

SOC – SIC

20-25 Vision

Christoph PELLKOFER

OVERVIEW

Outline

- The Most Important CISO in the World
- Past SOC
- Future SOC
- Final Thoughts

Intent

- Share our experience and research into building a SOC
- Help you build a better SOC

Let me tell you how us
big boy CISOs build a SOC



Lou:
The Most
Important
CISO
in the World

Lou, we're afraid of hackers and people without ties, protect our business

Thank you for this opportunity. I will build us the WORLD'S GREATEST SECURITY OPERATIONS CENTER



THE SUPER IMPORTANT CORPORATION

Acceptable Use Agreement for SIC Computing Resources

The following document outlines guidelines for use of the computing systems and facilities located at or operated by The Super Important Corporation (SIC). The definition of SIC and SIC computing facilities will include all computer facilities of the computer facilities stored on magnetic tape, floppy disks, and other media used in support of the SIC. The "user" of the computing system is responsible for ensuring that all SIC computing facilities in an effective manner.

First, write long, complex, and super detailed polices that show everybody your incredible expertise with information security

SIC accounts and facilities are not to be used for non-SIC purposes and may be prosecuted to the full extent of the law. The use of SIC accounts and facilities may constitute grounds for criminal prosecution.

In the text below, "users" refers to users of the SIC computing systems and facilities.

1. The SIC computing systems are unclassified systems. Therefore, classified information may not be processed, entered or stored on a SIC computing system. Information is considered "classified" if it is Top Secret, Secret and/or Confidential information that requires safeguarding or control in the interest of National Security.
 2. Users are responsible for protecting any information used and/or stored on/in their SIC accounts. Consult the SIC User Guide for guidelines on protecting your account and information using the system protection mechanisms.
- Users are required to report any weaknesses in SIC computer security, any incidents of security or violation of this agreement to the proper authorities by contacting SIC <IT Security> or by sending electronic mail to infosec@sec.com.
- Unauthorized attempt to access any data or programs contained on SIC systems for which they do not have authorization or explicit consent of the owner of the data/program, the SIC Officer.
- Users are prohibited from divulging Dialup or Dialback modem phone numbers to anyone.





Then buy all the best tech.
That blue one is in the
Gumper Magic Quaalude





Hire a team of the best of the best security gurus

Watch logs, me?!?!
I am a CISSSQPADRSICA certified
Monitoring logs is for the intern



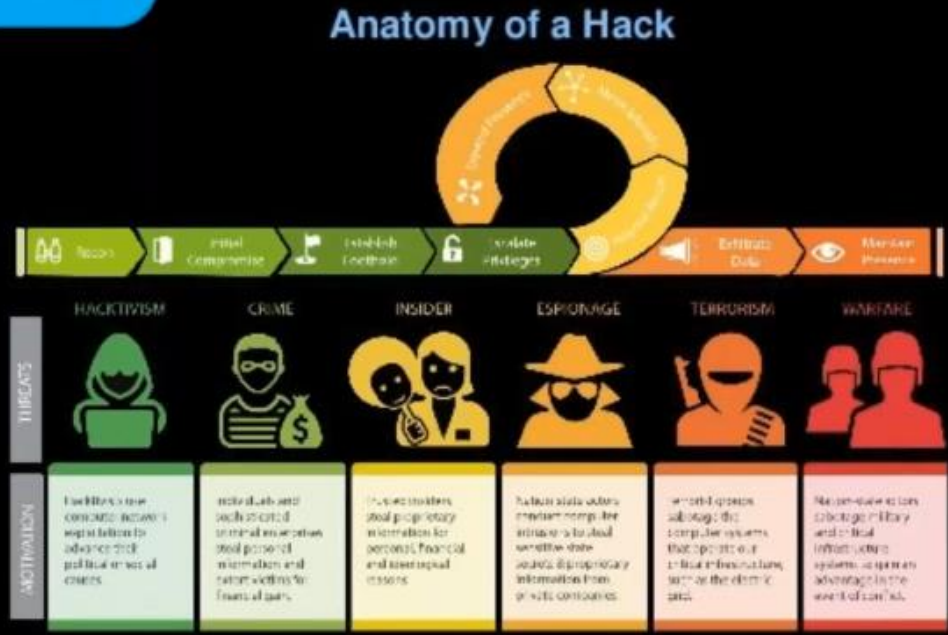
Tell those stupid
developers and
users NO!





