RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-R03

Your SecOps Don't Catch Bad Guys and Waste Your Money. We Know Why!

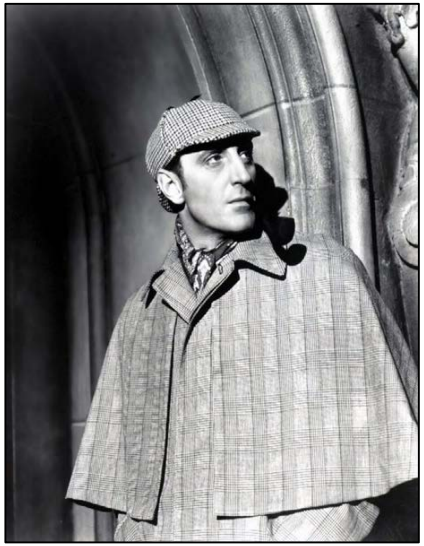
Mark Manglicmot
Senior Manager
EY

Adam Tyra
Manager
EY

#RSAC

Your average security analyst?

Source: *By Mack Sennett Studios [Public domain], via Wikimedia Commons*



Source: By Employee(s) of Universal Studios (Photograph in possession of SchroCat) [Public domain], via Wikimedia Commons

Agenda

- Why aren't we catching bad guys?
- How can we improve?
  - Adversary focus – what is it and why is it important?
  - Deliberate planning – not just for supervillains anymore
- Testing a methodology
- Takeaways and next steps

We already pulled the technology lever, and the people lever says “out of order!”

The limitations of cookie cutter controls

Source: http://www.publicdomainpictures.net/view-image.php?image=23618&picture=leftover-cookie-dough&large=1
[Public domain]

You probably have enough technology

- Your tool *deployment* might be suboptimal
  - "Defense in depth" *should* account for any remaining attack surface
  - How "deep" is it around your critical assets?
  - Did you build from the outside in or from the inside out?
- Your tool *selection* might be suboptimal
  - "Only 3% of 606 unique combinations of two security products managed to detect all exploits." Source: "Correlation of Detection Failures." NSS Labs. 2013.
  - Who architected your resource deployment, anyway?

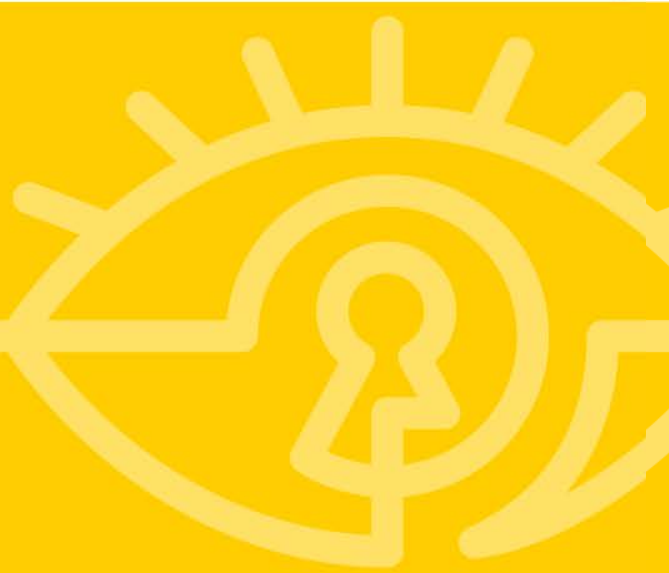
"Expense in depth- the multilayered approach to ensuring minimal return on investment."

Source: Rick Holland's Blog. "Expense In Depth And The Trouble With The Tribbles." December 9, 2012. Accessed February 10, 2016.

The SOC team and security alerts

- How many of those alerts represent actual intrusions/security incidents?
  - "395 hours are wasted each week … because of false positives."
    Source: "The Cost of Malware Containment." Ponemon Institute. Jan 2015.
  - That's 10 full-time employees!
- Is this an effective use of time?
- We call it available capacity!

