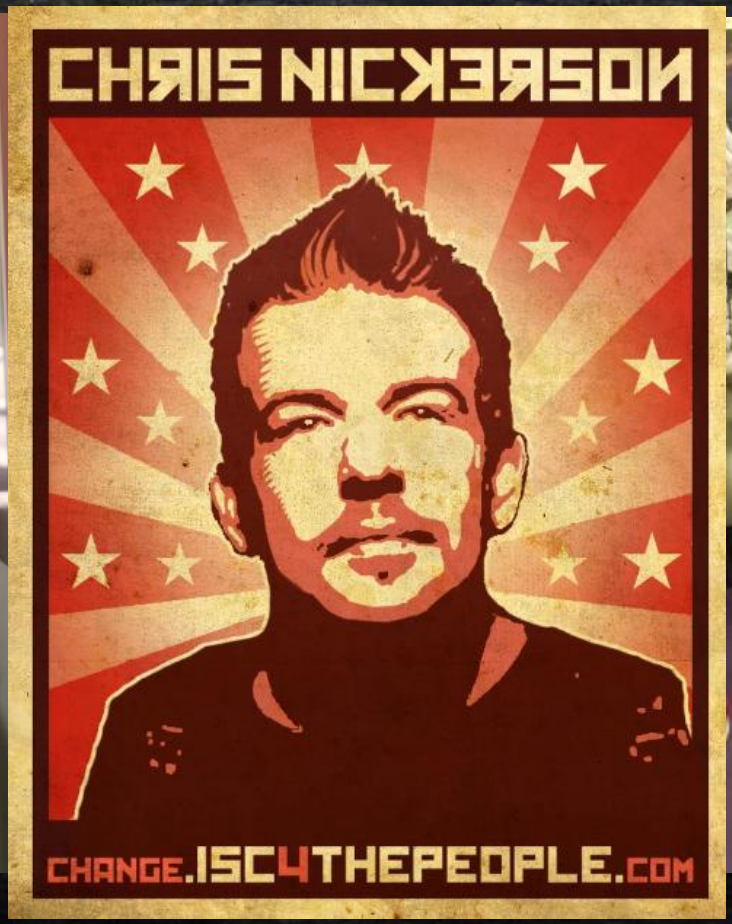
Flipping the Script

Becoming your attackers **boogeyman**

BEFORE
WE GET
STARTED

HI…I'm Chris



Disclaimer

Trigger Warnings

- Loud Anoying American
- Cursing
- Racism
- Religious Prejudice
- Sex
- Drugs
- Daddy / Abandonment issues
- Socio Economic Hate crimes
- Thin Skin
- Lack of sense of humor
- Sexual orientation
- Sexism
- Violence
- Vomiting
- Abuse
- Truth
- Fear
- Honesty
- Facts
- Emotions
- Tears

I

Exoticliability.com

AKA

cnickerson@laresconsulting.com

@indi303

http://www.scribd.com/Lares

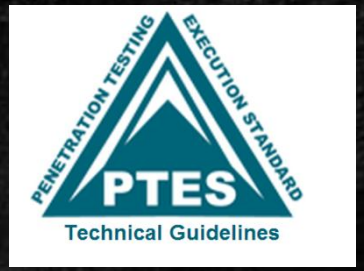
https://vimeo.com/laresconsulting


Shook,
Hardy&
Bacon L.L.P.


Sprint


KPMG


ALTERNATIVE
TECHNOLOGY INC
an Arrow Company


PENETRATION TESTING EXECUTION STANDARD
PTES
Technical Guidelines


A PROUD MEMBER OF
INFRAGARD
PARTNERSHIP FOR PROTECTION


.trust


CERTIFIED INFORMATION SYSTEMS
CISSP
SECURITY PROFESSIONAL
(ISC)2


ISACA
Trust in, and value from, information systems


www.lares.com

justbewell

hypnotherapy & nlp
making lives better

HOME | PRODUCTS | TESTIMONIALS | CONTACT US

ADDICTIONS/

You Can Stop Compulsive Shopping And Over-Spending

Book An Appointment »

Or visit our online shop »

HOME> ADDICTIONS> COMPULSIVE SHOPPING AND OVER-SPENDING>

Hypnotherapy and NLP to Help You Stop Comp

- How about you stop compulsive shopping,
- And take control of your overspending.
- How much better will you feel,
- When everything is under your control
- Overcome your shopping addiction,
- Hypnotherapy and NLP provides the cure.

Why Am I Addicted To Shopping?

