

A Quick Intro

Vuln Counts, Risk  
Scores, Reputation,  
Zero Trust  
and  
BUDGET...

Unify  
Prioritize  
Execute

The Challenge

Finding a  
Better Way!

Q&A

# A PROGRAMMATIC APPROACH TO ENTERPRISE SECURITY

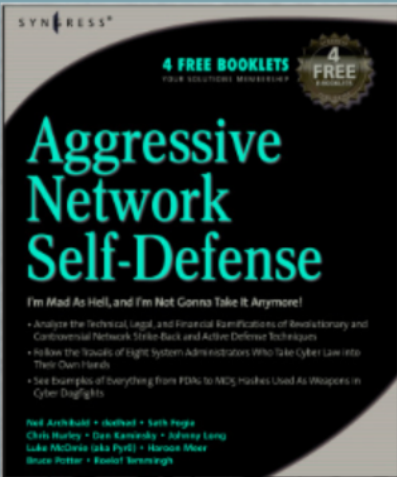
Luke McOmie | Pyr0

VP | Offensive Security 6/13/2023



The Omni Richmond: June 13-14, 2023





# Whois: Luke McOmie

## Biography

Luke McOmie is the Vice President of Offensive Security at Blue Bastion (an Ideal Integrations Company). In this role he is leading the development of our new Red Team and OffSec practices. These new units of our business support multiple industry verticals with specializations in enterprise security, ethical hacking, red teaming, physical security, threat modeling, social engineering, and incident response.

Luke joined Blue Bastion and Ideal Integrations on April 20th, 2021, bringing 25+ years of experience. Luke is industry certified and recognized for his excellence in leadership, execution, communication, and delivery. He has lead research groups (Distributed Computing / Machine Learning), Labs & Risk and Compliance programs (COALFIRE / ALTTECH / ARROW / BT / OWL) and conducted security engagements for federal agencies & state governments, financial, healthcare, industrial, and other global businesses. These efforts and his diverse background have all contributed to his extensive and unique understanding of the challenges and risks that threaten the modern business and operating environment.

## Community Involvement:

- Off Grid Hackers \ Hummingbird Hollow
- OG-CTF / 303CON (UPCOMING!!!)
- He founded Skytalks in 2008
- 303
- Security Tribe
- RETIRED - Goon at the DEF CON Security Conference.
- Tiger Team (TV Show)
- Aggressive Network Self-Defense (Book)



# In the next hour, we will:

- Discuss the challenge
- Old ways are not necessarily the best ways
- Change our mindset, approach, and understanding of how to win
- See how we have focused on the wrong metrics for success
- Address why budget, time, and capabilities are the upper limits
- Talk through ways to do it better

# Why is it so damn hard?



Best  
Practices  
gone bad!

We are learning

Nintendo Hard



# Audience Participation

Why do you have a security program?

Why do you conduct assessments?

How often do you perform pentesting?

Change up your security provider?

Find yourself fighting fires / focusing on immediate need?

What are you focused on this year?

Do you have cyber insurance, have you used it?

How many partners do you have? (MSSP/MDR/OFFSEC/INFRA/ETC.)

Who determines your final scope?

Do you have executive support?

What you said:

We want to check  
the box

(compliance /insurance driven)

What we hear:

No real value

The legal minimum

Not secure, not going  
to be secure.



What you said:

We perform pentesting  
once a year

What we hear:

We are barely  
scratching at the  
surface!

"I go to the gym once a  
year"

What you said:



What we hear:  
We are barely  
scratching at the  
surface!

"I go to the gym once a  
year"



What you said:

"We change our provider yearly."

What we hear:

We start from scratch.  
Wash, Rinse, Repeat.  
Year over Year

=

VERY LITTLE  
PROGRESS FOR THE  
EFFORT

What you said:

Fighting Fires  
and

Focused on Immediate  
Needs

What we hear:

Very Expensive  
Ticking Bomb  
Slow (if any) forward  
progress.



## What you said:

We are focused on:

MFA / IAM

Security Awareness

SOC2 | PCI | HITrust

Endpoint Protection

## What we hear:

We are spending all of our resources (time, money, people) on accomplishing a single project vs. making big moves.

## What you said:

We have cyber insurance  
Never been hacked  
We aren't a target

## What we hear:

Don't care.  
Don't know.  
Don't get it.

What you said:

Company A = Infra

Company B = MSSP

Company C = OFFSEC

Company D = GRC

Company E = Etc.

