

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>
- 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?



Nevil Maskelyne



Guglielmo Marconi

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

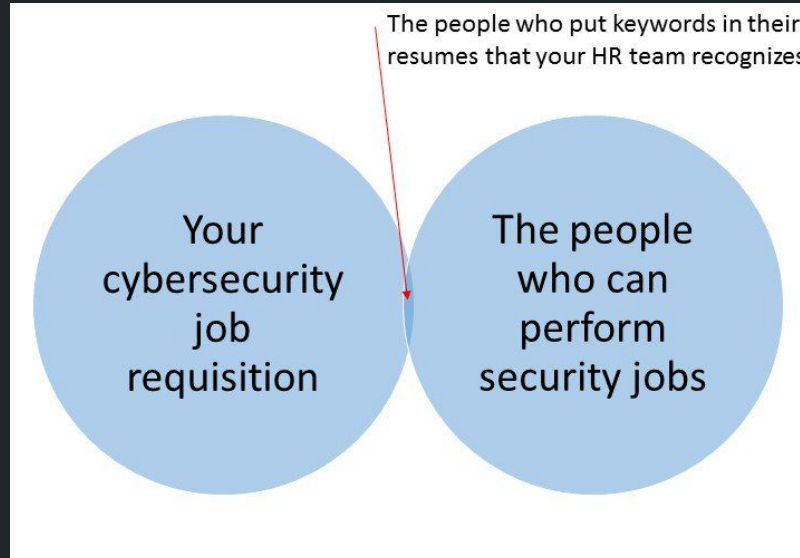
Common problem statements

- 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

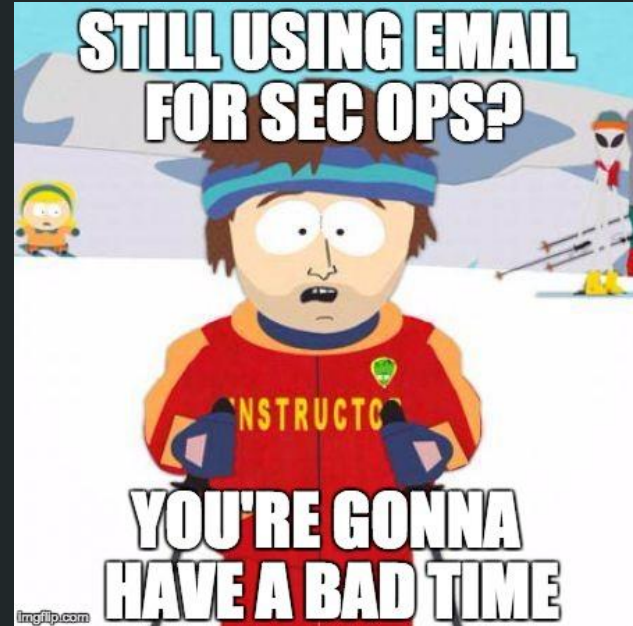


Take care of the team that you have

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



IP Blocker APP 13:33

IP:213.186.33.40 (URL:none) has been added to the [REDACTED] Blacklist by ron. Reason: CS-20170424-004

Verify your entry here [http://\[REDACTED\]](#)