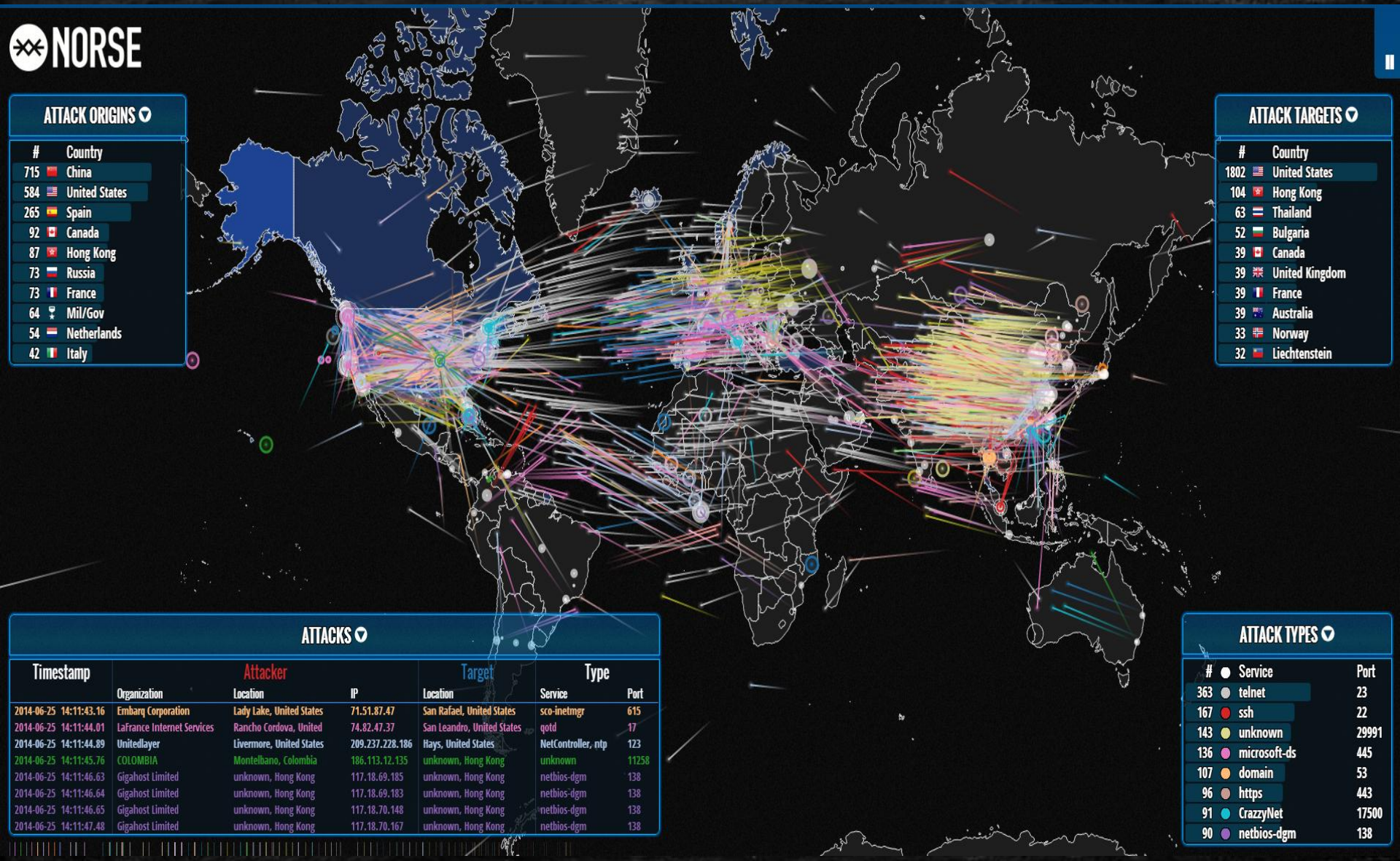
Two reasons:

Either:

You feel bad (bored or anxious or angry or depressed or desperate etc) and th
'bad' feeling so you go and shop. Often there is a 'good feeling' associated wit


SHIT'S ON FIRE, YO


You can't beat having friends like the Lares team whose amazing Badge System work makes this possible!
www.HackerStrip.com


NORSE
ATTACK ORIGINS
Country
715 China
584 United States
265 Spain
92 Canada
87 Hong Kong
73 Russia
73 France
64 Mil/Gov
54 Netherlands
42 Italy
ATTACK TARGETS
Country
1802 United States
104 Hong Kong
63 Thailand
52 Bulgaria
39 Canada
39 United Kingdom
39 France
39 Australia
33 Norway
32 Liechtenstein
ATTACKS
Timestamp | Attacker: Organization, Location, IP | Target: Location | Type: Service, Port
2014-06-25 14:11:43.16 | Embarq Corporation | Lady Lake, United States | 71.51.87.47 | San Rafael, United States | sco-inetmgr | 615
2014-06-25 14:11:44.01 | LaFrance Internet Services | Rancho Cordova, United | 74.82.47.37 | San Leandro, United States | qotd | 17
2014-06-25 14:11:44.89 | Unitedlayer | Livermore, United States | 209.237.228.186 | Hays, United States | NetController, ntp | 123
2014-06-25 14:11:45.76 | COLOMBIA | Montelbano, Colombia | 186.113.12.135 | unknown, Hong Kong | unknown | 11258
2014-06-25 14:11:46.63 | Gigahost Limited | unknown, Hong Kong | 117.18.69.185 | unknown, Hong Kong | netbios-dgm | 138
2014-06-25 14:11:46.64 | Gigahost Limited | unknown, Hong Kong | 117.18.69.183 | unknown, Hong Kong | netbios-dgm | 138
2014-06-25 14:11:46.65 | Gigahost Limited | unknown, Hong Kong | 117.18.70.148 | unknown, Hong Kong | netbios-dgm | 138
2014-06-25 14:11:47.48 | Gigahost Limited | unknown, Hong Kong | 117.18.70.167 | unknown, Hong Kong | netbios-dgm | 138
ATTACK TYPES
Service Port
363 telnet 23
167 ssh 22
143 unknown 29991
136 microsoft-ds 445
107 domain 53
96 https 443
91 CrazzyNet 17500
90 netbios-dgm 138

PENTEST KING

6 GREAT MODELS TO CHOOSE FROM! A TEST FOR ANY BUDGET!

If you're in the market for a new penetration test, look no further!