Source: http://uncyclopedia.wikia.com/wiki/File:Hamster-wheel.jpg
[Public domain]



Squeezing value from your existing technology and current staff

Injecting adversary focus

- Adversary focus- a product of adversary knowledge combined with self-knowledge
  - Do you know your enemies?
    - Which named threat actors are your most likely adversaries?
    - What, specifically, do they want? **Hint: It might not be what you think!**
  - Do you know yourself?
    - Which of your assets are most critical to your (business, not IT) operations? **Hint: It isn't your domain controllers!**

Understanding adversary intent

- Differentiate between high-value and high-payoff targets
  - Penetration testers pursue high-value targets….and then stop
  - Real adversaries pursue high-payoff targets
- Remember- data theft is just one potential outcome of an attack

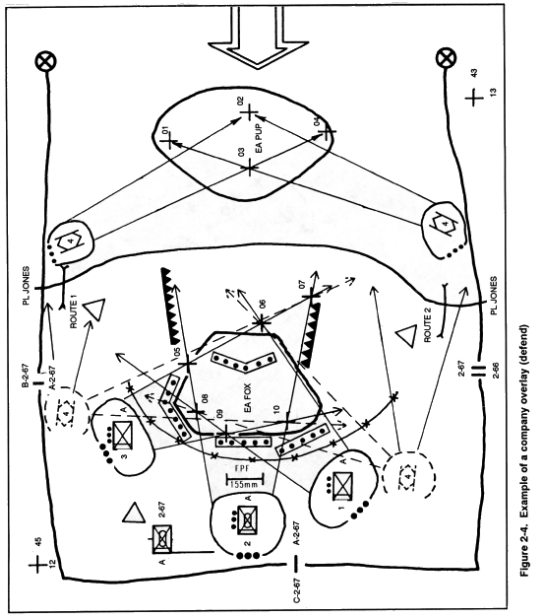
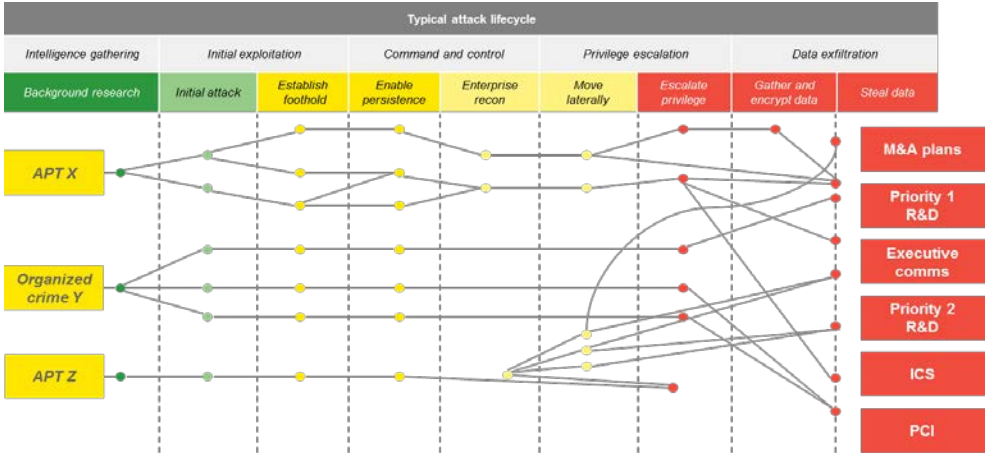


Figure 2-4. Example of a company overlay (defend)

Source: FM 7-7: The Mechanized Infantry Platoon and Squad, U.S. Army.

The value of adversary focus

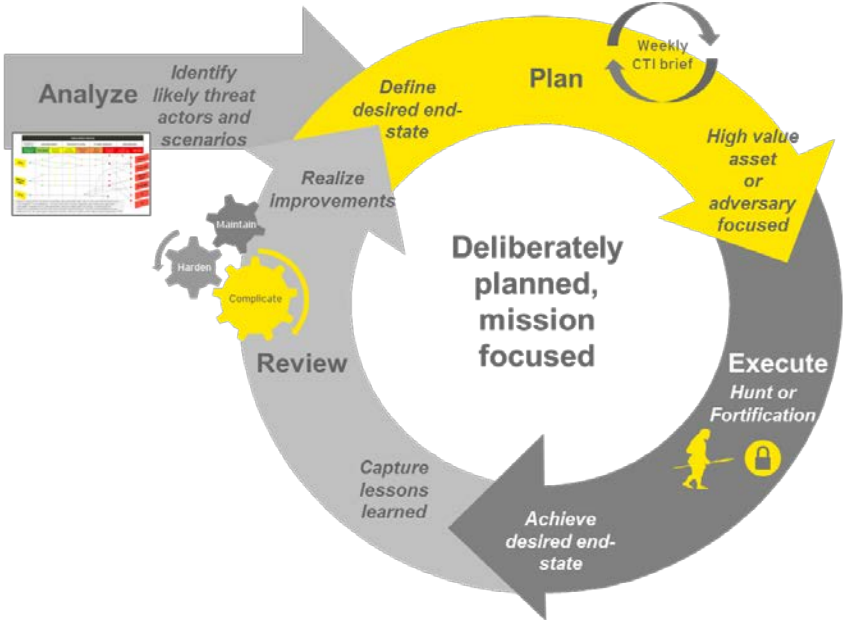
- Enables resource deployment optimization
- Blocks known tactics and techniques of named adversaries:
  - Cyber kill-chain analysis links real tactics to real targets
  - Targeted countermeasures complicate legitimate threat scenarios