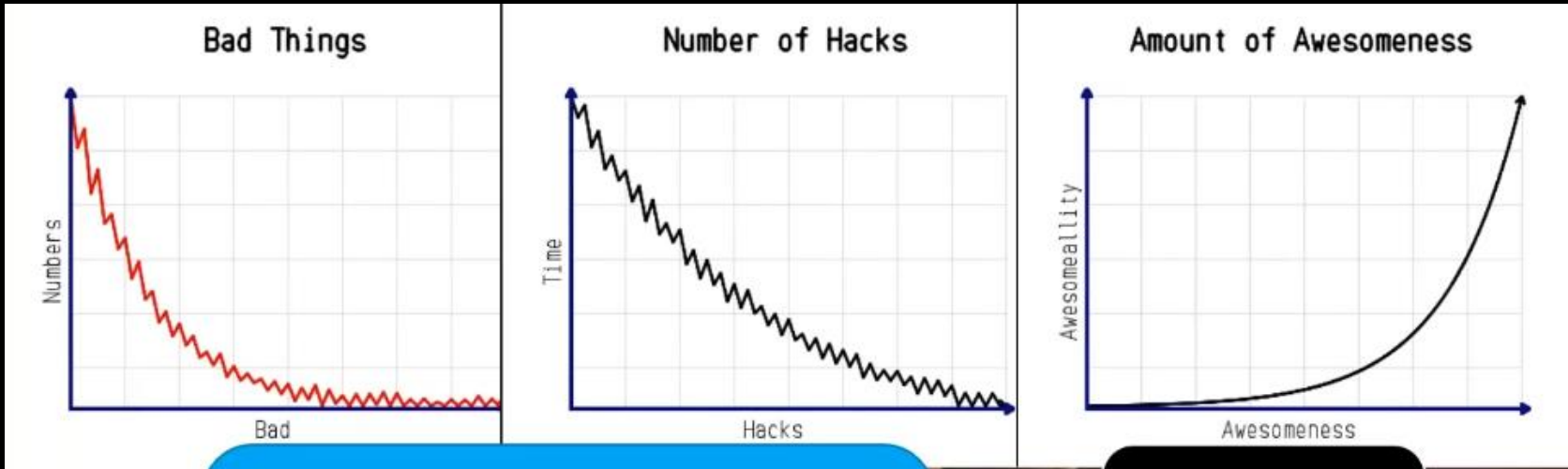
Have everybody on your team be an uber-hacker. Go to every hackercon.

"ANATOMY OF A HACK"
 Learn how to protect your business





Get a massive bank of huge monitors to display those *pew pew charts* to executives, because this is how you stop the hacker scum



Show the boys on the board how secure you made everything with *metrics* and all those big-boy appliances

Yes, yes, yes, we have the best cyber



In 2019 Lou's company had a huge breach

Lou's SOC never saw it

All those big boy products never stopped it

None of those policies did a thing

They found out when a customer informed them

Lou had to meet with the Boys on the Board

Their decision was swift...



Don't be Lou

The Breached Database Directory

Last updated: Sun Sep 15 2019 01:04:01 GMT+0200 (Central European Summer Time)

Search: _____

Lots of these big boys had a BIG impressive SOC

Entries	Database	Detected Hashing Algorithms	Category	Dump Date	Acknowledged?
19,546	WidM.nl	MD5	Fanpage - TV Series	2019-08	
6,846,740	StockX.com	MD5(salt)	Shopping	2019-07	Yes
562,122	Forums.XKCD.com	MD5(phpBB3)	Comics	2019-07	Yes
92,807	GetPaidTo.com	VB	Paid to click	2019-07	
42,835	Ruby-Web-Links.com	plaintext	Search Engine Optimization	2019-07	
20,407	Pirate4x4.no	VB	Vehicles - Cars	2019-07	
12,842	Soundohm.com	MD5	Shopping - Music	2019-07	
8,571	FLStudio.biz	VB	Software & Music	2019-07	
3,151	SW-RPG.net	VB	Gaming	2019-07	
179,673	MCPSP.com	VB	Gaming	2019-06	
117,902	Android.net	VB	Software - Android	2019-06	
75,343	InsideTheGame.it	VB	Gaming	2019-06	
55,122	SocialEngineerd.net	MyBB	Social Engineering	2019-06	
30,285	LegendaryHacker.com	VB	Hacking	2019-06	
29,941	KNOPPIX.net	VB	Technology	2019-06	
9,545	Velocia.ca	VB	Sports - Cycling	2019-06	
7,699	MacGurus.com	VB	Technology	2019-06	
5,784	CoasterFriends.de	VB	Entertainment	2019-06	
4,888	ProjectGorgon.com	bcrypt	Gaming	2019-06	
2,143	AmstelveenCollege.nl	plaintext & MD5 & no passwords	Education	2019-06	

