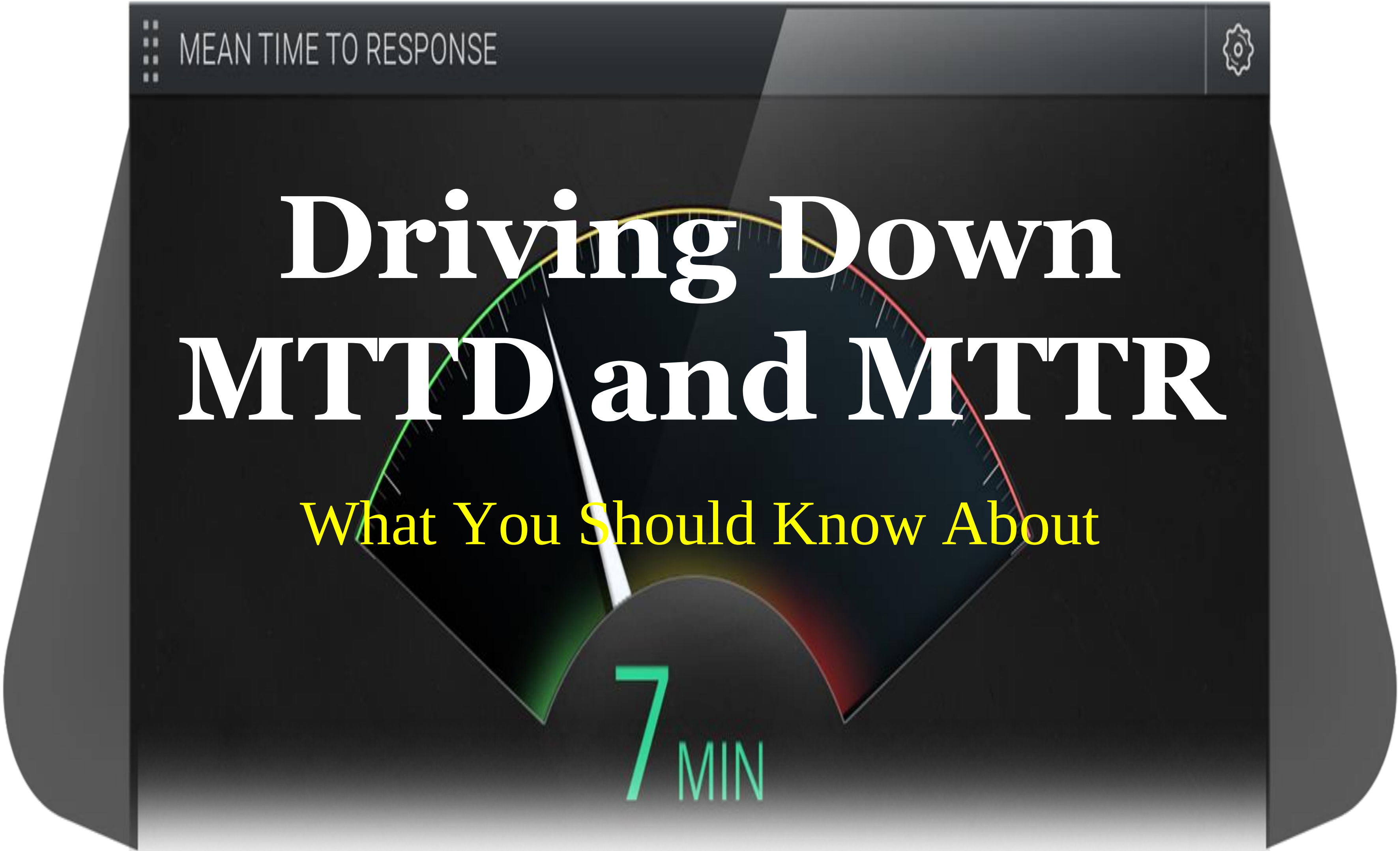

Driving Down MTTD and MTTR

What You Should Know About

Introduction

Effectively connect people, process and technology to minimize MTTD and MTTR

There’s a reason it’s said that what gets measured gets managed. In order to successfully achieve a goal, you have to be able to measure progress. It’s the only way to know if you’re heading in the right direction.