Source: Manglicmot, Mark, and Adam Tyra. “Enhancing Your Security Operations with Active Defense.” 2016.

Seizing the initiative via deliberate planning

- You know what the adversary may do. What will you do?
- Craft a coherent enterprise security strategy:
  - Develop concrete objectives
  - Survey the means available
  - Develop courses of action



Source: Manglicmot, Mark, and Adam Tyra. "Enhancing your security operations with Active Defense." 2016.

Iterate rapidly! Plan, execute, review, repeat!

Turning cops into detectives with adversary focus and deliberate planning

Testing our ideas

- We tried this at a global technology company …
  - Data centers located in Europe, North America, Asia, Australia
  - Cloud environment hosting virtually all web-based technologies, OS variations, etc.
- … with a sophisticated cybersecurity apparatus:
  - 24x7 global security monitoring
  - In-house cyber threat intelligence team

What we did

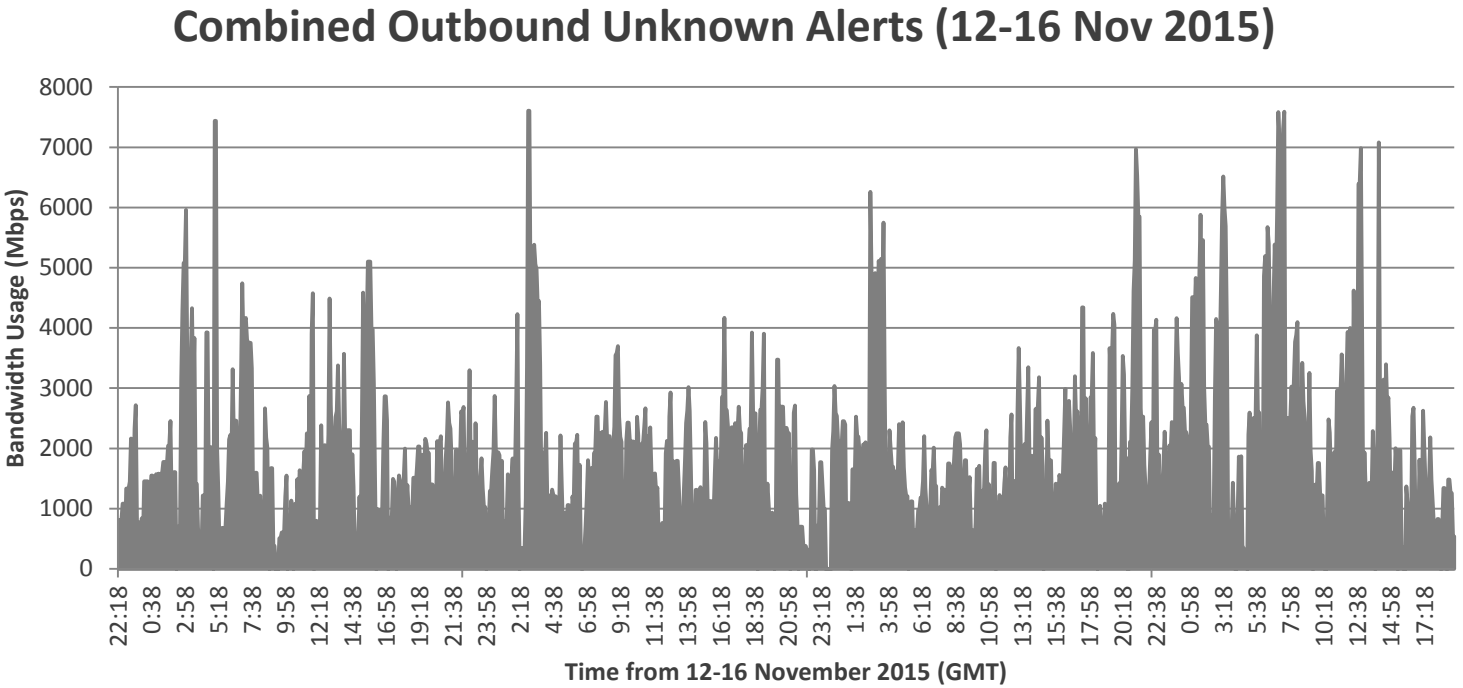
Developed multiple insight-driven, deliberately planned “missions”:

Threat Scenario	Our Response
“Bad Guy A” uses Tor with custom malware to circumvent security monitoring tools and hide data exfiltration.	Develop and deploy targeted countermeasures to detect Tor usage. Identify and eliminate rogue connections.
“Bad Guy B” exploits Kerberos “golden tickets” to gain access to high payoff targets. Kerberos servers cannot be rebooted to destroy existing tickets.	Conduct anomaly analysis by comparing authentication logs to ticket creation logs in order to detect golden ticket usage. Deploy additional monitoring to surveil high payoff targets.
“Bad Guy C” targets cloud infrastructures to build low-cost, easy to maintain botnets for hire resulting in resource theft and bandwidth cost overages.	Identify and dollarize malicious traffic. Deploy targeted countermeasures to block malicious traffic. Identify and remediate compromised hosts participating in botnet activity.

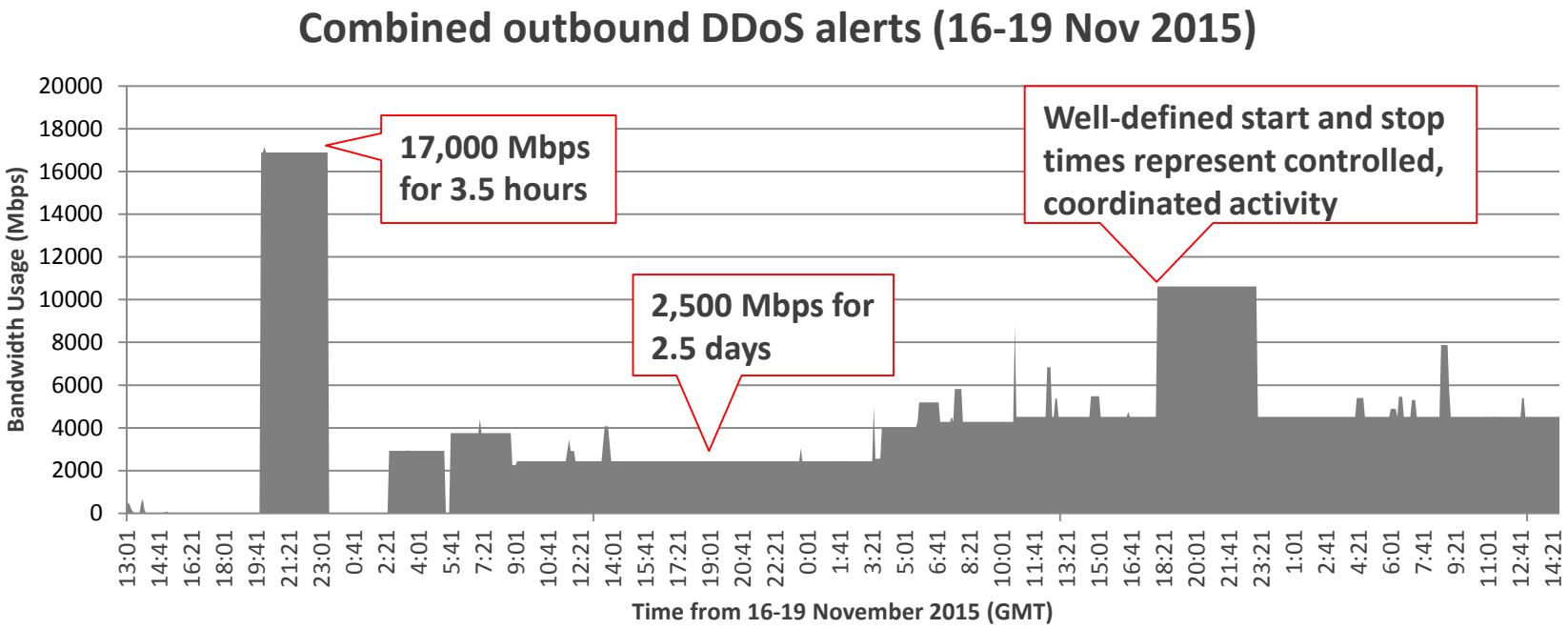
Key outcomes

- Identified and eliminated malicious activity:
  - Every hunt achieved a reduction in targeted activity.
  - Average time required to identify and trace activity cut significantly.
- Exposed weaknesses in organizational processes:
  - Failures in information sharing-multiple cybersecurity silos
  - Missing procedures for critical activities
- Enhanced operational efficiency (saved the client $$$)