Source: <https://vigilante.pw/>



Past SOC

Are you waiting for something **bad**?



Or going somewhere **good**?

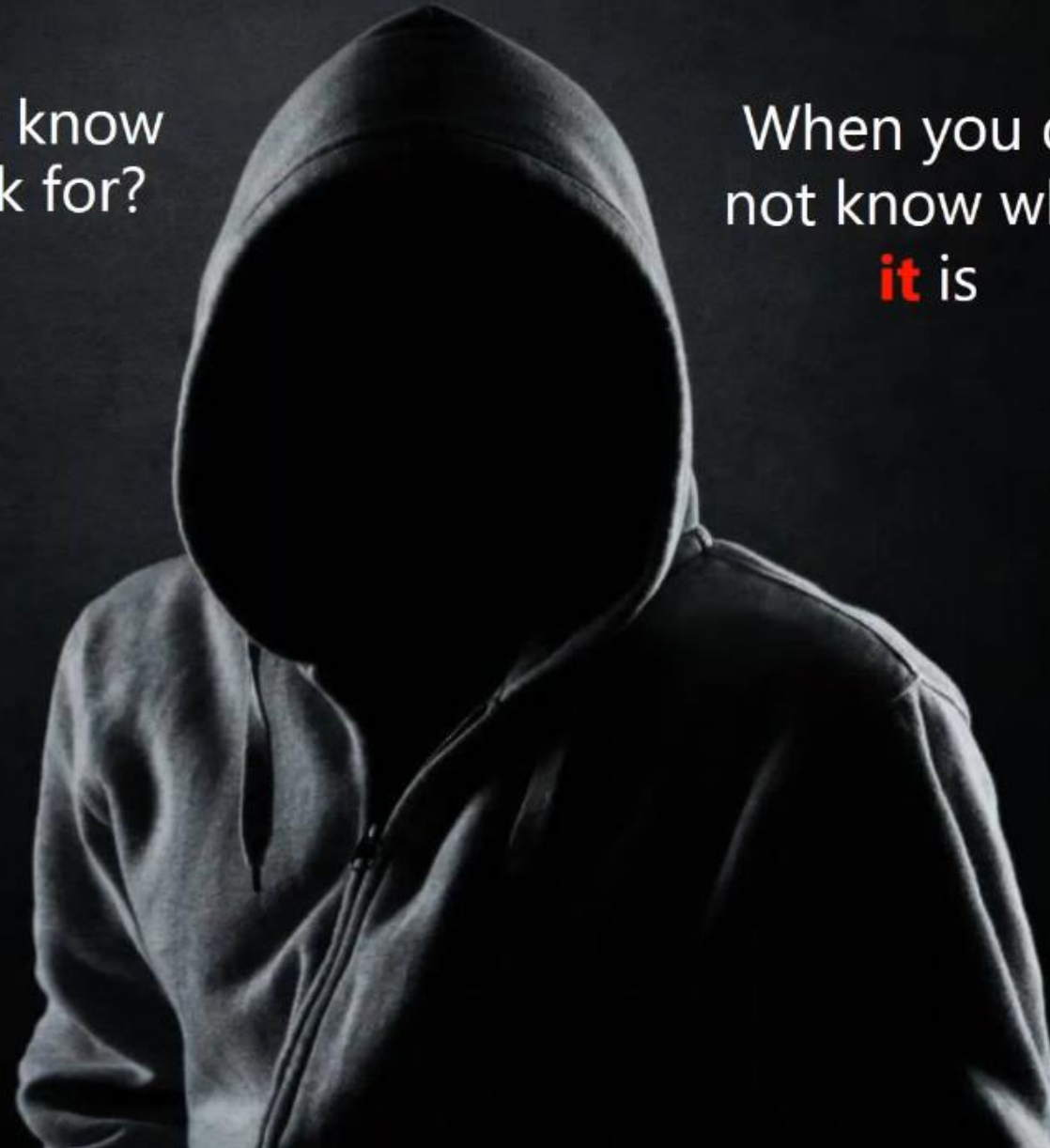