Level 1 – THE CLASSIC

This classic is sure to pretend to do something!

CALL FOR A QUOTE!

Level 2 – SMASH AND GRAB!

Get ready to have your network DESTROYED!!!!

Features:

- **No regard for your business!**
- **Huge reports**
- **Scanners, scanners, scanners!**

CALL FOR A QUOTE!

Level 3 – THE PACIFIER

You'll get a great report every time (that doesn't mean everything is ok...)

Features:

- **Might sell or service your office printer!**
- **Wont break anything!**

CALL FOR A QUOTE!

Level 4 – THE RFCist

The tester knows EVERYTHING! Except the why part!

Features:

- **Technical genius**
- **Anti-social**

Level 5 – THE AUDITOR

After careful risk analysis, your score is.....!

Features:

- **Tight, neat packages**
- **No technical know-how**
- **Lots of letters after their names**

Level 6 – THE RICH KID

They spent all their money on this tool... It's got to work!

Features:

- **Loves buzzwords!**
- **Includes really expensive accessories**

CALL FOR A QUOTE!

CALL FOR A QUOTE!

CALL FOR A QUOTE!

All of these products come with absolutely no guarantee whatsoever and the purchaser of these products should buy at his/her own risk...


RED
TEAM
GO!

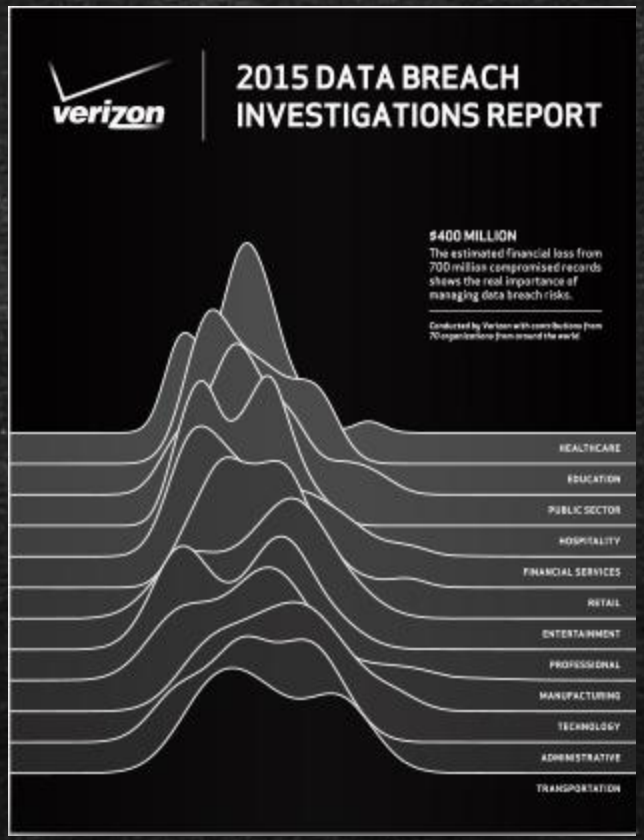
Custom Services

- OSINT
- SIGINT
- TSCM/ Bug Sweeping
- Exploit Development
- Tool Creation
- Attack Planning
- Offensive Consultation
- Adversarial Intelligence
- Competitive Intelligence
- Attack Modeling
- Business Chain Vuln Assessments
- Custom Physical Bypass Tool Design
- Reverse Engineering
- Other stuff I can't write down…

Your PowerPoint presentation makes Jesus cry.

GET TO WORK

YOU AREN'T BEING PAID TO BELIEVE IN THE POWER OF YOUR DREAMS.



http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf

- 80,000 security incidents and more than 2,000 data compromises from 61 countries.
- The top three industries affected are the same as previous years: Public, Technology/Information, and Financial Services.
- In 70% of the attacks where we know the motive for the attack, there's a secondary victim
- 23% of recipients now open phishing messages and 11% click on attachments