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

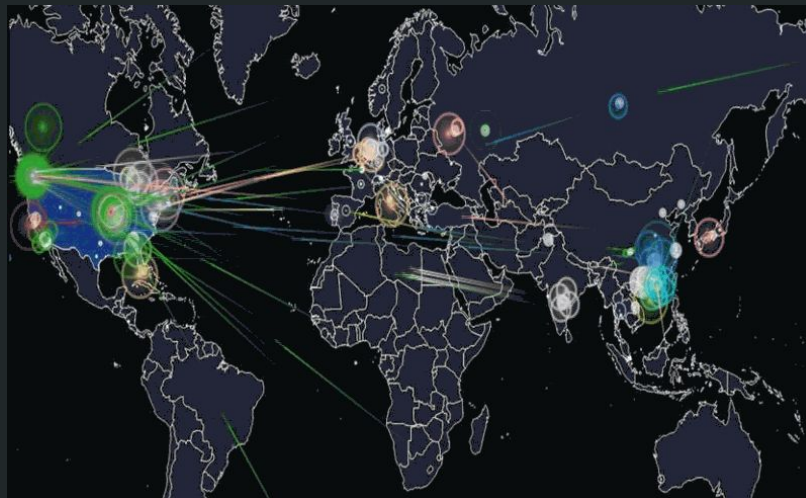
```
/**
 *
 * @author jeff
 */
public class Main {

    public static String AppName = "SQL Mail";
    public static String AppVersion = " 0.0.1 ";
    public static String AppAuthor = "Jeffrey Cobb";
    public static String AppDate = "August 8th, 2007";
    public static String AppPath = System.getProperty("user.dir");
    public static String AppDriver = "smallsql.database.SSDriver";
    public static String AppDBHeader = "jdbc:smallsql:";
    public static String AppDBPath = AppPath + "/sqlmail";
    public static String AppPreferences = AppPath + "/sqlmail_prefs";
    /** Creates a new instance of Main */
    public Main() {
    }

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) throws Exception {
        // TODO code application logic here

        boolean bDBConnect = false;
        int result = 0;
        frmMain SQLMailForm = new frmMain();
        System.out.println("\r\n" + AppName + "\r\nVersion" + AppVersion + "\r\nAuthor: " + AppAuthor + "
        .. " + AppDate + "\r\n");

        Toolkit tk = Toolkit.getDefaultToolkit();
        Dimension screen = tk.getScreenSize();
        System.out.println(screen.getWidth() + " --- " + screen.getHeight());
    }
}
```



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



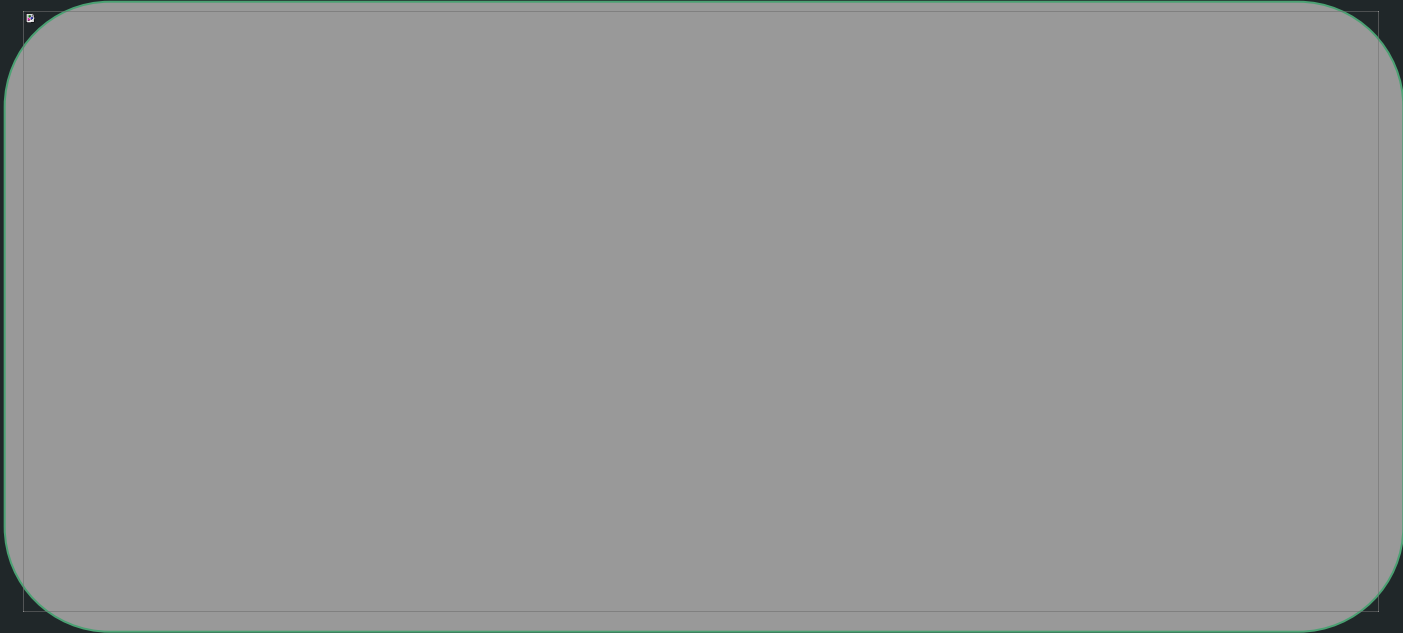
Tabletop Scenarios @badthingsdaily · 10h