The 4:00 AM Fallacy





It assumes you know everything

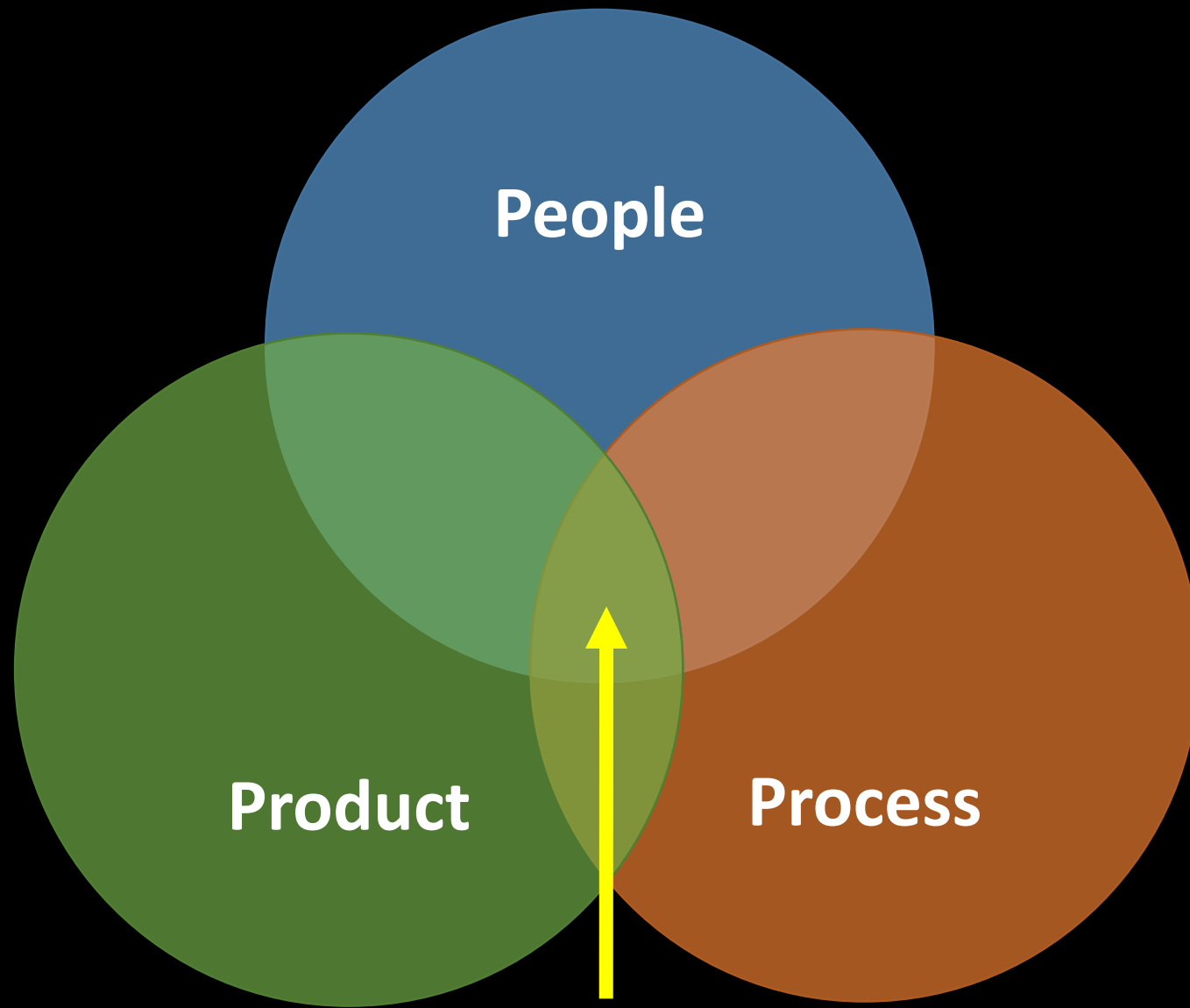
How do you know
what to look for?