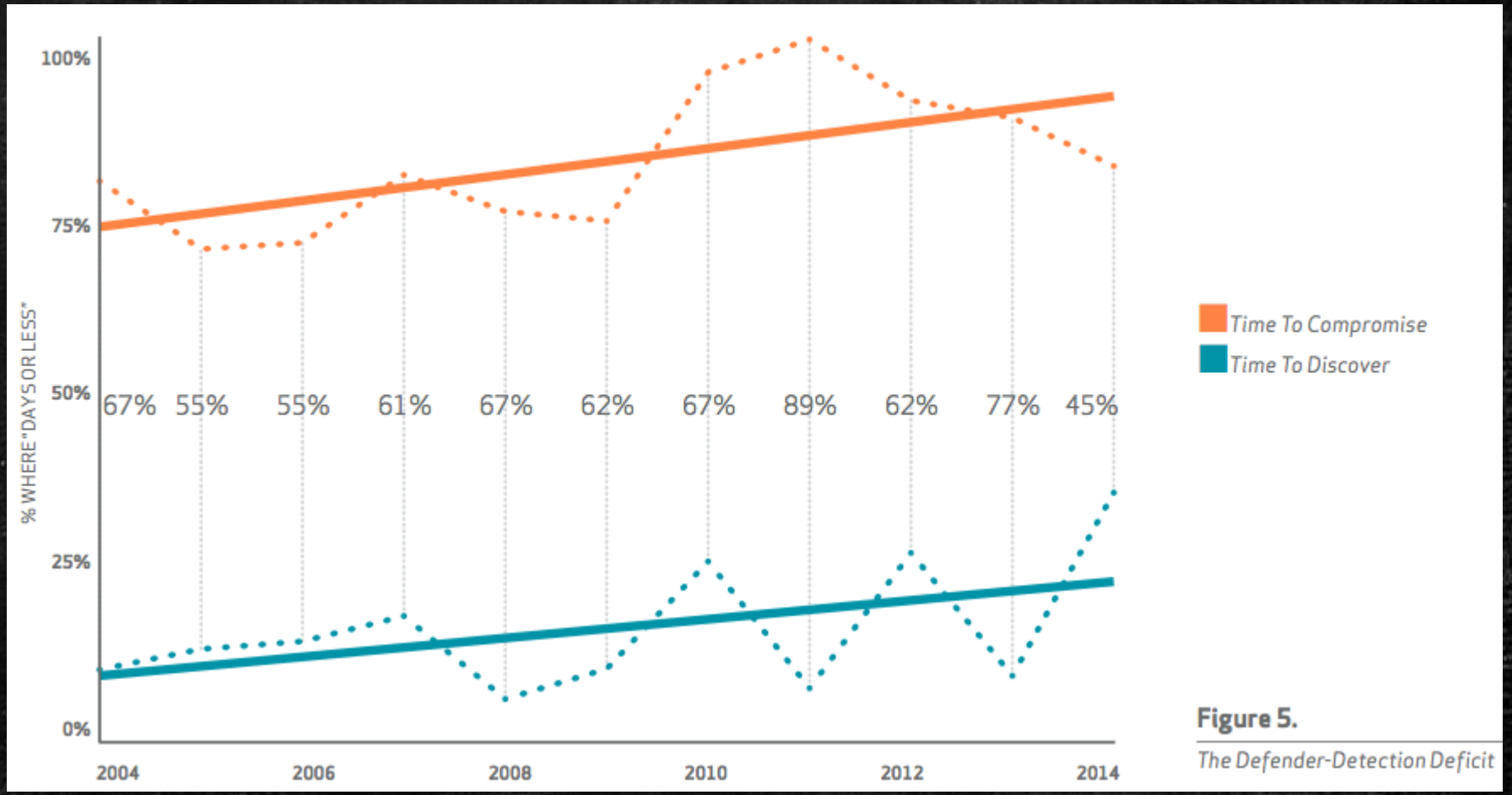
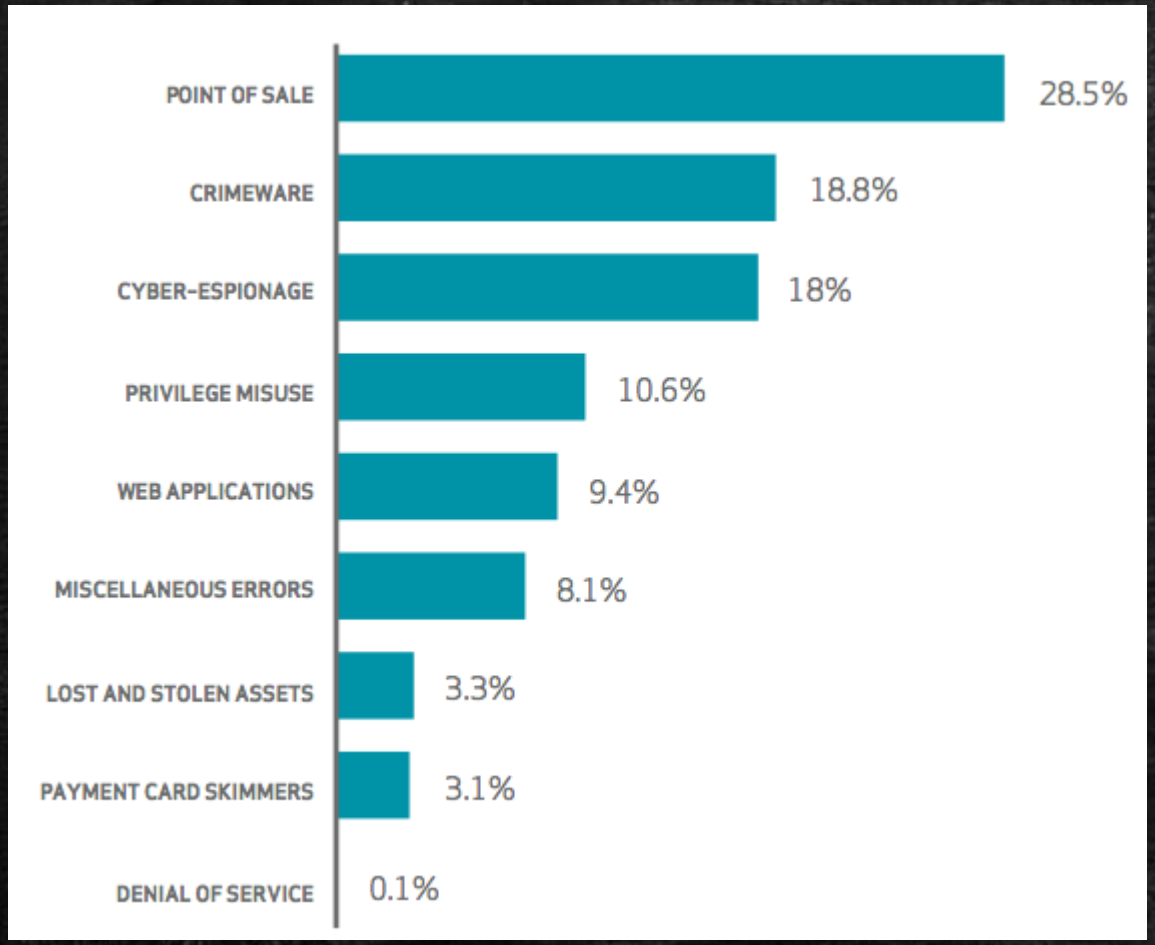