What we hear:

Lack of focus,  
communication, and  
connection. We repeat  
work, 3PA/Audit  
fatigue, always over  
tasked

What you said:

Our legal controls project  
scope and approach

What we hear:

Lack of understanding  
of purpose, need,  
value



## What you said:

Can't get executives to understand the problem, risk, impact, challenge.

## What we hear:

Can't get budget and I'm speaking the wrong language

# It's not hard, it's just new (to you!)

Be prepared to fail.

Adopt a "learning mindset".

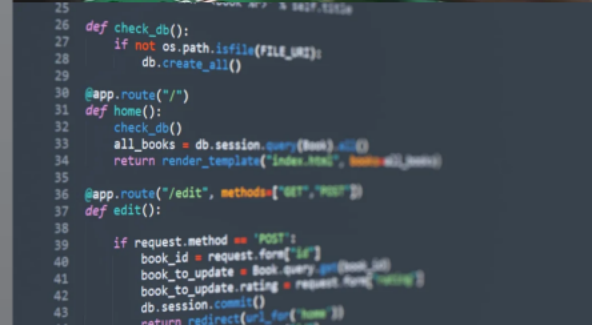
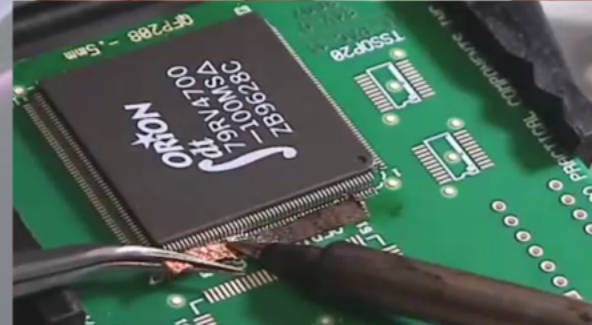
Set clear goals.

Adapt, Adopt, Achieve.

Use different learning mediums / methods.

Learn from someone with more experience.

Practice, Practice, PRACTICE



```
25
26 def check_db():
27     if not os.path.isfile(FILE_URI):
28         db.create_all()
29
30 @app.route("/")
31 def home():
32     check_db()
33     all_books = db.session.query(Book).all()
34     return render_template("index.html", books=all_books)
35
36 @app.route("/edit", methods=['GET', 'POST'])
37 def edit():
38
39     if request.method == "POST":
40         book_id = request.form["id"]
41         book_to_update = Book.query.get(book_id)
42         book_to_update.rating = request.form["rating"]
43         db.session.commit()
44         return redirect(url_for("home"))
```

# Nintendo Hard

Refers to extreme difficulty, characterized by trial-and-error gameplay and limited or nonexistent saving of progress. The term originated with Nintendo Entertainment System (NES) games from the mid-1980s to early 1990s



# Flipping the Game

"Impossible" games could often be beaten with tricks. Learning patterns, understanding timing, finding secrets, better ways, and tons of patience.

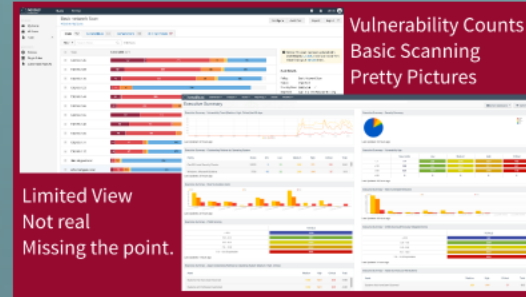
WINNING THROUGH MASTERY OVER TIME





# Big Spends - Little Returns

You're Doing it Wrong:  
Vulnerability Counts  
Industry Risk Scoring  
Reputational Damage  
Zero Trust



NESSUS Professional Scans Settings admin

### Basic network Scan

Configure Audit Trail Report Export

Hosts 112 Vulnerabilities 272 Remediations 500 VPR Top Threats

Filter Search Hosts 112 Hosts

Host	Vulnerabilities
192.168.1.46	147 278 59 189
192.168.1.83	60 333 86 184
192.168.1.10	42 320 81 186
192.168.1.53	28 48 508
192.168.1.44	39 293
192.168.1.66	22 228 52
192.168.1.55	113 172
192.168.1.40	65 154
192.168.1.56	48 166
192.168.1.11	15 87 178
192.168.1.12	15 87 177
data.tehgeek.local	12 266
sshsvr.tehgeek.local	26 16 225

tenable.sc Dashboard Analysis Scans Reporting Assets Workflow

Notice: This scan has been updated with Live Results. Launch a new scan to confirm these findings or remove them.