When you do
not know what
it is



passive security is a failure



SOC 2019

SOC Components	Strengths	Weaknesses
 <p data-bbox="570 368 891 459">People</p>	<ul data-bbox="1116 139 1421 311" style="list-style-type: none"> • Creative • Intuitive • Innovative 	<ul data-bbox="1602 139 2033 382" style="list-style-type: none"> • Inconsistent • Unreliable • Slow • Might be drunk
 <p data-bbox="545 773 912 865">Product</p>	<ul data-bbox="1116 539 1431 711" style="list-style-type: none"> • Consistent • Reliable • Fast 	<ul data-bbox="1602 539 2018 716" style="list-style-type: none"> • Uncreative • Merciless • Might kill us all
 <p data-bbox="555 1179 907 1270">Process</p>	<ul data-bbox="1116 945 1508 1179" style="list-style-type: none"> • Creates trust • Demonstrates capability • Comfortable 	<ul data-bbox="1602 945 2135 1122" style="list-style-type: none"> • Inflexible • Be used against you • Creates blindspots

SOC Components



FOCUS ON
AGILITY AND INGENUITY



FOCUS ON
FORMALITY AND STRUCTURE

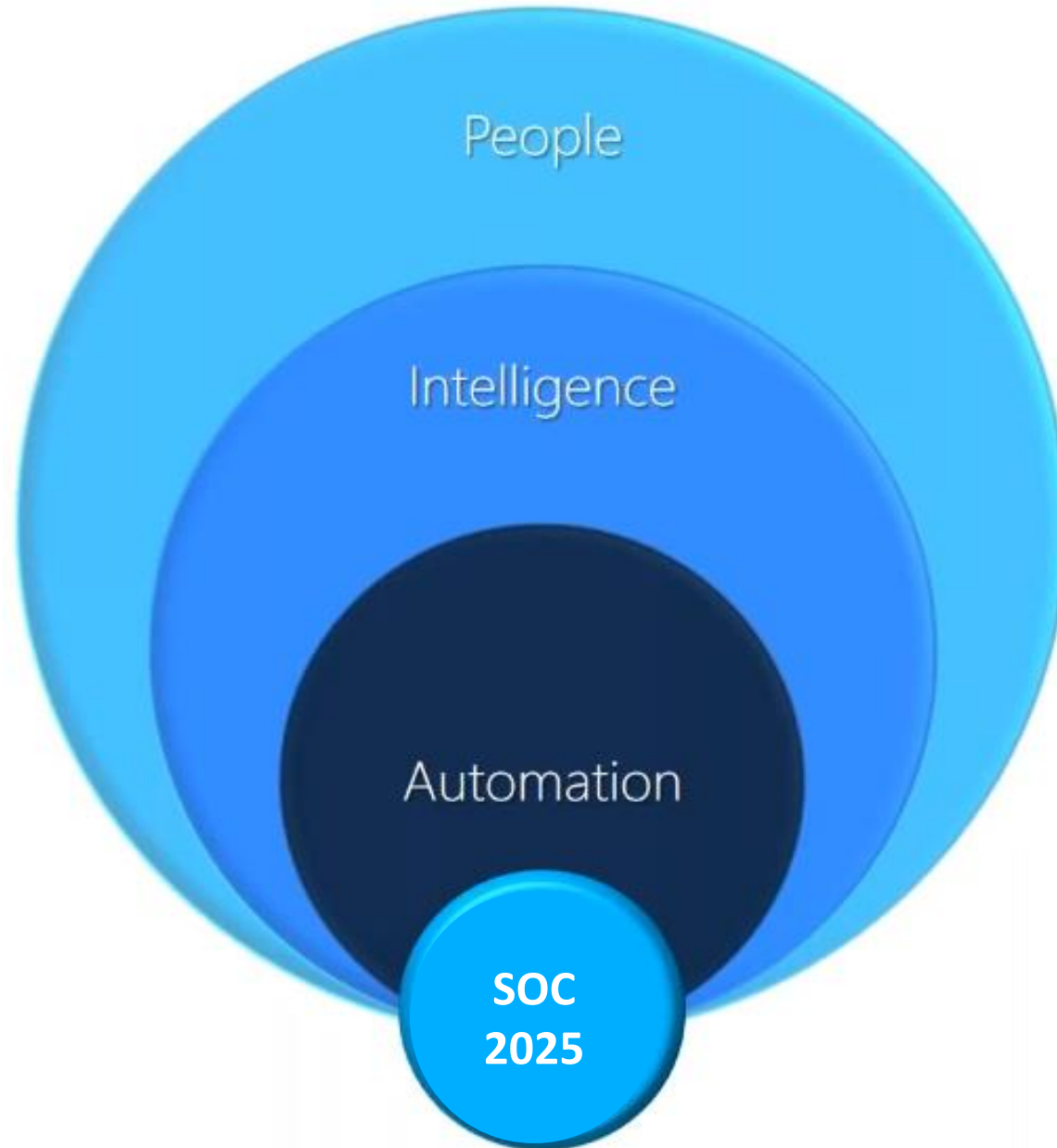


FOCUS ON
FLEXIBILITY AND DIVERSITY

FUTURE SOC



SIC 2025



1. HIRE FOR 2025

- Stop trying to hire for tech skill
- Hire for opportunity and behavior

Look for these people...