Figure 5.

The Defender-Detection Deficit



The common denominator across the top four patterns – accounting for nearly 90% of all incidents – is people


MAXIMUM SECURITY ENTRANCE

What do we do to try and DEFEND?

Buy stuff

- Firewalls
- WAF
- IDS/IPS
- AV
- SIEM
- Etc…

Test our stuff

- Conduct Audits
- Do "PenTests"
- Vuln scanning?
- Hire 3rd parties
- Hire industry "Experts"

And what happens?

WE STILL GET HACKED ALL THE TIME!!!!!!!


HERE
THERE?

Stories from the OTHER SIDE

When attackers DON'T WIN! Because your infosec is FORCE is

STRONG

The following things are a brief view of how customers have DEFENDED their networks and made it HURT for us.

GOOD SECURITY PROGRAMS ARE BUILT IN AND NOT BOLT ON

External Defenses

Sounds cool if you buy them and actually use them.

Rule #1 DON'T TALK TO STRANGERS

- Implemented blocks from all emerging threats lists
- Honeypots that if SCANNED or traffic was sent to, that IP was blocked. FOR GOOD.
- External SIEM integration that correlated logins. *Magic* the same address tries more than 3 usernames in an APP or SMPT it is banned for a certain time, if it happens after timeout, its banned for good
- Constant monitoring and baseline analysis of open ports. If it changed, a SEV1 ticket was created.
- Port scanning bans.
- Injection Bans
- Rejection of specific user agent strings (most tools out there have specific UA strings.
- Test it all until BLOCK mode WORKS! Monitor mode will just make you feel bad when u go back to your logs and see WHEN you got owned
- Big data like a boss. DO THREAT INTEL IN HOUSE!!!!
- Protect your OSINT (anonymize info like DNS records)

Quick fixes

Tons of free stuff out there to get you started.

- External honeypot Network http://threatstream.github.io/mhn/
- Drupal honeypot: https://www.drupal.org/project/honeypot
- External honeypot starter https://www.binarydefense.com/project-artillery/
- Tools to monitor open ports https://github.com/subinacls/Filibuster
- Wordpress honeypots http://leadin.com/plugins/wordpress-honeypot
- Use the Emerging threats lists and other threat intel feeds http://rules.emergingthreats.net/
- Check your osint / attack surface and threat landscape http://www.spiderfoot.net/

Phishing is for kids

#2 If you are going to talk, be sure u know who it is

- Disable SMTP verify/validation
- Mailer verification (**USE SPF**)
- Use Mail filtering solutions that can intercept ALL mail protocols Encrypted and unencrypted
- Strict enforcement of Site Classification
- Analysis of certificate age and domain age "marination"
- Inspect all attachments and disallow all attachments except for a very specific set which have mitigating controls at the host or can be used in a sandboxed viewer.
- Browser based controls whitelisting 3rd party loaders like java, flash etc… (or disabling all together)
- Verification of sender identity
- USE DNS ANALYSIS
- Don't forward DNS. Split DNS is not hard

Quickies

- Enable SPF
- Implement spamcop and other blocking lists https://www.spamcop.net/fom-serve/cache/291.html https://www.spamhaus.org
- Implement a Mail inspection gateway Preferably cloud and local
- Check security setting of SMTP/SPF/DNS http://mxtoolbox.com/diagnostic.aspx http://www.dnssy.com/
- Create Split DNS don't allow forwarding and use only the validated internal resolver. http://shorewall.net/SplitDNS.html
- Create automated Phishing reporting process in client or train users on process to submit
- Phish the users, test them, train them. And UPDATE your new hire training to include how to defend.