Scan Details  
 Policy: Basic Network Scan  
 Status: Imported  
 Severity Base: CVSS v3.0  
 Modified: April 1 at 1:00 PM (Live Results)

# Vulnerability Counts Basic Scanning Pretty Pictures

Limited View  
Not real  
Missing the point.

### Executive Summary

Executive Summary - Vulnerability Trend (Medium, High, Critical) last 90 days

Last Updated: 22 hours ago

Executive Summary - Outstanding Patches by Operating System

Family	Score	Info	Low	Medium	High	Critical	Total
CentOS Local Security Checks	10576	0	31	505	371	133	1040
Windows - Microsoft Bulletins	7750	40	23	269	544	37	913

Last Updated: 22 hours ago

Executive Summary - Most Vulnerable Hosts

Last Updated: 22 hours ago

Executive Summary - CVSS Scoring

Score Range	TOTALS
< 2.9	1230
3.0 - 4.9	1801
5.0 - 6.9	3362
7.0 - 10.0	2812
7.0 - 10.0 Exploitable	48%

Last Updated: 4 hours ago

Executive Summary - Asset Outstanding Patches by Operating System (Medium, High, Critical)

Asset	Medium	High	Critical	Total
Systems that have been Scanned	1932	1921	335	4188
Systems with Software Inventoried	1932	1921	335	4188

Executive Summary - Severity Summary

Last Updated: 22 hours ago

Executive Summary - Vulnerability Age

Age	New Hosts	Low	Medium	High	Critical
< 7	114	283	2948	1947	486
< 30	263	551	3975	2311	627
< 90	824	1317	4972	2458	748
> 90	0	0	0	0	0

Last Updated: 20 hours ago

Executive Summary - Most Vulnerable Networks

Last Updated: 22 hours ago

Executive Summary - CVSS Scoring (Previously Mitigated Items)

Score Range	TOTALS
< 2.9	362
3.0 - 4.9	2298
5.0 - 6.9	4972
7.0 - 10.0	8584
7.0 - 10.0 Exploitable	52%

Last Updated: 4 hours ago

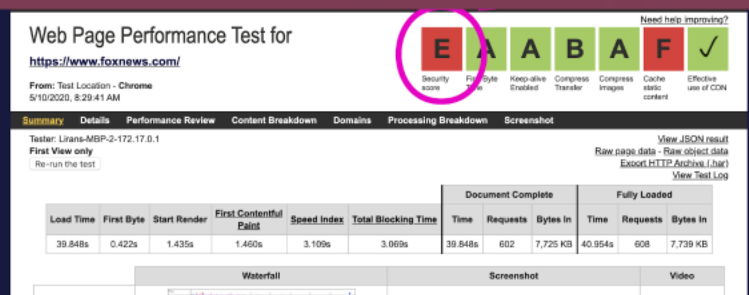
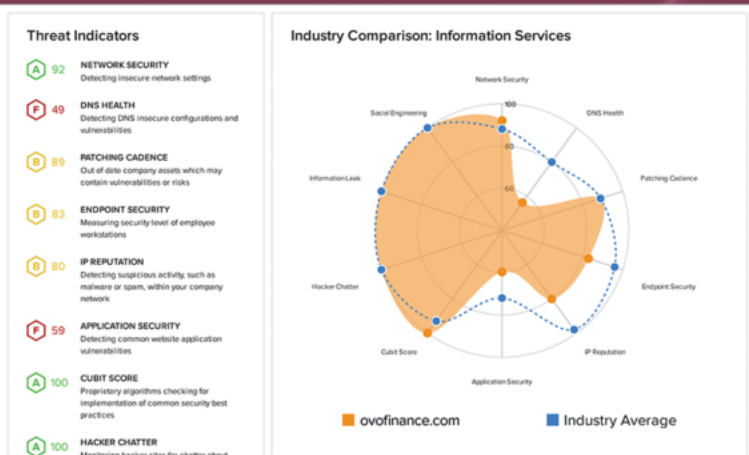
Executive Summary - Asset Summary by MS Bulletins

Asset	Medium	High	Critical	Total
Systems that have been Scanned	209	544	37	850

# Assessment of Business Cybersecurity

October 2018

Published by the U.S. Chamber of Commerce and FICO



# Security Scoring

"Primary Colors & Single Syllables"

Industry standard scoring problem

Roll ups and digging deep

Limited capabilities

Accepted Risk?