You've detected a malware beacon from an unmanaged host. Only have it's IP and MAC address on corporate network. Physical location unknown.



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/>
(the only reputable source on 'Cyber Squirrel 1' Ops)

Agent	Success
Squirrel	927
Bird	461
Snake	84
Raccoon	76
Rat	41
Marten	23
Beaver	15
Jellyfish	13
Human	3*

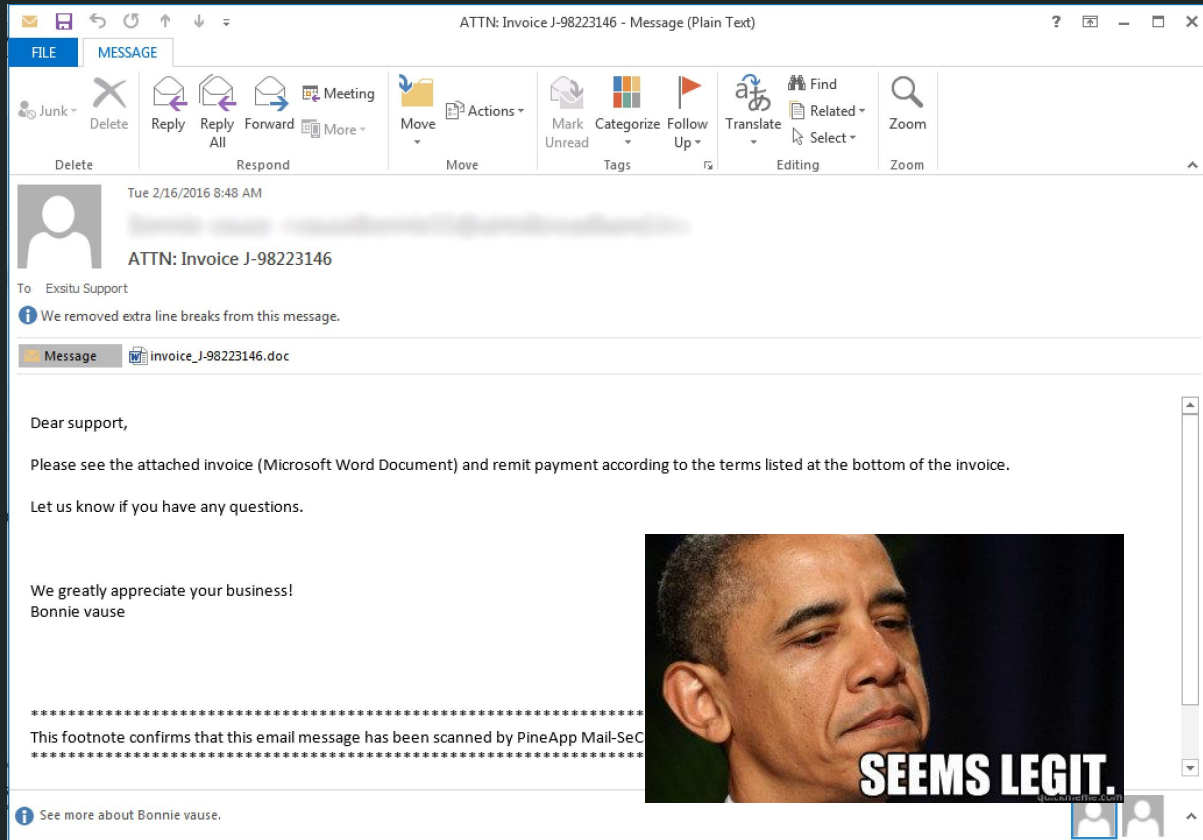
Work Smarter - Think Critically

- 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

