Coach’s Corner
A Belichickian Approach to Security Operations
$DayJobs

Security Practitioners, SOC Managers, and Consultants
- SecOps Management
- Incident Handlers
- Malware and Forensic Analysts

Present & Past RSA Advanced Cyber Defense Consulting
- Security Operations Center Design
- Incident Response Program Development
- Threat Intelligence Program Development
Objective

If you take away one thing from this presentation it is that you must have a systematic approach to security operations.

A successful SOC is one that is built on fundamentals and strategic innovation.
Why Football Coach Bill Belichick?

Good Players + Execution = Success
  • 4X Super Bowl & 6X AFC Champ
  • Focuses on fundamentals with a blue collar effort = “Patriot Way”

• Football Ops vs SecOps

Hoodie Powahh!
Do Your Job!

Do your job = Be prepared, pay attention to the details, know your role, put the team first and execute your tasks.

- Third & Fourth string players must be ready to go. Next Man Up!
- Senior SOC Analysts must mentor juniors analysts.
- Play all 60 minutes = Executing all phases of Incident Response
- Don’t Skimp on Eradication or Lessons Learned
What Is My Job?

- What are your objectives?
- Define the “Right” Roles and Responsibilities
- Subbing for the “Security QB”
- Demonstrate how all the pieces work together

Leadership

Middle seat in coach class
Nobody Expects an Outlier

- Using the 3-4 when every one else was a 4-3
- Identifying different skills and schemes
  - Two Tight End Set Offense
  - Deceptive Formations

Goal:
Capitalize on talent /skillset that are available to you
Un-conventional Security

Take a less conventional approach to Incident Response

System of Records – Is it True?

Honey Tokens & Canary Folders

Threat hunting instead of L1 Response

Content Intelligence

Targeted Forensics & Malware Analysis
Finding Talent

• Stephen Neal former NCAA D1 Wrestling Champ, Freestyle World Champ

Find Talent Elsewhere

• In other Departments and Industries
• Many SOC Ninjas came from non-traditional backgrounds – LEO, Auto Mechanic, Chef, Archaeology
Building Your Team

• It’s the People who build your Process & implement and enrich your Technologies

• Got a rockstar? Challenge Them!

• ROI on People
  • Documentation, Knowledge Transfer, Mentoring
Building Your Team

Developing Talent
Next man up Strategy
• Contractors to FTE
• Interns (Value)
• Job Rotation
  • Did they pass the test?
  • Easier to get approved

Signing Talent
Fill specific holes
• Data Scientist
• Automation Guru
• Skilled Engineer who prefers working remote and at odd hours
Building Your Team

Spend the money for a specific capability
Sometimes you’ve got to let them walk when the price gets too high
• Vinatieri (2x SB game winning kicks)
• CJones (sack leader)

Salary matching a 25% increase?
No go, next man up! > Trust in your System

Move on from that MSSP and build in-house!
This is where your talent will come from
Situational Football – The Playbook

• Practice is more than running routes & blocking

• Different situations warrant different types of reactions
  • Know the rules
  • Know the formations
  • Simulate the environment

Malcolm Butler’s Game Winning Interception Super Bowl 49
Situational Security

- Response Procedures are our Playbooks
- Build Use Cases with Specific Courses of Action
  - Must be specific in order to get more from your juniors
  - You make the rules, use to your advantage
  - Most orgs will have a Malware Removal Procedure - How about a “Exploit Kit on High-Value Asset”?
- Tie Threat, Asset and Environment Together
- Incidents on Friday afternoon?
  - Contingencies, Call Trees & Out of Band Comms
Bend Don’t Break Defense

• If you hold a team to ONLY 197 total yards but they score more points, then you lose

- Capitalizing in the red zone and turnover ratios are what decide most game outcomes

- Tighten it up inside the 20, force the opponents to kick long field goals.
“Determined adversaries will find a way in no matter how strong your perimeter”

- **Goal:** Detect earlier on in the Kill Chain (Exploitation/Install)
  - Vulnerability Management is key
  - More focus on Endpoint Response
  - Resiliency – backups and business processes
On to Cincinnati......

• Pats routed by the Chiefs 41-14 on MNF

• Comments on Tom Brady.....

“He is just not that good anymore.” (Trent Dilfer)

The message here is, lets not get caught up in things that have no effect on the current situation, learn from it and move on to the next one.
On to the Next Incident

Stuck down the incident rabbit hole?

• When is enough, enough?
• It's ok to move on. Consider:
  • What is the priority?
  • Do you have the visibility you need?
  • Will you have to write or learn a new tool or skill?
  • What will be the benefit of complete analysis?
A Win is a Win

The Patriots play close games usually. Get the Win! No style points.

• Prevent defense to run out the clock

Containment vs. Attribution

• Is Containment good enough?
• Do We need to have attribution?
  • Of what? Malware, Threat Actor, etc.?
• Depends on mission and what you can do with that knowledge.
Losing & Getting Better

Belichick & Pats have lost some hard ones
- Super Bowls and AFC Championship
- Reviewing Game Film == Lessons Learned in IR
- “Never let a breach go to waste” – CISO Folklore
- What went wrong? How could we be better?

……..Show your leadership the #GAINZ you’ve made as a result of a painful incident…..

“We now have 3 new use cases for earlier detection on the kill chain and an updated response procedure”
Losing & Getting Better

- Practice makes perfect
  - Perfect practice makes perfect!

Challenge your SOC!
- Be realistic – SIEM should fire an alert in the first iteration of the exercise
- Test the response, comms, in particular with other BU’s
- Table Top Exercises & DFIR Net Wars, Capture the Flag (CTF)
- Reward with Challenge Coins and more training
Belichick vs Ransomware - Game Plan

Take away Opponent’s top players
- Attack Vector = Email > Coverage there?
- Resiliency > Backup & Restore - VSSAdmin
- Attack Surface Reduction > Network Drives

Game 2: Adjust tactics / add a new wrinkle
- Study Opponent, Game film = TTPs, IOCs, ISACs
- Use Honey token/persona for earlier detection
- Worst Case Scenario > Bulk Bitcoins available?
What about SpyGate & DeflateGate?

If you ain’t cheatin’, you’re not trying hard enough

• Pats focus on winning…
  Sometimes they push the boundaries of what is legal #Gate

Use same Principle to WIN support for your Mission
Mold Key Performance Indicators to your advantage
  • Dwell, Triage, Containment and Recovery Time
  • VERIS is VERY good
  • Kill Chain Detection & Containment Phases
Thank You

Contact: @ThomasJNeedham & @JGrosfelt