Mitigating Controls?

A lot of fine tuning and tweaking

Bad business practices (fear)


Insurance companies. . . .

Value for spend



# Reputational Damage

JOURNAL ARTICLE

Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018 

Christos A Makridis 

*Journal of Cybersecurity*, Volume 7, Issue 1, 2021, tyab021,

## Abstract

While data breaches have become more common, there is little evidence that companies that incur them experience a persistent decline in financial performance or security prices. Using new firm-level data between 2002 and

**yahoo!**

 Microsoft

  
The First American Corporation

**Linked in**

**facebook**

**JPMORGAN  
CHASE & CO.**

 **Adobe®**

**ebay**

  
**Marriott.**

**THE  
HOME  
DEPOT**

**EQUIFAX**



# Zero Trust

## Great goal but. . . .

### Most Significant Challenge Building Zero Trust Strategy



# A Better way...

Automate the simple, repetitive things

Tune your tools, teams, and talents!

Bringing all the pieces together

Shared knowledge (NO SILOS!)

Measure once / report many

Risk/Budget focused vs. vuln counts

Collaborative approach vs. zero knowledge

Quicker compliance driven decisions

TAKE A PROGRAMATIC APPROACH





**WHAT IF I TOLD YOU**

**IF YOU DO IT RIGHT THE FIRST TIME YOU WILL  
NOT HAVE TO DO IT AGAIN**



**IT'S THE ONLY WAY  
IF YOU WANT IT JUST RIGHT**



**WOW**

# A Programmatic Approach



Business:

Mission

Vision

Culture

Budget

Focus

Customers

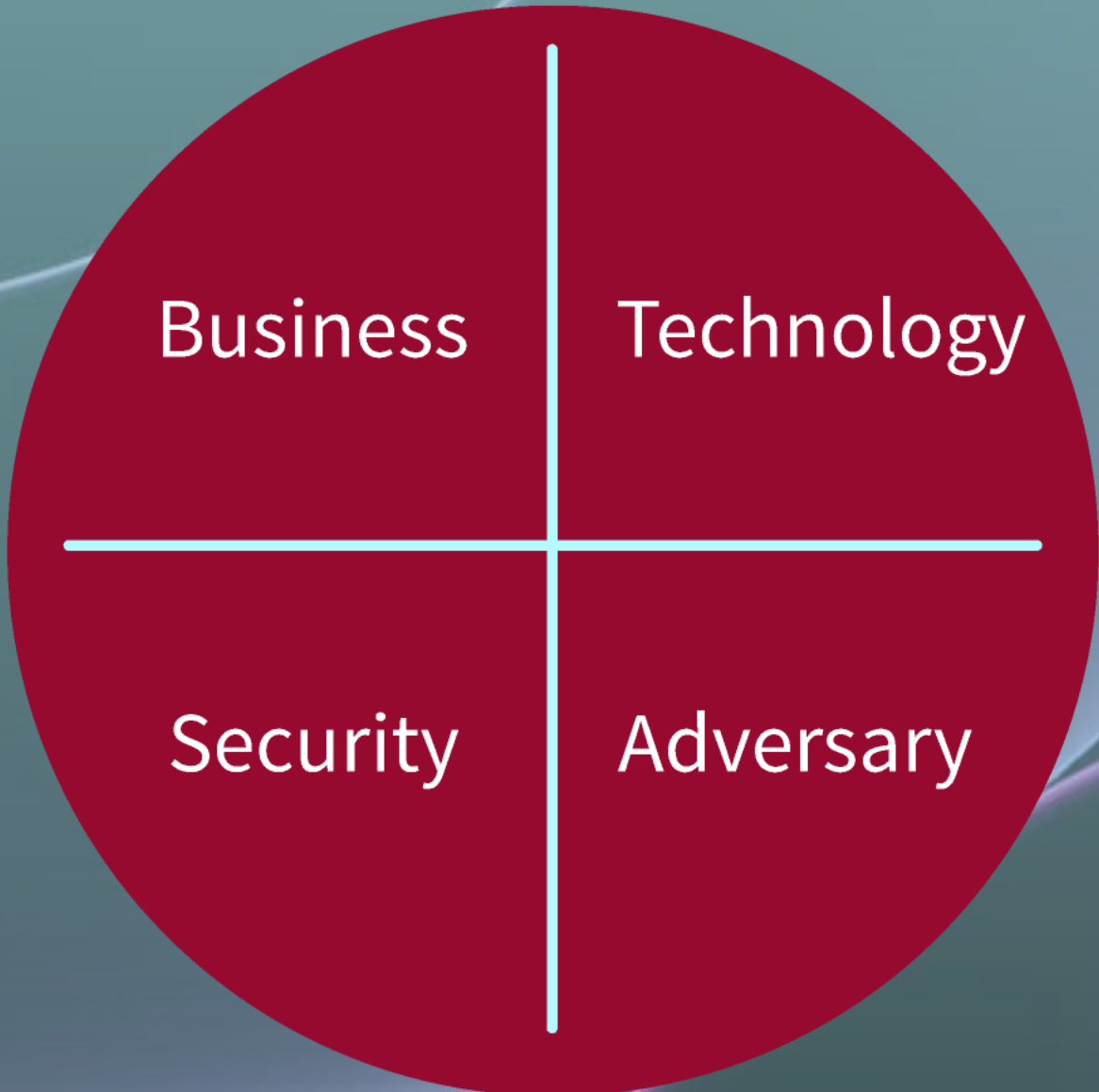
Leadership

GRC

BC/DRP



# A Programmatic Approach



Technology:  
Inventory  
Capabilities  
Staff / Partners  
Value vs. Debt  
Gaps  
Maturity  
Policy &  
Procedures

# A Programmatic Approach



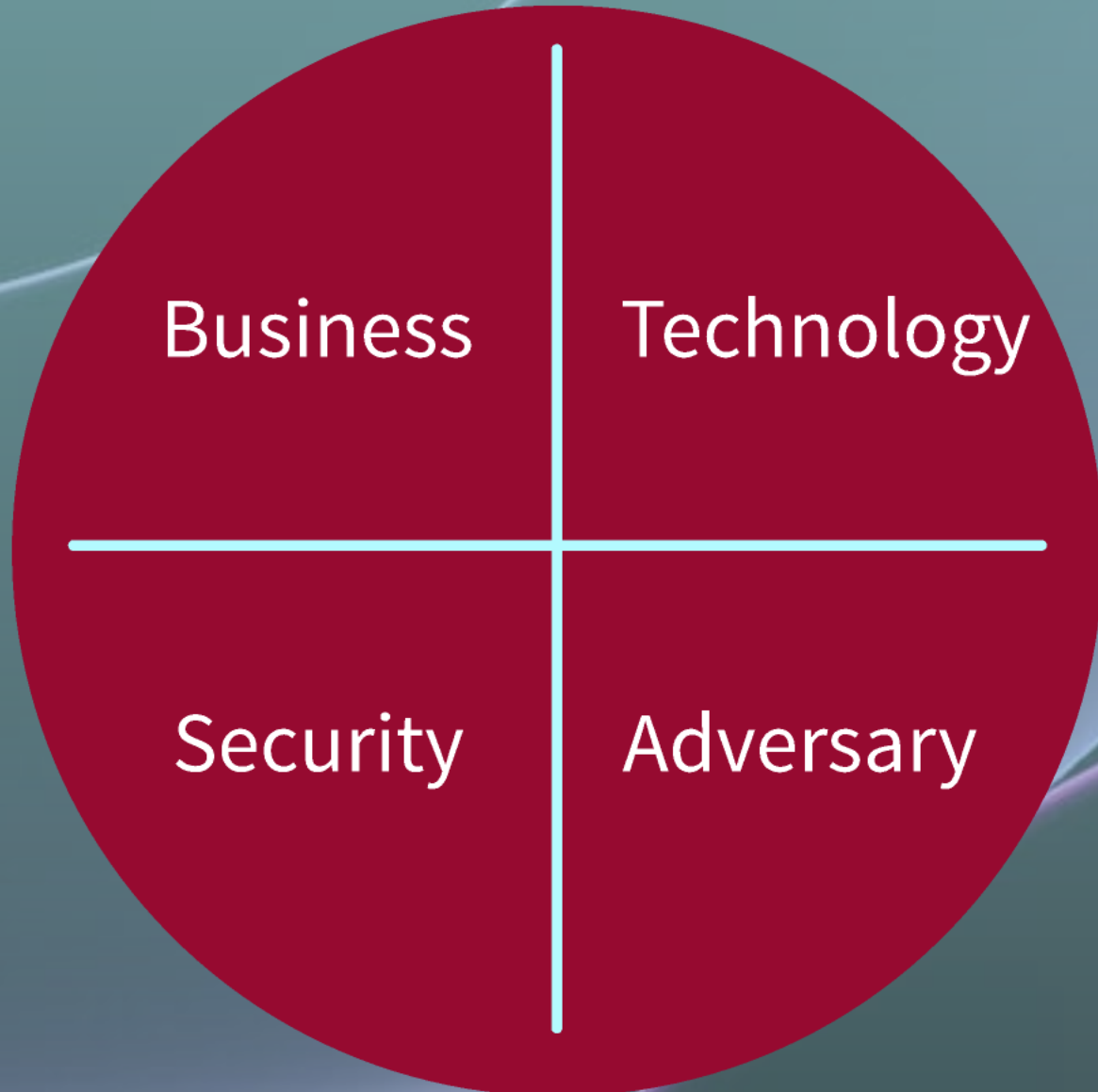
Security:  
Maturity  
Controls  
Solutions  
Challenges  
Effectiveness  
Assessment  
Vaildation