Analyzing large bandwidth usage events

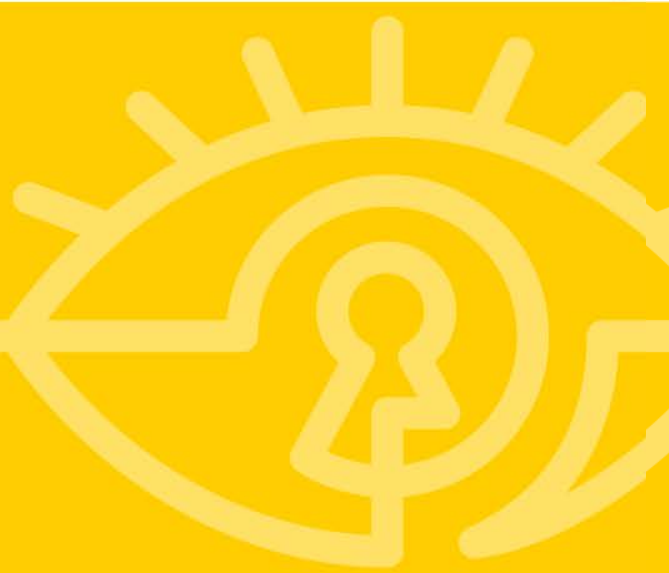


Is that a botnet picking your pocket?



Bonuses of deliberate planning

- Planning as a professional development tool:
  - Staff are forced to devise new tactics and procedures.
  - Staff become adept at predicting outcomes/roadblocks
  - Gathering lessons learned is critical to creating a learning organization
- Planning enhances effectiveness:
  - Reduces ad hoc resource expenditure
  - Reduces susceptibility to “leading practices” and other fads:
    - Vulnerability of the month?



Takeaways

Takeaway themes

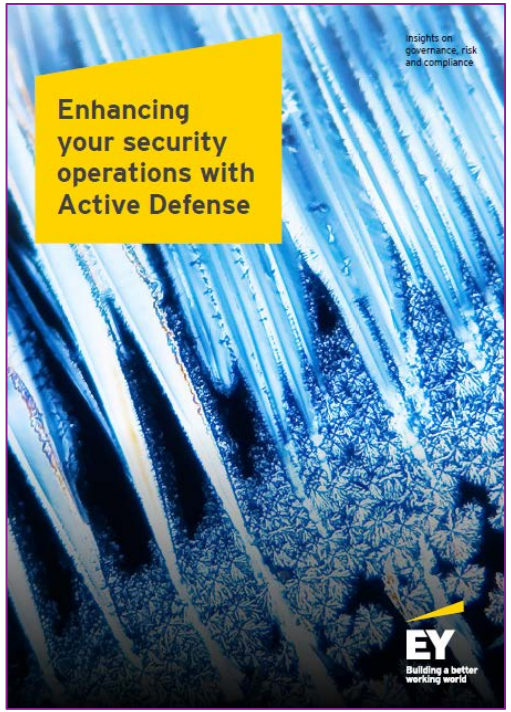
- Focus your (limited) resources on protecting your most critical assets:
  - Create defense in depth by building outward from likely targets
  - Plan to defeat the most likely threat scenarios against the most likely targets- not to defeat all attacks from all adversaries
- Put your staff to work:
  - Stop waiting for your tools to find/stop advanced attackers!
  - Deliberately plan and conduct missions to identify and eliminate legitimate threats and harden critical assets

Next (first?) steps

- This month – identify and study your adversaries:
  - Discuss with industry peers, review past security incidents and start consuming cyber threat intelligence
- This quarter – develop an security operations strategy:
  - What will you defend and from whom?
  - How will you defend it?
- This year – seize the initiative from attackers:
  - Initiate continuous proactive operations (plan, execute, review, repeat)
  - Capture and apply lessons learned

Where to learn more (free stuff)

- "Enhancing your security operations with Active Defense"
  - ey.com/cybersecurity
- Questions?



EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.