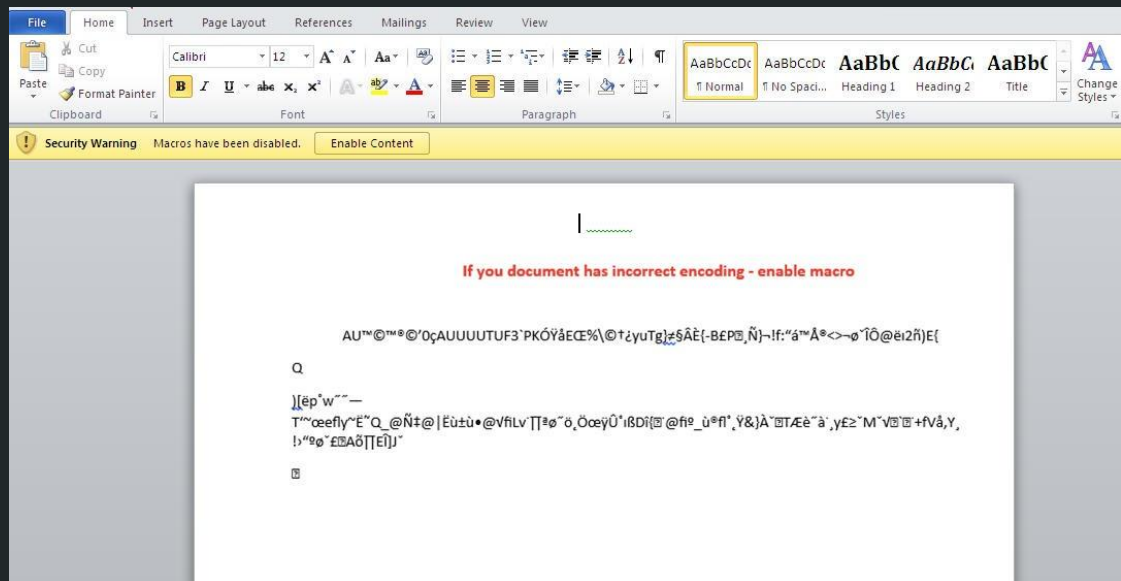
- Real world example - Ransomware
- Average 6 month period at DPS
 - 140+ campaigns multiplied by a user base of 10,000+ users

Work Smarter - Be Proactive



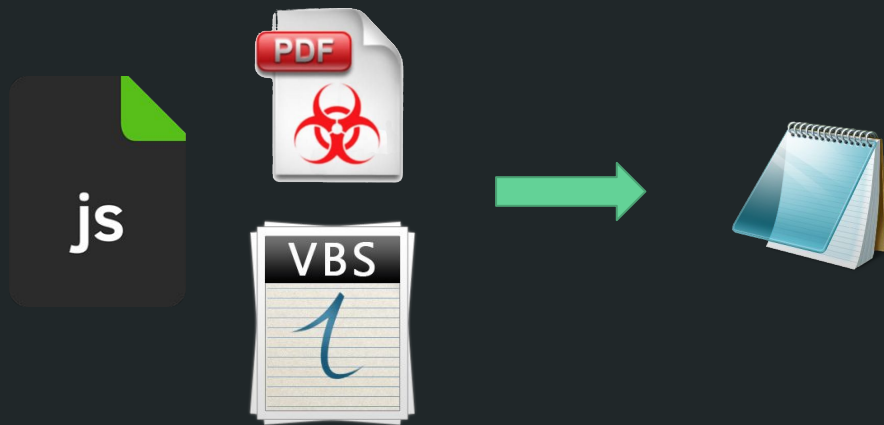
Work Smarter - Be Proactive

- **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**

www.sanagustinturismo.co/Facebook/


facebook

Email

Password

☒ Stay logged in

[Forgot your password?](#)



Connect with your friends faster, wherever you are.