That’s why any security operations team worth their salt will be paying close attention to both their mean time to detect (MTTD) and mean time to respond (MTTR) metrics when it comes to resolving incidents.

MTTD & MTTR - Dwell Time

The average dwell time for attackers still sits somewhere within the ranges of 100 – 140 days and frankly, we can do better. Security operations teams need to be fanatical when it comes to lowering these metrics within their organizations.

Significantly reducing dwell time, MTTD and MTTR starts with an understanding of attacks. From there, you need multiple groups working together in harmony enabled by technology to automate and orchestrate **incident response** processes.

Three Quick Definitions

- Mean time to detect, or MTTD, reflects the amount of time it takes your team to discover a potential security incident.
- Mean time to respond, or MTTR, is the time it takes to control, remediate and/or eradicate a threat once it has been discovered.
- Dwell time captures the entire length of a security incident – reflecting the duration from when an attacker first enters your network to the time they are removed and you have returned to a known-good state.

Factor In Reducing MTTD and MTTR

People are always the first layer when it comes to reducing MTTD and MTTR within any SOC. Up and down the chain, your team needs to deeply understand both the processes and the technologies in order to detect and respond to threats quickly. This is accomplished through education and constant training.

Consistent training and tabletops are also useful to test your security operations team’s understanding, alertness and procedural readiness to harden and lower your MTTD and MTTR and ensure battle-readiness when it comes to real incidents.

Security Orchestration & Automation

For starters, ensure your security team fully understands your incident response processes and life cycles, common attacks and hacker techniques, and best practices for how to defend against them. As an example – **security orchestration and automation** tools can be used effectively by analysts of any skill level, but you'll get even more out of your investment if your team already has a good foundation for analyzing and making judgement calls about malicious activity.

Clarify & Codify The Processes

SOC teams need a detailed understanding of the assets they’re protecting, the roles and responsibilities within each group, what internal resources are available to assist with the incident and how each incident effects their organizations from a priority standpoint.

Having proper processes established for security operations teams, tied to the appropriate groups and responsibilities, will significantly lower the MTTR metric within organizations since the predefined rules of engagement on how to tackle incidents has already been outlined. This builds confidence and empowers the SOC to contain and remediate threats efficiently and within the guidelines the organization has set forth.

Enable Team With Right Tools

Using technology to lower MTTR and MTTD is an integral part of reducing these KPIs in today’s SOCs. Security operations groups are working with a multitude of tools, many times within in disparate consoles that can limit their visibility into an attack, so having technology that allows for a central point of reference where this data can be correlated and analyzed is required.

Right Tools To Drive Down

Drive Down MTTD and MTTR

Assuming data is being directed to a central location, the next step is to start automating and orchestrating efforts to detect and remediate attacks. Having the data directed to one location is important because your SOC needs a central point of authority when it comes to making decisions on attacks.

Security orchestration, automation and response (SOAR) tools are used to take the intelligence from disparate systems to enable SOC teams to make quicker decisions, which lowers the MTTR when working incidents. In this way, technology becomes the connective tissue between the SOC’s ecosystem of tools, processes and personnel.

Conclusion

Cybersecurity is a collaborative effort and effectively using the people, processes and technologies in tandem is what enables security operations teams to continuously improve performance and protect their organizations. Many organizations tackle technology first and try to adapt their processes and people based on the technology stack. In reality, it should be the reverse – technology should be the enabler that allows the other components to be streamlined into a well-oiled machine. Using SOAR technology allows for security operations teams to utilize their processes and procedures in automated ways to significantly **reduce the MTTD & MTTR** within their organizations.