- Creative
- Agile
- Resourceful
- Curious
- Ethical
- Social, great communicator
- Enjoys a challenge
- Hands on tech skill

Avoid these folks...

- Rigid, highly formulaic
- Obsession with hacker culture
- Enforcement mentality
- Tech tinkerer
- Antisocial
- Blames others
- Audit/compliance focus



SOC analysts of the future

2. GET THE TECH

You do need tech...

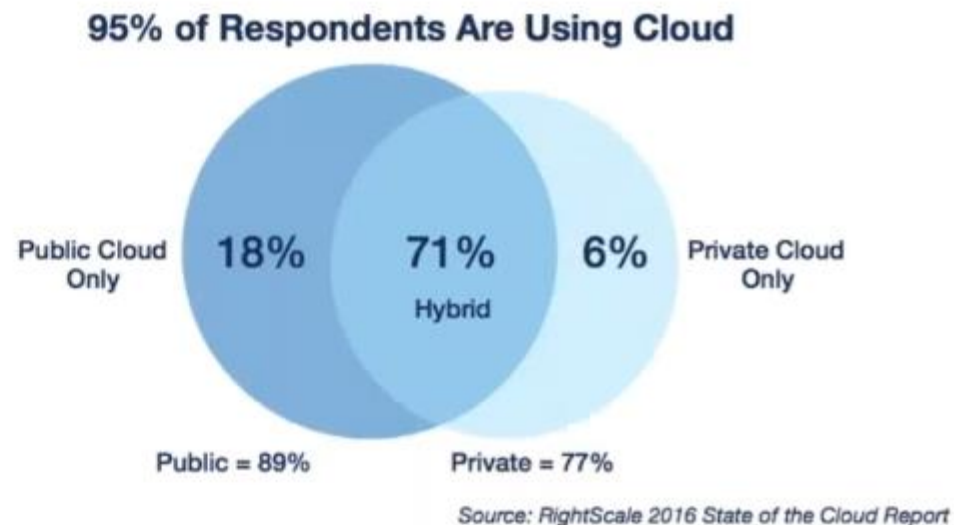
- SIEM
- Perimeter NGFW
- Core NGFW
- Vulnerability Scanning
- Comprehensive asset inventory
- Endpoint security
- DNS security
- File integrity
- Behavior analytics
- Forensic tools

You may also consider

- Deceptions
- DLP
- User behavior analytics

3. GET YOUR SIC SERVICE IN THE CLOUD

- This is where IT is going
- Only 17% of workloads are in the cloud
- Cloud is more secure
- Cloud can scale to any size
- You can put your team anywhere
- Connect to on-premise
- AWS is #1 by a long shot, and its more flexible



4. AMASS INTERNAL INTELLIGENCE

Breaches and attacks happen because people are not paying attention to the real problems

- How well patched are you?
- How do you manage change?
- How many open vulns do you have in your environment?
- Who is watching the SIEM logs?
- What are they looking for?