The Facebook application is available in more than 2,500 phones.

- Faster navigation
- Compatible with the camera and your phone contacts
- Without regular updates: download only

[Discover Facebook Mobile](#)

Sign up

It's free (and will remain).

Name:

Surname:

Your email:

Re-enter your email address:

Password:

Gender:

Date of Birth: Day: Month: Year:

[Why do I have to provide my birthday?](#)

Work Smarter - Be Proactive

```
index.html
1 <!DOCTYPE html>
2 <html lang="en" id="facebook" class="no_js">
3
4 <!-- Mirrored from www.facebook.com/ by HTTrack Website Copier/3.x [XR&CO'2014], Sun, 30 Apr 2017 03:16:51 GMT -->
5 <head><meta charset="utf-8" /><meta name="referrer" content="default" id="meta_referrer" /><script>function envFlush(a){func
  requireLazy(['Env'],b);}else{window.Env=window.Env||{};b(window.Env);}}envFlush({"ajaxpipe_token":"AXijIaUk-NHqv9tu"});</
  noscript><meta http-equiv="refresh" content="0; URL=index4964.html?_fb_noscript=1" /></noscript><title id="pageTitle">Faceboo
  Facebook /><meta property="og:url" content="https://www.facebook.com/" /><meta property="og:image" content="https://www.face
  content="en_US" /><meta property="og:locale:alternate" content="www" /><meta property="og:locale:alternate" content="es_LA" /
  og:locale:alternate" content="fr_FR" /><meta property="og:locale:alternate" content="it_IT" /><meta property="og:locale:alter
  th_TH" /><meta property="og:locale:alternate" content="vi_VN" /><meta property="og:locale:alternate" content="ko_KR" /><meta
  application/ld+json>{"@context":"http://schema.org","@type":"WebSite","name":"Facebook","url":"https://www.facebook.com/"
  opensearchdescription+xml" href="osd.xml" title="Facebook" /><link rel="canonical" href="index.html" /><link rel="alternate"
  " /><link rel="alternate" media="handheld" href="https://m.facebook.com/" /><link rel="alternate" hreflang="ar" href="https://ar-ar.facebook.com/" /><link rel="alternate" hreflang="bg-ba.facebook.com/" /><link rel="alternate" hreflang="ca" href="https://ca-es.facebook.com/" /><link rel="alternate" hreflang="el" href="https://el-gr.facebook.com/" /><link rel="alternate" hreflang="fa" href="https://fa-ir.facebook.com/" /><link rel="alternate" hreflang="fr-ca" href="https://fr-fr.facebook.com/" /><link rel="alternate" hreflang="hr" href="https://hr-hr.facebook.com/" /><link rel="alternate" hreflang="it-it.facebook.com/" /><link rel="alternate" hreflang="ko" href="https://ko-kr.facebook.com/" /><link rel="alternate" hreflang="ms" href="https://ms-my.facebook.com/" /><link rel="alternate" hreflang="pt-pt" href="https://pt-pt.facebook.com/" /><link rel="alternate" hreflang="sr" href="https://sr-rs.facebook.com/" /><link rel="alternate" hreflang="vi" href="https://vi-vn.facebook.com/" /><meta name="description" content="and videos, send messages and get updates." /><meta name="robots" content="noodp,noydir" /><link rel="shortcut icon" href="https://www.facebook.com/favicon.ico" /></head></pre>
```



