



Hook, Line, & Cyber

A Fisherman's Guide to Building a Security Operations Center

Introduction

Nick Gipson

Founder & CEO, Gipson Cyber



- 7 years experience in Security & Technology
- Built & operated 5 SOC's in various organizations; including US Cyber Command
- Led SOC teams for private & public sector orgs; such as US Central Command
- 6 year prior career as an Army Reconnaissance Soldier (OIF/OEF)



Outline

1. Planning
2. Design
3. Establishment
4. Operation
5. Improvement
6. Expected Results
7. Conclusion



Speaker's Goal -

To provide an understanding of the process involved in establishing a SOC, no matter the budget, *or lack thereof*.



Planning



Phishing for Information

Understand the Threat Landscape

Information is the bait that attracts cybercriminals to a target

- Examine potential threats to the network environment
- Run vulnerability scans
- Create mitigation plans for each finding
- Build monitoring solutions around mitigations
 - See Design section
- Use baseline such as CIS Benchmark



Moby Dick by Jerry LoFaro
Image sourced from fineartamerica.com

Chart the Course

Security Documentation

- Incident Response Plan
- Continuation of Operations Plan
- Disaster Recovery Plan
- Service Level Agreement
- Playbooks
 - Incident Response Process
 - Phishing Remediation
 - Host Isolation
 - Graceful Server Shutdown
 - Etc.



Ask the Local Fisherman

Open-source Threat Intelligence*



OPEN THREAT EXCHANGE



Paid-source Threat Intelligence

digital shadows_



MANDIANT
ADVANTAGE

*Use Three or More Sources



Design



Cast a Wide Net

Digital Footprint Assessment

1. **Identify** all online assets owned by the company
2. **Analyze** the security measures in place for each asset
3. **Evaluate** the company's online reputation
4. **Determine** the potential risks associated with the company's online presence
5. **Develop** a plan to address any identified risks and vulnerabilities



Select the Correct Gear to Catch the Intended Fish

Security Product Selection

- **LimaCharlie - My Favorite All-in-one Tool**
- Use Footprint Assessment
- Focus on Zero Trust for Endpoint & Business Security





Establishment



Select the Right Fishing Spot

SOC Location - On Premise

- Dependant on physical infrastructure
- Limited by geolocation for hiring
- Impacted by local weather & disasters
- 24x7 Ops causes burnout
- High night shift turnover rates
 - Breaks Circadian Rhythm

SOC Location - Distributed (virtual)

- Independent from infrastructure (cloud)
- Highly selective hiring
 - Country, State, Time Zone, etc.
- More Cost Efficient to Follow-the-Sun
- Not impacted by weather or disasters
- Better work/life balance for SOC
- Better analyst to client relations
- Lower turnover rates



Find a Fishing Buddy

Anti-burnout SOC Staff Structure

- **Optimal**
 - **12 Analysts, 3 Leads**
- Adequate
 - 9 Analysts, 3 Leads
- Minimum
 - 6 Analysts, 1 Lead
- Subadequate - **Burnout Expected**
 - > 6 Analysts, 0 Leads

The Gipson Hiring Process

1. Gather Reasonable Requirements
2. Post Job Description
3. Process Resumes - **Look for Passion!**
4. Identify Top 25
5. Interview Candidates
6. Onboard New Hires
7. Offboard Departing Employees
8. **Schedule SOC Shifts**
9. **Retain Top Security Talent**

Find a Fishing Buddy - SOC Shift Schedule

Schedule No-Go's

- 12 hour shifts
- Overnight shifts (in TZ)
- Working 7 days in a row

Analyst 1	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Week 1	9 hours	9 hours	9 hours	off	off	9 hours	9 hours
Week 2	off	10 hours	10 hours	10 hours	10 hours	off	off
Week 3	9 hours	9 hours	9 hours	off	off	9 hours	9 hours
Week 4	off	10 hours	10 hours	10 hours	10 hours	off	off

GOOD - 2x2 Schedule

- Rotation for **2 Analysts** per shift, over **3 shifts**
 - **6 Analyst** total
- Analysts get **10 days** off per month

Find a Fishing Buddy - SOC Shift Schedule (Cont.)