Internal Defenses

They ARE gonna get in, so knowing that
WHAT U GONNA DO ABOUT IT?

#3 Your internal network is a HOSTILE environment. Treat it as such

- Monitor inside MORE than outside.
- Portscan inside = Block and SEV1 IR response
- Segmentation of all servers from users.
- Create Classified zones, These will require 2 factor auth to a Jump box. Only jump box will be allowed to get into secured zone. Or Create VPN from user desktop directly into the Environment
- NEVER use VPN Pools. Always tie a user to a specific ip address and firewall rule limit ALL users to resources needed.
- Alert on ALL network device configuration change IMMEDIATELY.
- Use Netflows or other traffic analysis to identify top talkers and tune to find future anomalies
- Set up "HoneyNets"
- LOCK DOWN YOUR CONFIGS!!!!!!!
- Remove your default route and intercept all HTTP/S

Quick hits

- Set up your AV to disallow/ban anything port scanning
- Segment and firewall protect ALL servers from user segments
- Tune internal IDS to look for port scans and inappropriate user to server traffic. Also to identify protocols that shouldn't be used (ex. DNS traffic to things other than the registered internal DNS)
- Enable config monitoring on ALL network Devices http://www.rconfig.com/
- Restrict network device management to only validated addresses of network engineers OR setup mgmt. network that Engineers MUST vpn into.
- Monitor all ports open and look for changes. http://sourceforge.net/p/dnmap/wiki/Home/ distributed nmap
- Audit your configs https://github.com/pello/routerdefense https://www.titania.com/nipperstudio

Workstations are for WORK

#4 Users have the ability to use the companies resources.

- Only ad user accounts through secured methods. **DO NOT USE GPO's that have cPassword or add accounts with cleartext values.**
- Users should only be allowed to go to categorized sites. Any/all other traffic must be denied.
- Whitelist approved and managed software.
- Disallow Local admin privs
- Do NOT let local admins to log on remotely
- Randomize ALL local admin passwords
- Maintain internal software reports for updates
- Manage all the things
- Host based firewalls, IDS, and behavioral analysis
- SCAN ALL HOSTS for vulnerabilities on a regular basis

Quickies

- Manage local admin passwords with a commercial solution or some of the open sources. Microsoft LAPS https://technet.microsoft.com/en-us/library/security/3062591.aspx
- Create GPO's to whitelist or blackist services
- Remove admin rights
- Deploy anti exploitation defenses EMET https://support.microsoft.com/en-us/kb/2458544
- Harden your devices. Linux, AIX, BSD, Etc.. hardening https://cisofy.com/lynis/ Windows: Microsoft Baseline Security Analyzer
- Enable hardening locally with detection and protection http://www.fail2ban.org/ and windows firewall + AV
- Use Authenticated Scans to inventory software , find non compliant software and define hardening.
- Harden default images

It’s a SERVER...

Make it serve you.

#5 Servers have a specific purpose

- Do not install workstation software on a SERVER. Office, Adobe Acrobat….etc.
- Most of them do NOT need to connect to the internet. Not only does this mean NO access with firewall it means, unless the product would require an exception… NO BROWSER!
- Manage updates centrally and in house
- Segment, Segment, Segment….. SEGMENT THE DAMNED SERVERS!!!!!!!
- Standard image should have NO additional services installed and build guidelines should be followed before release.