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

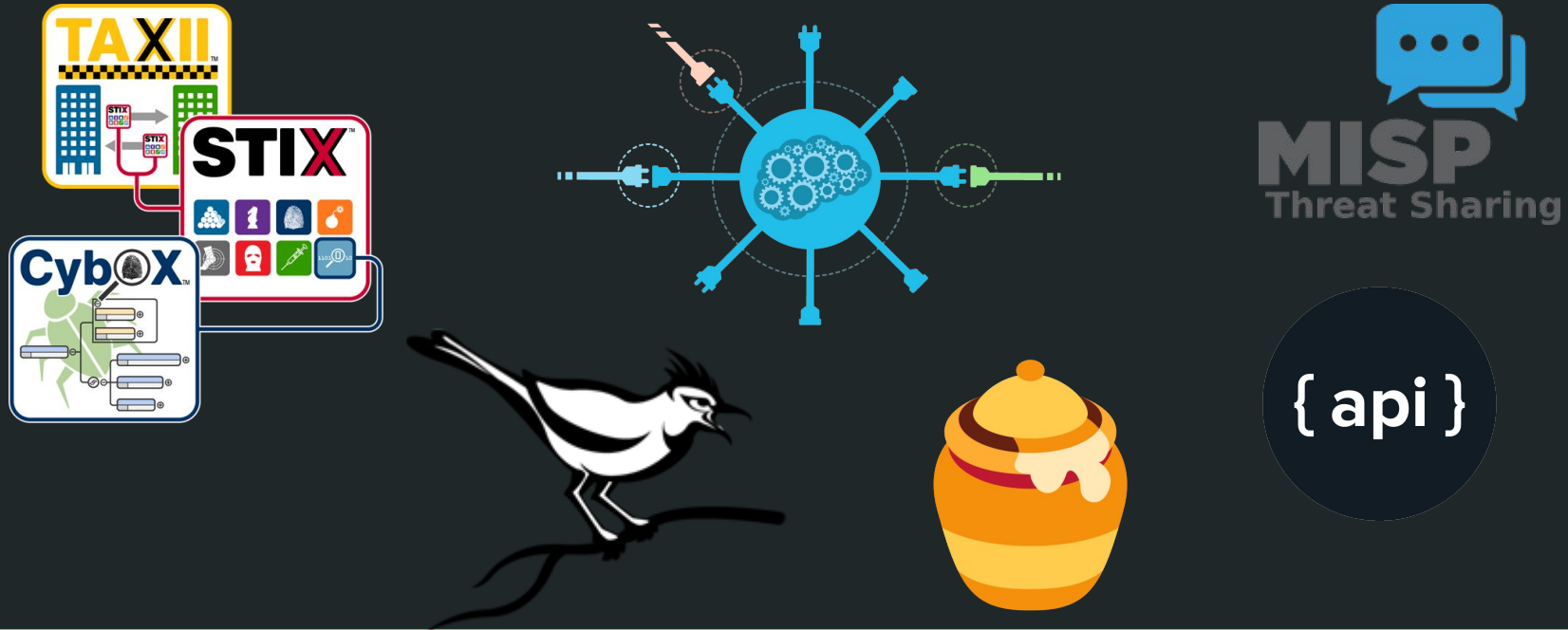
- Does this solution solve a problem that actually **exists**?
- Are you using your **existing solutions** to 100% of their capability?
 - Let's be honest...

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

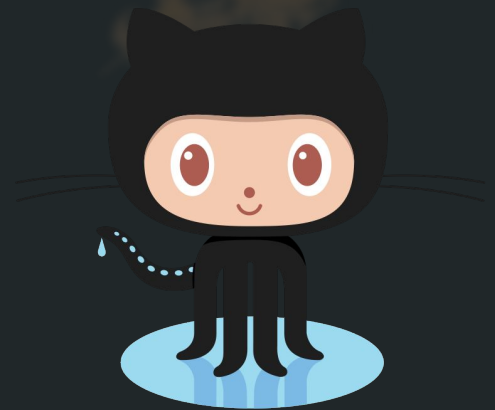
- **Scenario 2 - Perimeter UTM / NGFW**
 - *Almost-as-Big Brand - Almost-Zero Marketing*
 - **\$36K** buy in // **\$40K** annually (compare to **\$750k** // **\$274k**)
 - Great **support** / responsive engineers
 - **Outperforms** Big Brand on NSS Labs threat detection tests
 - In-house testing observed **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