Analyst 1	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Week 1	9 hours	9 hours	9 hours	off	off	9 hours	9 hours
Week 2	off	10 hours	10 hours	10 hours	10 hours	off	off
Week 3	off	10 hours	10 hours	10 hours	10 hours	off	off
Week 4	off	10 hours	10 hours	10 hours	10 hours	off	off

BEST - 1x3 Schedule

- Rotation for **4 Analysts** per shift, over **3 shifts**
 - **12 analyst total**
- Analysts get **11 days off** per month

Find a Fishing Buddy - Retain Top Security Talent

1. Salary plus benefits package

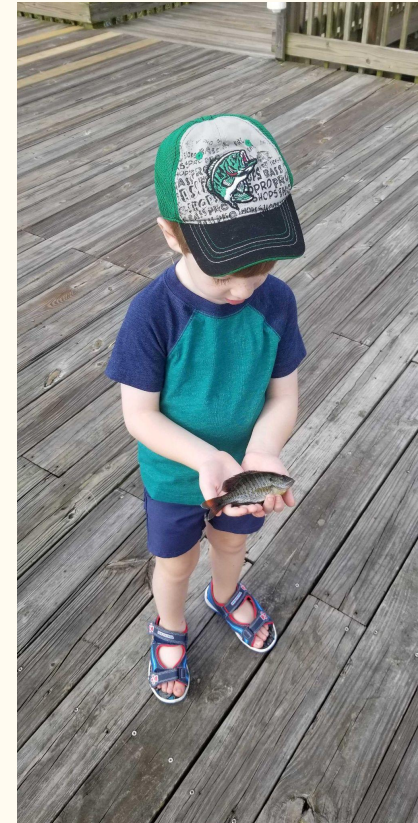
- a. Comparable to or higher than market equivalents

