Fortune 100 InfoSec on a State Government Budget

Eric Capuano
@eric_capuano
Introduction

- SOC Manager at Texas DPS
- Cyber Warfare Operator for Air National Guard
- InfoSec Consultant
- Packet Hacking Village / Wall of Sheep @ DEF CON
  - Emerging Threats, honeypots / deception systems
- Cyberpatriot Instructor
  - Everyone should do this - pay it forward!
- “Security Against Obscurity” [https://blog.ecapuano.com](https://blog.ecapuano.com)
- InfoSec hobbyist / teacher / student
Disclaimers

- Opinions are mine and mine alone
- Nothing is absolute - YMMV
- CYA - All products, vendors, figures and potentially anything else in this presentation are completely fictional
- “The only wisdom is in knowing you know nothing” - Socrates
Why is Enterprise Security So Hard?

... and why is it so damn expensive?
Why is Enterprise Security so hard?

- After 114 years, why are we still failing at securing information systems?
Because Security *is* hard...

- It does not come from padlock.png on your website
- It does not come from magic box that you install in your datacenter
- It does not come from next-gen magic box, either
- It does not come from spending millions on “security stuff”
- It does not come from checking “Yes” on your compliance audit

- It does, however, start with a mindset
Common problem statements

● I can’t hire good people - a.k.a. - The a “talent shortage”
● I can’t train the people that I have
● I am too busy responding to incidents to improve incident response
● My budget has a lot of zeros, but on wrong side of the decimal
Common problem statements

- My users are dumb and keep clicking/opening/downloading $ROOTCAUSE
- Next-Next-Gen-Anti-APT-Signatureless-AV-Firewall™ is too expensive
- If only there was an affordable way to solve $PROBLEM
- Open source solutions are not feasible because $REASONS
Hire and keep good people, the rest will take care of itself.

Your team is your foundation
Your team is your foundation - Know how to hire

Credit: https://twitter.com/@mtanji
Your team is your foundation - Know how to hire

- Stop hiring solely by *degrees* or *certifications*...

...instead, look for

- **Passion**
- **Drive**
- **Ability to learn** new skills on the fly
Take care of the team that you have

Provide what they need to succeed
Your team is your foundation - **Communicate**

- Communication is key
Your team is your foundation - Communicate

- A SecOps communication platform can be much more than just “chatting”.
  
  - Integrate alerting from critical systems.
  - Automate analysis activities
  - Automate incident response actions

The bot above and a few additional examples can be found at https://github.com/ecapuano/slackbot
Your team is your foundation - Train & Spread Knowledge

- Constantly **train your security team**
Your team is your foundation - Train & Spread Knowledge

● **Written Tactics, Techniques and Procedures**
  ○ A *must have* for training, continuity and standardization

● **Internal Wiki** - a repository of “tribal knowledge”
  ○ BookStackApp.com
  ○ MediaWiki
Your team is your foundation - Train & Spread Knowledge

- Participate as a team in local or remote Capture the Flag events
- Cybrary.it - over 400+ free courses in IT & Security
- Send them to conferences like BSides/DEFCON!
- Have budget? Send them to SANS
Your team is your foundation - Train & Spread Knowledge

- Routinely train for worst case scenarios while the storm is calm
Your team is your foundation - Train & Spread Knowledge

- DFIR Simulations
Your team is your foundation - **Lead, Don’t Manage**

- **Lead - Don’t Manage**
  - Avoid micro-management
  - Encourage *innovation* and *ownership*
  - Promote the pursuit of knowledge in *desired areas*
  - Make *morale* a priority
Be less busy with this *one simple trick*!

Shift from a *reactive* to a *proactive* posture
Work Smarter - Know Your *Actual* Threats

How “Fansmitter” Malware Steals Data from Air-Gapped Computers

Changing a computer’s fan speed produces an audio signal that can be hijacked to steal data, say computer security experts who have tested the technique.
Work Smarter - Know Your *Actual* Threats

"I don't think paralysis [of the electrical grid] is more likely by cyberattack than by natural disaster. And frankly the number-one threat experienced to date by the US electrical grid is squirrels."

- John C. Inglis, Former Deputy Director, National Security Agency 2015.07.09

Credit: [http://cybersquirrel1.com/](http://cybersquirrel1.com/)
(the only reputable source on ‘Cyber Squirrel 1’ Ops)
Work Smarter - Think Critically

- Apply this mindset to all common, noteworthy incidents
  - How frequently do we see this type of incident?
  - Does this incident have similarities to other recent incidents?
  - What type of in-house, proactive controls can mitigate this threat and prevent similar incidents?
Work Smarter - Be Proactive

● Real world example - Ransomware

● Average 6 month period at DPS
  ○ 140+ campaigns multiplied by a user base of 10,000+ users
Dear support,

Please see the attached invoice (Microsoft Word Document) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your business!
Bonnie vause

This footnote confirms that this email message has been scanned by PineApp Mail-SeeK.
Work Smarter - Be Proactive

- Macros - because “Ron” in IT is a full-stack developer now!
  
  - https://blog.ecapuano.com/macro-security-for-enterprise-defenders/
Work Smarter - Be Proactive

- Billys_Resume.pdf.exe.js.wsf.vbs.lol.wtf
Work Smarter - Be Proactive

- Real world example - Phishing campaigns
Work Smarter - Be Proactive
No executive support / budget?

Maybe you’re selling it wrong...
Do Work, Get Money - Sell it Better

- Instead of *asking for budget*...

...*persuade leadership why they want to give it to you* instead.
Do Work, Get Money - **Sell it Better**

- Stop with the *fear tactics*
Do Work, Get Money - **Show Value**

- Attract more bees with honey...