The screenshot shows the 'Create a new case' modal in TheHive. The modal has a blue header with the title 'Create a new case'. Below the header, there are two sections: 'Case details' and 'Case tasks'. In the 'Case details' section, there are fields for 'Title' (with a red asterisk indicating it is required), 'Date' (with a red asterisk), 'Severity' (with a red asterisk and buttons for L, M, H), 'Tags' (with a red asterisk), 'TLP' (with a red asterisk and buttons for WHITE, GREEN, AMBER, RED), and 'Description' (with a red asterisk). In the 'Case tasks' section, there is a 'Task title' field and an 'Add task' button. At the bottom of the modal, there is a 'Cancel' button, a red asterisk with the text 'Required field', and a '+ Create case' button. The background shows a list of cases and a task log.

Create a new case

Case details

Title *

Date * **now**

Severity * **L** **M** **H**

Tags *

TLP * **WHITE** **GREEN** **AMBER** **RED**

Description *

Case tasks

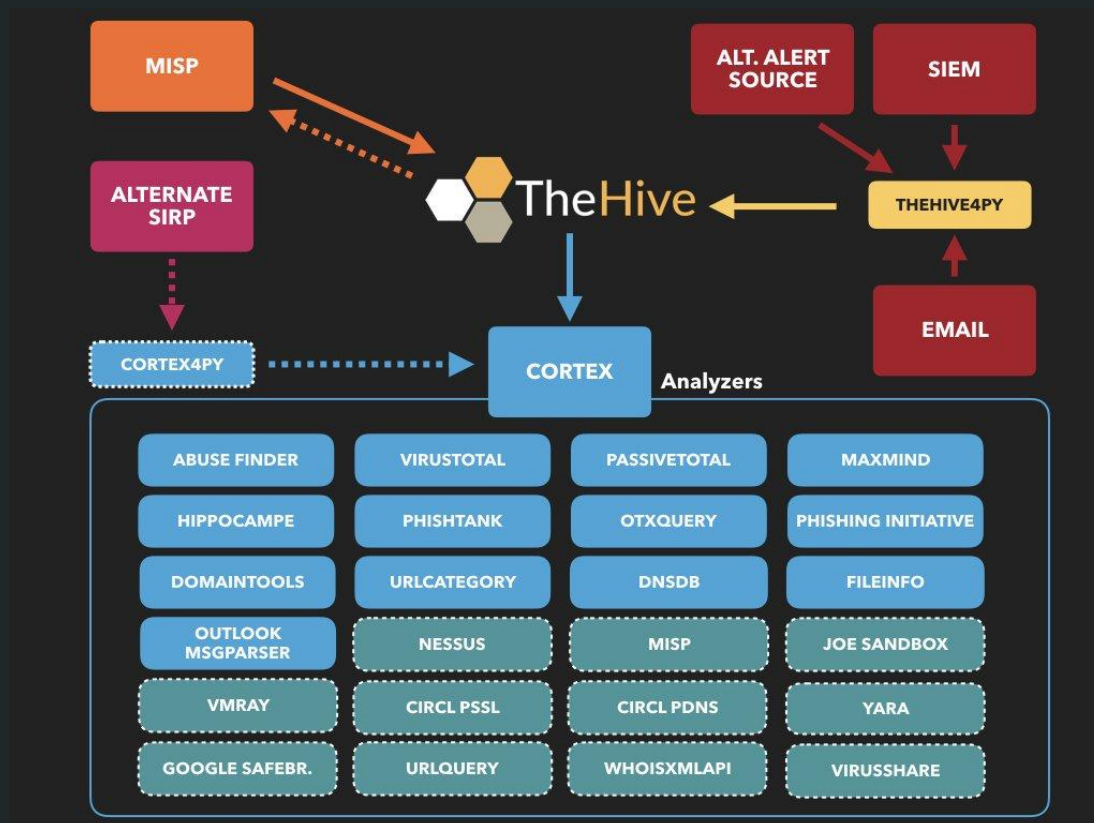
Add task

No tasks have been specified

Cancel *** Required field** **+ Create case**

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