2. Good work-life balance

- a. Flexible work schedules
- b. Remote work options
- c. Paid time off

3. Opportunities for career growth and advancement

- a. Training programs
- b. Mentoring
- c. Transparent career development paths





Operation

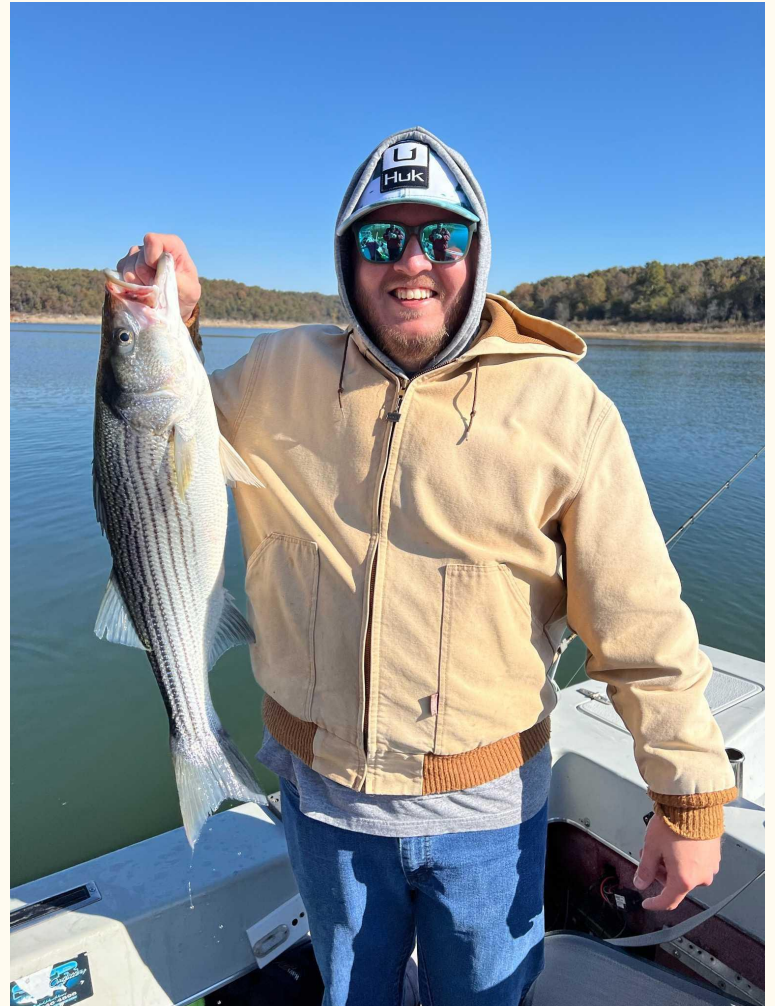


Clean the Catch

The Incident Response Process

Based off the Incident Response Plan

1. Detection of events
2. Preliminary response actions
3. Incident analysis
4. Response and recovery
5. Post-incident analysis



Fish Finders

Automation Centralization Using Security Orchestration and Response (SOAR)

Basic SOC Automation Use Cases

1. Rule Tuning
2. Data Enrichment
3. Report Writing
4. Event Correlation





Improvement



Location, Lure, Luck

Internal Process Testing

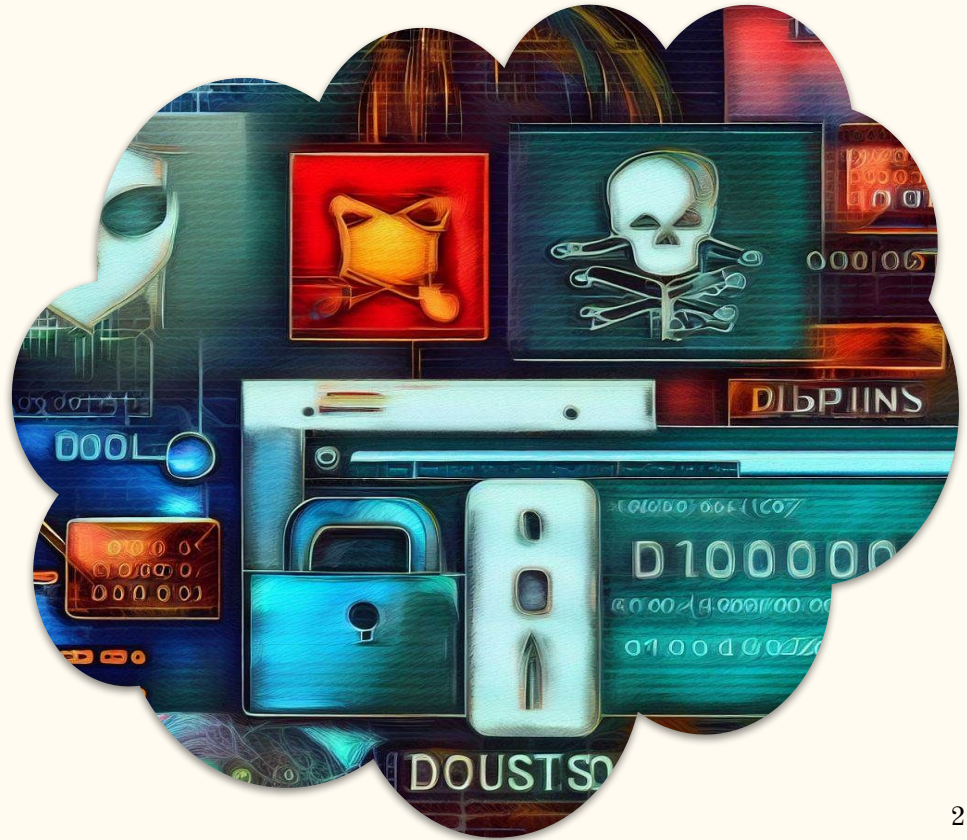
- **Location** - The Most Likely Attack Vectors
- **Lure** - The Method Used to Catch Cyber Threats (Incident Response Process)
- **Luck** - The Unpredictable Nature of Security Operations



Try Different Lures at Different Times of Day

Testing Abnormal Attack Vectors

- Example Tabletop Exercises
 - Exposed Admin Creds on GitHub
 - Impersonating Domain
 - Non-compliant User
 - Etc.