You need to understand your current situation

- Do an enterprise risk assessment
- Inventory everything
- Consistent, but flexible change management

5. AMASS THREAT INTELLIGENCE?

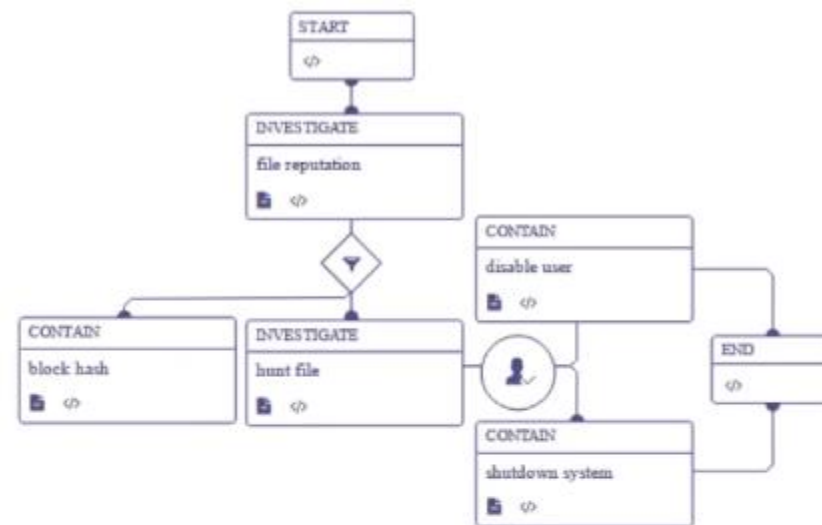
- Vendors: NGFW, SIEM, etc.
- Free...
 - Virustotal.com
 - Malwr.com
 - Malware-Traffic-Analysis.net
 - Shodan.io
 - Emergingthreats.net
 - Iblocklist.com
 - Nullsecure.org
 - FireHOL
 - Packetstorm
 - Open Source Security
 - Cymon.io
 - Abuse.ch
 - CVE-Mitre/NIST NVD

6. USE INTELLIGENCE TO HUNT FOR BAD BEHAVIOR

- Query to bad DNS
- Movement of sensitive files
- Use of credentials
- Bad actor list matches:
 - Botnet C&C
 - Ransomware
 - Proxy/TOR
- Workstation activity during non-user hours
- Server activity outside of historical patterns
- Use of suspicious protocols:
 - IRC
 - FTP
 - Telnet/SSH
 - RDP/VNC
 - SNMP
 - SMB/NetBIOS
- Bruteforce attempts
- Unusual outbound bandwidth consumption

7. AUTOMATE AND INTEGRATE

- Point security solutions are useless
- Integrated “fabrics” that can react at multiple levels
- Fusion of detection, prevention, logging, and response technologies
- You will never react fast enough...
 Get your people out of the reaction mode, into the analysis mode
- Numerous automation platforms: Phantom, Hexadite, Swimlane, FireEye, Exabeam