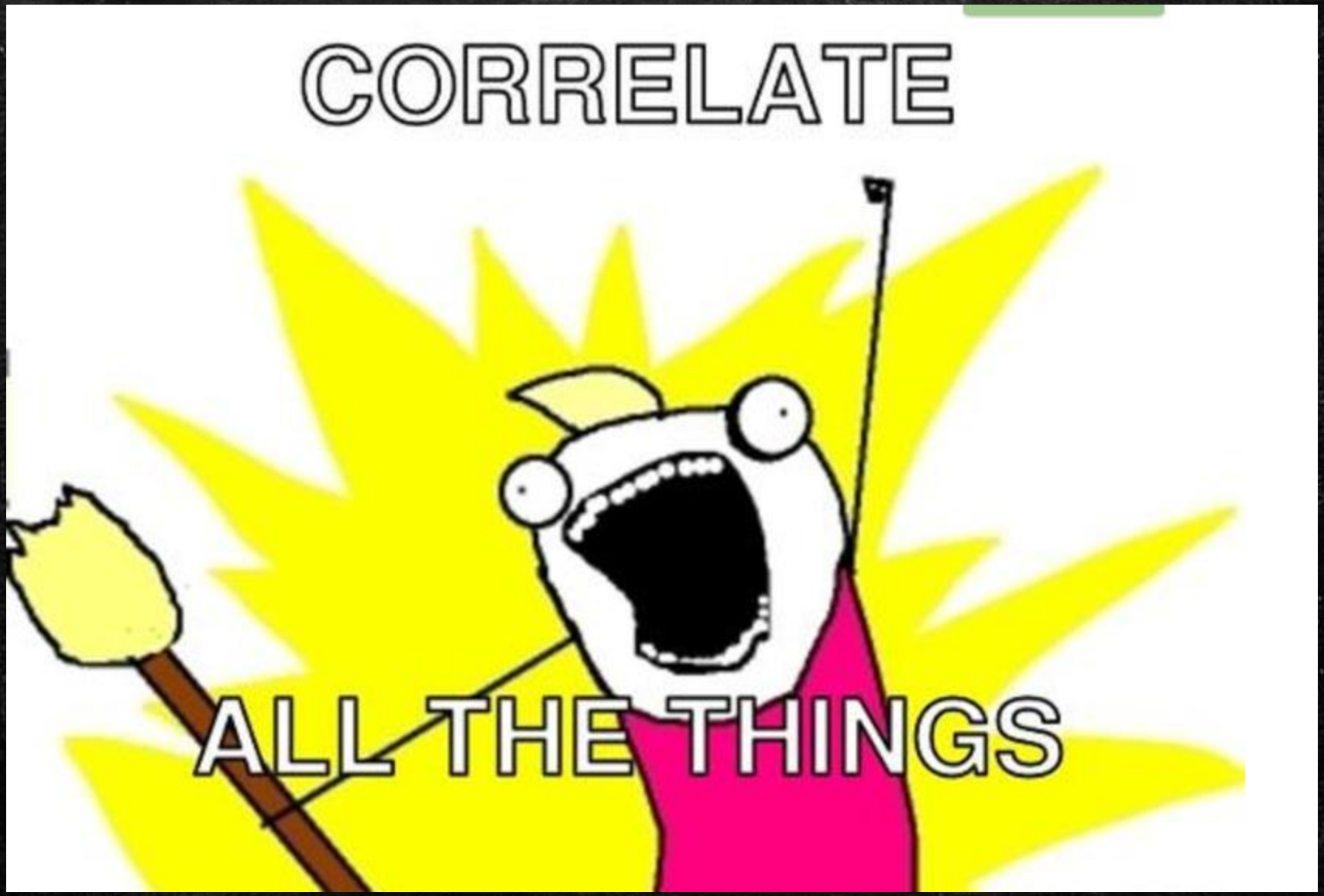
Quickies

- Remove all non essential services from servers RIGHT AWAY. They will run faster and more secure.
- Disallow install of any readers,office type programs or all workstation software in server hardening policy.
- Run Full AV on EVERY server.
- If you can't get ids.ips for your servers try opensource like OSSEC http://www.ossec.net/
- Use DLP https://code.google.com/p/opendlp/
- Disallow all non authenticated services.
- Do not allow the use of local accounts to log in remotely (that includes you SQL!!! No local sql accounts.. Integrate it)
- Make sure all report to the SIEM for security and login events.

Two Content Layout with Table

- First bullet point here
- Second bullet point here
- Third bullet point here

	Group A	Group B
Class 1	82	95
Class 2	76	88
Class 3	84	90


CORRELATE
ALL THE THINGS

#6 Awareness > Knowledge

- Create Security Event Management Environments
- Implement logging on ALL servers and eventually specific workstation events.
- Consolidate logging
- Have packet capture capabilities on the fly in ALL areas
- Looks at the hotness of attack surfaces and start to build defenses based on techniques used in offense. (ex. WMI trend)

Quick hits

- Set up IDS/IPS and have it report to a consolidated platform
  http://blog.securityonion.net/p/securityonion.html
  https://www.bro.org/
- Set up logging and have it report to a consolidated platform
  http://www.splunk.com/en_us/products/splunk-light.html
  http://blog.qbox.io/welcome-to-the-elk-stack-elasticsearch-logstash-kibana
- Make it easy for yourself. Help correlate from multiple sources.
  https://bammv.github.io/sguil/
- Fireeye-FLARE Windows WMI-IDS
  https://github.com/fireeye/flare-wmi/tree/master/WMI-IDS

WMI (WHY?)

- 1. An attacker uses WMI as a persistence mechanism • Effect: Instances of __EventFilter, __ EventConsumer, and __FilterToConsumer Bindingare created. An __InstanceCreationEvent event is fired.
- 2. The WMI Shell utility is used as a C2 channel • Effect: Instances of __ Namespace objects are created and modified. Consequently, __ NamespaceCreationEvent and __Namespace ModificationEvent events are fired.
- 3. WMI classes are created to store attacker data • Effect: A __ClassCreation Event event is fired.
- 4. An attacker installs a malicious WMI provider • Effect: A __Provider class instance is created. An __ InstanceCreationEvent event is fired.
- 5. An attacker persists via the Start Menu or registry • Effect: A Win32_ StartupCommand class instance is created. An __ InstanceCreationEvent event is fired.
- 6. An attacker persists via other additional registry values • Effect: A RegistryKeyChangeEvent and/or RegistryValueChangeEvent event is fired.
- 7. An attacker installs a service • Effect: A Win32_Service class instance is created. An __InstanceCreationEvent event is fired.