Practice Casting

Analyst Training Matrix

An effective way to aid in retaining top talent; no more “18 months-and-out.”

Level	Mandatory Analyst Retention Period	Pay Rate Increase	Automation	DFIR	Threat Intelligence	Penetration Testing
Master	4+ Years	20%	<i>Lvl-4 Training</i>	<i>Lvl-4 Training</i>	<i>Lvl-4 Training</i>	<i>Lvl-4 Training</i>
Guide	3+ Years	15%	<i>Lvl-3 Training</i>	<i>Lvl-3 Training</i>	<i>Lvl-3 Training</i>	<i>Lvl-3 Training</i>
Specialist	2+ Years	15%	<i>Lvl-2 Training</i>	<i>Lvl-2 Training</i>	<i>Lvl-2 Training</i>	<i>Lvl-2 Training</i>
Apprentice	1+ Years	10%	<i>Lvl-1 Training</i>	<i>Lvl-1 Training</i>	<i>Lvl-1 Training</i>	<i>Lvl-1 Training</i>

Attend a Casting Clinic

System and Organization Controls Type 2 (SOC2) Audit

- Assess a SOC team's controls and mitigations
- Educates SOC teams on the necessary controls and procedures
- Improves the SOC's detection capabilities and response time



Observe Nature to Catch More Fish

The Open-source Community

- Free for Commercial Use
- Data evaluated by many
- Can be considered more secure





Expected Results of a Successful SOC

Good Fishing Tips

Actionable Metrics

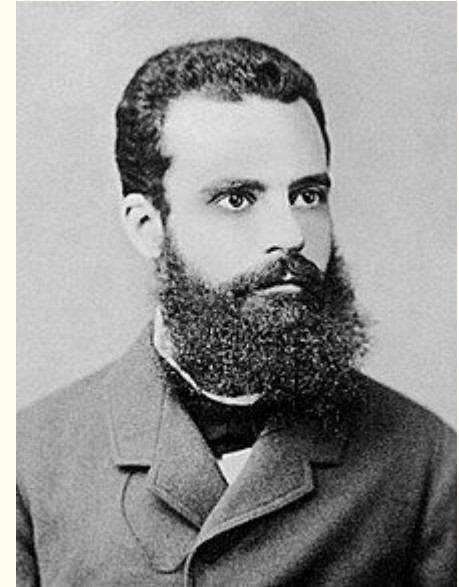
- The Honey Hole of Cyber
- Leads to identifying and mitigating security threats
- Captures key data points
 - SLA time metrics
 - Number of investigations worked, and their outcomes
 - Frequently detected users
 - Tunable alert rules (false positives)
 - Etc.



Catch 80% of Your Fish with 20% of Your Casts

The Pareto Principle in the SOC

- AKA the 80/20 rule
- 80% of the effects come from 20% of the causes
- The Golden Metric:
 - 80% True Positive, 20% False Positive/Benign
- SOC Automation:
 - 80% Automated Response, 20% Analyst Decision



Wilfried Fritz Pareto
1848 - 1923



Conclusion



Big Fish Stories

Top 7 Takeaways

1. Security documentation is the foundation of the SOC
2. Focus security tools around endpoint & business ops
3. Apply the Zero-Trust Method
4. Automate repetitive SOC tasks
5. Test the SOC against abnormal situations
6. Hire based on passion not education
7. Retain SOC analysts with:
 - Competitive Compensation and Benefits
 - Suitable Work/Life Balance
 - Relevant Training
 - Career growth

Questions?



Follow Me On    