SANS SOC Summit 2015
After the Breach: 4 Years of Lessons Learned

Garrett Schubert – CIRC Manager
EMC Corporation
May 1st, 2015
Not a RSA breach discussion!
It’s a Journey

Ad Hoc
Technology Focused
Bystander
End User
Business Risk Focused
Cyber Prophet
Creator
Improved Collaboration

1. I get Dark Reading RSS feeds...
2. I am an ISAC member
3. I apply threat data to my SIEM data
4. I write rules and synthesize data
5. The AV companies rely on me for data
An Evolution

CIRC 2009
- Eyes on Glass
- Analysis
- Forensic
- Coordination
- Remediation
- Rule/Report Creation
- Workflow Development

Today
- Cyber Threat Intelligence
- Advanced Tool & Tactics
- Content Analytics
  - Specific functions
  - Reduces “Scope Creep”
  - Focused workflow
What we grew into

Cyber Threat Intelligence

- Reverse Malware Engineering
- Host & Network Forensic
- Root Cause Analysis
- Hunters

Advanced Tools & Tactics

- Eyes-On-Glass
- Event Triage
- Incident Containment
- Incident Command
- End User Intake
- 24x7 Coverage

Content Analytics

- Threat Indicators (IOC's)
- Actor Attribution
- Attack Sensing & Warning
- Social Media
- High Value Target (HVT)

Incident Response

- Content Development
- Integration
- Scripting
- Workflow
- Rules/Reports

24x7 Coverage

Eyes-On-Glass - On Glass

Event Triage

Incident Containment

Incident Command

End User Intake

24x7 Coverage
The People
The Process

Log and Packet data

- IPS
- AV
- Auth
- WAF
- EP
- DLP
- FW
- WLAN
- AD

Identity
- Division
- Geo Info
- Data
- Asset Value

Data Enhancement

Incident Workflow
- Incidents
- Threats
- GRC

Eng.
HR
Legal

CIRC
IT
1. Single views of SOC\CIRC activities

- Single pane of glass – reduced pains
- Report metrics
- And shift lead reporting – Incident coordination

http://map.ipviking.com/
2. Context - Give analysts more data up front

• “Business Context”
  • What does the asset do, what else does it interact with?
• Automated data pulls
  • Why make an analyst run a query you know they want?
  • Aggregation – many events to one incident
• Kill Chain stage
• Force multipliers!
3. Prioritize Intel

- T1-T4 – discuss how it helps the Frontline
  - Not all intel is created equal
  - Should you respond to Zeus before GhostRAT

- Is your industry vertical the same as party sharing the data?
The Technology

- Memory analysis linking suspicious network connections to file\process

- Limiting exposure time – discovery to containment

- VISIBILITY, VISIBILITY, VISIBILITY!
Managing the BIG Ones

• Single incidents verses “Declared” incidents
• Files\evidence naming conventions
• Tracking tasks
• Communicating to senior leadership – Initial\periodic communications
  • Weekly communications – 4 hour verse daily
• Resources not utilized if roles not identified
• SLA’s for external teams
Game Changers

• **Cyber Threat Intelligence**
  • Prioritize your intel!
    • Not all IoCs have the same impact to your org

• **Content Analytics**
  • Get business\organizational context at alert
  • Don’t make the analyst query for data you know they need, do it for them. Automate!

• **“Frontline” IR Analysts - CIRT**
  • Level 1 analysts need the right tools
  • Stop training run books – THINK out of the box

• **Malware Team - ATTA**
  • Share\document TTP and pivot points of specific campaigns
Thank you

Questions?