NEW SHERIFF IN TOWN

Creating and Supporting a New Pen Testing Program
### What this talk isn’t:
- A technical deep dive on our pen testing activities
- A copy/paste step-by-step guide
- Gospel

### What this talk is:
- An honest sharing of our experience
- Areas of focus to help in establishing this new capability in your org
- Pitfalls and stumbling blocks

---

**WANTED**

**DEAD** or **ALIVE**
SolarWinds Orion Vulnerability

- CVE-2020-10148
- Supply chain attack that resulted in massive disruption

1. Caught by IS prior to hitting the news cycle, but only by happenstance (well-informed engineer, weekend reading)
2. Leadership informed on subjective basis
3. No usable logs via SIEM, CrowdStrike only usable to check IOCs after the fact
4. Little to no continuous communicating with IT, so new IOCs were not effectively checked as they were released
No consistent threat intel

Informal IT/IS communication

No access to usable logs

Trust but no verify
Apache Log4Shell Vulnerability

- CVE-2021-44228
- Logging platform threat that resulted in massive disruption

1. IS became aware due to established Threat Intel process
2. Leadership immediately informed via process chain
3. Defense-In-Depth status verifiable via correlation between Crowdstrike logs and firewall logs in Splunk
4. Coordination with IT partners throughout all testing and remediation actions
DEC 2020

- No consistent threat intel
- Informal IT/IS communication
- No access to usable logs
- Trust but no verify

DEC 2021

- Threat Intel process established
- Firewall log ingestion in Splunk
- Continuous collaboration with IT
“Charged with the mission of operating beyond the boundaries of civilization … they lived and often died by the motto, 'Order first, then law will follow.”

- Thomas W. Knowles, They Rode for the Lone Star, Volume 1
1. PLAN
2. ENUMERATE
3. SCAN
4. EXPLOIT
5. REPORT
6. REMEDIATE
**BUILD CAPABILITY**

Validate the results of 3rd party pen test engagements
- Tools will need to be established
- Processes will need to be created, adjusted, and documented

**BUILD TRUST**

Gain the cooperation and support of the people you’re pen testing
- Cross-leadership conversations need to happen
- Document your partners’ pre-agreed scope for testing and exploitation

**BUILD PROOF**

Take a noteworthy issue to prove that your capability is self-sufficient
- A full penetration testing cycle needs to be accomplished
- That means fully self-driven action, end-to-end
Self-Driven Penetration Testing

- Pre-engagement and scopes written in-house
- Conducted and executed without 3rd party engagement
- Tabletop and report delivery generated in-house
- Remediation efforts continuously assisted by InfoSec

WANTED

- Agile Threat modeling
- Vendor confidence
- Acquisitions testing
THANK YOU