*Your C-Levels, probably*
Without spending all the money...
SecOps on a Budget - Be Skeptical, Spend Wisely

- Stop suffering from contract paralysis, blind renewals and brand romances.
  - “Well, this is what we’ve always used so I guess we’ll just renew it...”
  - “Why have we been paying for $X when we only need $Y?”
  - “I really love $BIGBRAND because the blinking lights are my favorite color!!!”
SecOps on a Budget - Know when NOT to buy

- Does this solution solve a problem that actually exists?

- Are you using your existing solutions to 100% of their capability?
  - Let’s be honest...
SecOps on a Budget - Buy smarter

- For the tools you must buy, do your research!

- Resist the marketing

- Demand a hands-on demo and use as if it was in production
SecOps on a Budget - **Buy What Fits**

- How well does this solution *integrate* with your other capabilities?
SecOps on a Budget - Why buy what might be free?

- Is there an open source tool that can solve this problem?
  - (Probably, yes)
SecOps on a Budget - Why buy what might be free?

What if I told you there was a free tool that could:

- block TOR exit nodes
- blacklist phishing URLs and Ads
- automate analysis and incident response
- pull hundreds of open source intel feeds
- Deceive adversaries and warn defenders in the early stages of an attack
- ...almost anything else you can imagine
SecOps on a Budget - Constantly assess your existing tools

- For every noteworthy security incident, answer these questions:
  - Are the indicators new or old?
  - What systems had visibility of this threat?
  - Of those systems, which should have detected / mitigated the threat, but did not?
    - Why?

- Hold your solutions accountable or replace them
SecOps on a Budget - Walking the Walk at DPS

- Past year at DPS - Making changes and breaking vendors hearts
SecOps on a Budget - Walking the Walk at DPS

- Scenario 1 - Email Security
  - Big Brand - Big Marketing
  - $234k annually
  - Very difficult to use / configure
  - Stability and performance issues with custom filters
  - Zero “bells and whistles” - run of the mill capabilities
  - Clustering issues
SecOps on a Budget - Walking the Walk at DPS

● Scenario 1 - Email Security
  ○ Big Brand - Almost No Marketing
  ○ $34k annually (compare to $234k)
  ○ Far easier to configure
  ○ Attachment sandboxing included
  ○ In-house testing revealed significantly better threat detection ratios over old solution
SecOps on a Budget - Walking the Walk at DPS

- Scenario 2 - Perimeter UTM / NGFW
  - BIG Brand - *Basically a Marketing Firm that sells Firewalls*
  - $750k buy-in // $274k +4% annually
  - Consistently terrible support *(YMMV)*
  - False negatives on threats with 1+ year-old OSINT
    - “¯\_(ツ)_/¯ - That’s in the next threat signature update!” - With love, Tech Support
SecOps on a Budget - Walking the Walk at DPS

- Scenario 2 - Perimeter UTM / NGFW
  - *Almost-as-Big* Brand - *Almost-Zero* Marketing
  - $36K buy in // $40K annually (compare to $750k // $274k)
  - Great support / responsive engineers
  - Outperforms Big Brand on NSS Labs threat detection tests
  - In-house testing observed higher detection ratio of malicious URL categories
    - Great feature - blocking phishing sites *before* users get phished!
So where’s all this free stuff?
The Pirate Bay, of course!

Kidding.... Try Github!
YOU WOULDN'T GIT CLONE A SIEM
SecOps for Free - Nothing beats free-thousand-dollars

- SOC Incident Management / Automation
  - TheHive - thehive-project.org
    - Collaborate on incidents
    - Automate analysis
    - Track observables
    - Share intel
    - Much more...
SecOps for Free - Nothing beats free-thousand-dollars

Credit: http://chrissanders.org/2017/03/case-management-the-hive/
SecOps for Free - Nothing beats free-thousand-dollars
SecOps for **Free** - Nothing beats **free**-thousand-dollars

- **SIEM**
  - AlienVault OSSIM
    - Asset Discovery
    - Vulnerability Scanning (OpenVAS)
    - HIDS / NIDS
    - Behavioral Monitoring
    - Integration with OTX
  - SIEMonster

- **Log Aggregation / Visualization**
  - Graylog
  - ELK Stack
  - Grafana

- **HIDS / AV**
  - OSSEC
  - ClamAV
SecOps for **Free** - Nothing beats **free**-thousand-dollars

- **Vulnerability Scanning**
  - OpenVAS
  - Nikto
  - Wapiti

- **Firewall** *(Small-Med Business)*
  - PFsense
  - Endian

- **Intrusion Detection / Prevention**
  - Suricata + Scirius
  - Snort + Snorby

- **IOC Sharing**
  - Anomali STAXX
  - MISP
  - AlienVault OTX
SecOps for Free - Nothing beats free-thousand-dollars

- **Honeypots**
  - ModernHoneyNet
  - Cowrie/Kippo (SSH)
  - Rdpy (RDP)

- **NetFlow**
  - LogRhythm NetMon Free

- **Threat Research**
  - VirusTotal
  - Cuckoo Sandbox
  - ThreatCrowd
  - PassiveTotal
  - AlienVault OTX
  - Too many to list...

https://github.com/hslatman/awesome-threat-intelligence
SecOps for Free - Nothing beats free-thousand-dollars

- Forensics / Incident Response
  - Google GRR
  - Live Collection - Allosaurus
  - Magnet RAM Capture
  - FTK Imager
  - Autopsy

- Learning Management System
  - Moodle
  - PhishMe CBFree CBTs

- Penetration Testing
  - Kali
  - Metasploit
  - SETK
Questions, Feedback, Share intel / ideas?

eric.capuano@dps.texas.gov