# A Programmatic Approach



Adversary:  
Capabilities  
Known Threats  
Awareness  
Prepped 4 Worst  
Historical Events  
Risk & Impact  
Industry considerations  
Tomorrow's enemy

# A Programmatic Approach



Planning:  
Risk Model  
Big Picture  
Priorities  
Big Wins  
Next Steps  
Acceptance

Program Execution:  
Executive Buy-in  
Continuous Approach  
Quarterly, Monthly, Weekly?  
Partner or Internal?  
Tracking change  
Being flexible  
Stay out of the weeds  
Getting it right



# Unify, Prioritize, Execute

Enabling success



**GRC**  
Considerations

**Playing**  
**Together**

**Key**  
Points

# GRC

## Are you asking the right questions?

- Do those specific controls apply to your business?
- How many different compliance requirements overlap?
- What in your process can be automated?
- What else do your efforts (P&P) enable or support?
- Massive data set – what you gonna to do with it?
- Why are you spending you budget to meet your requirements vs. doing what's best for you and yours?

**ASK: “WHY DOES IT  
MATTER?”**

**Never because I need to  
“check a box”**

# Getting the team back together!

## Creating a unified vision, approach, and mission.

- Create a team compromised of leaders from all areas of your business.
- Use strong Project Management practices to set expectations, goals, and ensure forward movement.
- Focus on the larger task at hand (don't get lost in the weeds)
- Understand where overlap occurs and where you can reuse, recycle, repurpose data and efforts.
- Focus on doing what is right – not what is legally required.
- This is a steering committee – it's purpose is to define security goals, understand the mission, create a security program/plan that addresses the unique and specific needs of your business.





# A Programmatic Approach

## Key points for success:

- Moving away from one off engagements to enterprise programmatic relationships. Focus on assess & address vs. dealing w/ the dumpster fires, compliance demands, and moving targets.
- Look at the WHOLE business (P,P,T,D), not just your CDE, Cloud, or external facing environments
- Eating the elephant - chefs pairing / menu – bite at a time, focus on what makes the biggest change, then mop up.
- Create what is right for you – don't adopt the “industry standard”
- Security becomes part of the business process and culture vs. an afterthought or check point.
- Utilize real time / actionable data vs. point in time reporting to enable quick, intelligent planning, response, and decision making.
- Leverage your data to tell the story, understand why things are happening not just what is happening.
- Remember to focus on the bigger picture, then drill down.





# | Q&A

Hacker  
Happy Hour

Other  
Projects

THANK  
YOU!





**FLIPPER ZERO**



**OFFGRIDHACKERS.COM**







## Luke (Pyr0) McOmie

Vice President - Offensive Security at Ideal Integrations

Talks about #cso, #mssp, #hacking, #redteaming, and #informationsecurity

Loveland, Colorado, United States · [Contact info](#)

6,668 followers · 500+ connections

# THANK YOU!

*Ways 2 Connect*



Edit profile

## Luke McOmie / Pyr0

@lmcomie

That one guy.

#RedTeam since 1996, #OffSec since 94, #Offgrid since 2017 :)

Off Grid Hacker Nerd.

📍 Mountains of Colorado 🌐 [offgridhackers.com](http://offgridhackers.com) 🎂 Born December 23, 1977

📅 Joined May 2011

facebook



## Luke McOmie

3.4K friends