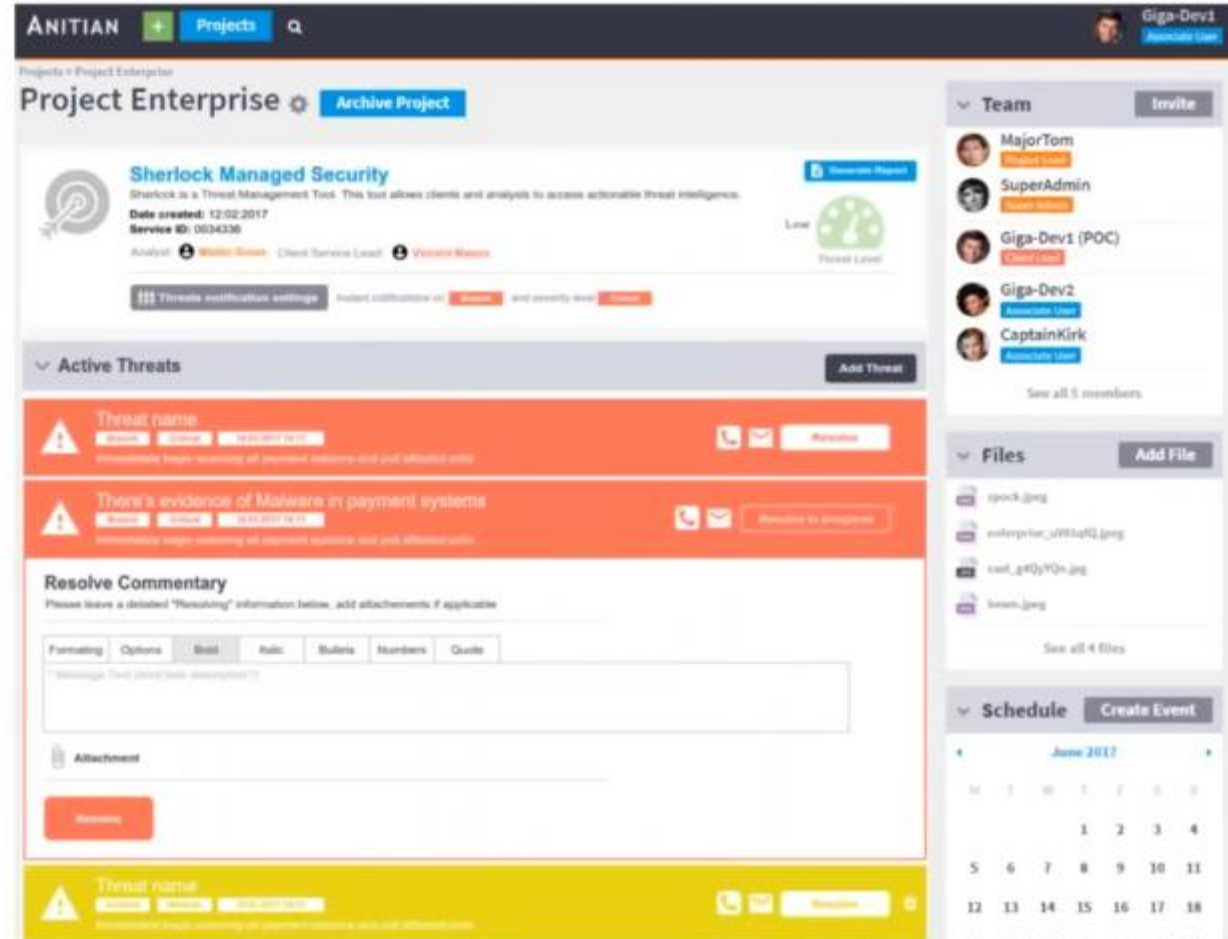
8. AUTOMATE BLOCKING AND HUNTING

- Autoblock at the core, perimeter, endpoint, everywhere you can
- Automate hunts, send them to dashboards on the SIEM
- Automate a response to strange user behavior <- this is tough to do
- Automate the wipe and build of all end user machines
- Automate forensic data collection at endpoint
- Be able to searching and eradication of any file based on hash

- Automate, so your analysts spend time reviewing the output, not sifting through data

9. GET SIMPLE REPORTS & DASHBOARDS

- Stop with the pew pew charts and pointless graphs.
- Focus on threats that need to be remediated



10. GET TO DISPOSABLE IT

1. Fully automate the build of your environment
 - a. System and storage instantiation
 - b. Configuration, hardening, patching
 - c. Code deployment
 2. On a regular basis, recreate the whole environment
 3. Migrate from old to new (automatically)
 4. Destroy the original
- Disposable IT forces
 - Structure into your systems
 - Agility into your people
 - Flexibility into processes

Final Thoughts



GET USED TO THE NEW NORMAL

- People are indifferent to breaches
- Privacy is gone, we expect our data to be stolen
- Data is rapidly declining in value
- Automation and orchestration allows for rapid detection, response, and repair
- Technology is necessary, but not what makes a difference
- Hacker tactics are not evolving

FINAL THOUGHTS

- It is not strength that protects you, its *agility*
- It is not compliance that assures, it is *discipline*
- It is not what you know, its what you *do not know*
- It is not skill that makes somebody qualified, it is *behavior*

Future SOC is not technology, per se;
it is *people, intelligence*, and *automation*
for a rapid response to threat

CONCLUSION

*Evolve to PIA**
or
accept the Cyber security risk

Thank you