Shout out to all my Basic bitches.

```
10 PRINT "HOLLA"
20 GOTO 10
RUN
```

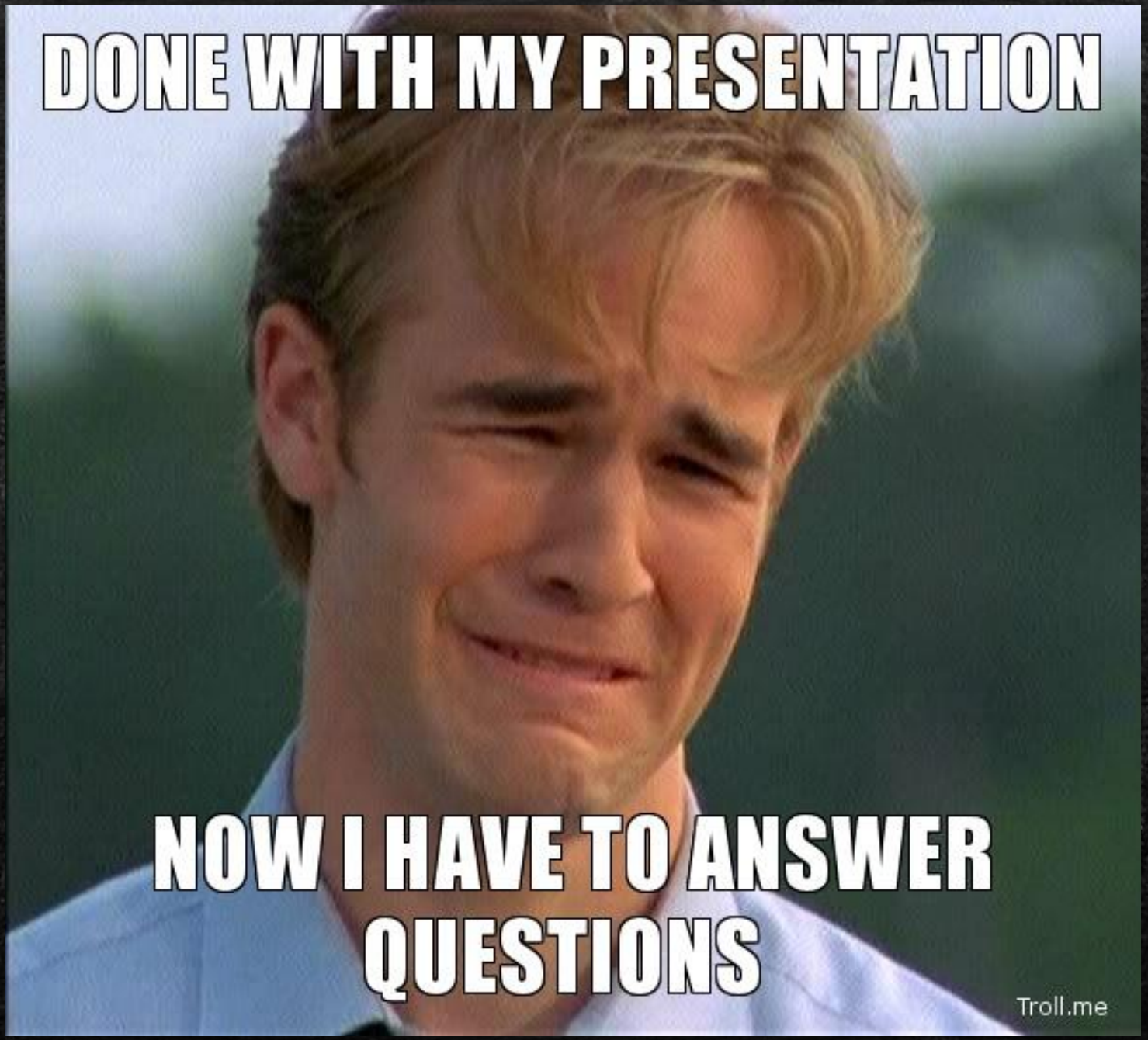
Get your IR game in order

#7 In order to say you have an information security program you need to have an Incident response plan.

- Humans must be assigned to this plan and the tasks in it
- Security response center must have defined plans, SOP's, and most of all a fully capable SLA to the business on risk response/identification
- Active defenses to stop attack in progress
- Forensic/ malware analysis on the fly and manual
- Coordination with all teams to have real time response.
- Defined skillsets of all team members to be sure the right skill for project.

Quick ways?

- Build a proper IR team. Define skills and roles to be played
- Setup an IR action group (from all of IT and the business)
- Create defined IR plans that can be run as part of DR plans
- Build an IR Team Sandbox toolkit / lab
  https://zeltser.com/build-malware-analysis-toolkit/
- Build an Incident response platform
  http://blog.crowdstrike.com/new-community-tool-crowdresponse/
  https://github.com/google/grr
  http://techblog.netflix.com/2015/05/introducing-fido-automated-security.html
- https://www.bestpractical.com/rtir/
- https://www.mediawiki.org/wiki/Download


DONE WITH MY PRESENTATION
NOW I HAVE TO ANSWER QUESTIONS
Troll.me

Exoticliability.com

AKA

cnickerson@laresconsulting.com

@indi303

http://www.scribd.com/Lares

https://vimeo.com/laresconsulting