React Faster:

How to Leverage Monitoring to Keep Attacks From Becoming Catastrophes

Mike Rothman

Chief Blogger

mrothman@securityincite.com

SECURITY INCITE
SECURITYINCITE.COM

A Day in the Life of CSO

1. Fight fires
2. Get reamed for last audit
3. Fight more fires
4. Grovel to CIO and CFO for budget and resources
5. Clean up after stupid user
6. Fill out a silly report
7. Fight yet another fire
8. Learn about new application that is going live tomorrow
9. Go home. Have stiff drink
10. Pray beeper doesn't go off at 3 AM

The Typical CSO

The Patient is Sick

- **Storm worm.**
- **Bot armies.**
- **Data breaches.**
- **Client-side attacks.**
- **XSS and CSRF.**
- **Vista and Mac exploits.**
- **What's next?**
  - Your guess is as good as mine…

Predicting the Future – Not so much!

- **Check your track record:**
  - Morris worm?
  - Melissa?
  - SQL*Slammer?
  - SAMY?
- **What about real "risk" managers?**
  - Internet bubble
  - Sub-prime mortgages
- **Predict the future at your own risk…**
  - Don't believe me? Read the Taleb's *Black Swan*

Level-set: The Reasons to Secure

- **Your job is to protect the assets of the organization and ensure business can operate**
  - Maintain business system availability
  - Protect intellectual property
  - Limit corporate liability
  - Safeguard the corporate brand
  - Ensure compliance

Ahead of the Threat? HA!

- The attack has started or has it? How do you know?
- Do you have your crystal ball handy?
- Can you risk a false positive?

React FASTER

- **The reality.**
  - You will get hit, be ready
  - You need to narrow down areas to investigate
- **Near real-time analysis.**
  - Contain the damage
- **Analyzing and thresholding.**
  - Knowing when you have a problem (and when you don't)
- **The answer is?**
  - MONITORING

Monitor What?

- **Yes, it's about detecting anomalies**
  - Get baseline
  - Look for strange results
- **Monitor across your infrastructure**
  - Networks
  - Servers
  - Databases
  - Applications
  - Endpoints (where possible)

Network Monitoring

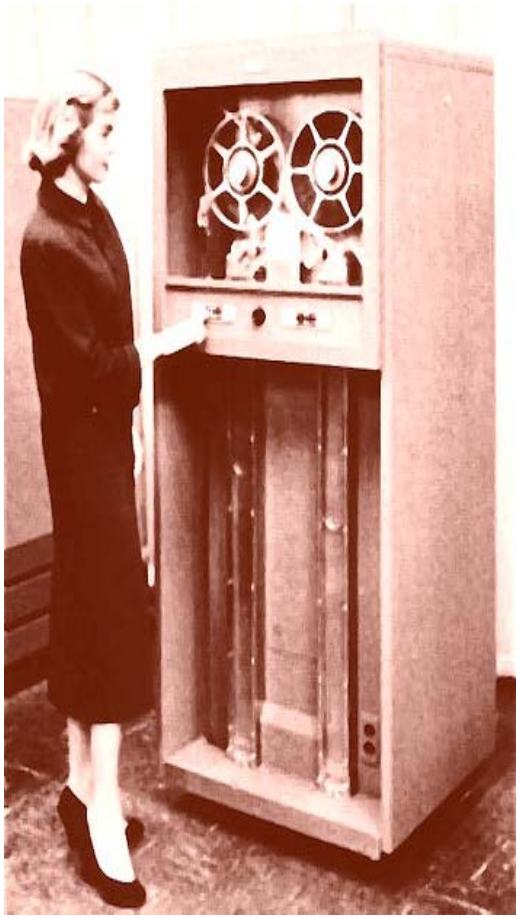
- **The network never lies**
- **Bejtlich's Network Security Monitoring.**
  - Read it, Live it, Love it.
- **Network behavioral analysis.**
  - Stand-alone or integrated.
  - Who controls the data?
- **Sensors.**
  - How many? Where?
  - Is IDS dead?
  - Monitoring vs. blocking.
- **How much data to capture?**

Server Monitoring

- **Configuration changes**
  - Unexpected updates are an indication that something is amiss
  - Enforcing change control process
- **Performance characteristics**
  - Race conditions
  - Unknown processes/executables
  - Anomalies
- **HIDS vs. HIPS**
  - Monitoring vs. blocking (again)
- **Multi-platform reality**

Database Monitoring

- **Looking for:**
  - Strange transactions
  - Fraud patterns
  - Unknown users
- **Network or server-based**
  - C: All of the above
- **Performance impact?**
- **How much data to capture?**



Application Monitoring

- **Nascent function from a security context**
  - Application performance monitors can help.
- **Build it yourself**
  - Profile application traffic, transaction rates, database requests.
- **Monitor app server logs and check for anomalies**
  - How good are you with scripts?

Security Management Integration

- **Lots of different ways to do the same thing (sort of)**
  - SIEM
  - Log Management
  - Network behavior analysis
  - Configuration Management
- **Pendulum swinging back towards integrated, multi-function security management platforms**
  - Your ops group must be able to evolve

Attackers Leave a Trail

- **It's very very hard to totally eliminate attack artifacts**
- **Logs are your best bet to piecing things back together**
  - Move the logs off the device
  - Sign and sequence
  - Watch the watchers

Documenting the Controls for Audit

- **A big part of compliance is documentation.**
- **Can reporting by automated?**
- **Can devices and monitors solutions pump data into a reporting package?**
- **Consistency is critical**
- **Must be able to substantiate the data.**
  - Data normalization is bad

Faking it #1: Leveraging Reputation

- **You can't get ahead of it, but you can infer intent**
- **The role of reputation moving forward**
  - Email
  - Web
  - Applications
  - Insiders vs. outsiders

Faking It #2: Hack Thyself

- **"Security Assurance" is a discipline and legitimate security role**
  - The world is dynamic, audits are a point in time
  - Pinpoint potential issues
- **Moving up the stack to applications**
- **The power of automation**

The Ethics of "Exploits"

- **Penetration testing requires the use of real exploits**
- **Some parties think exploits are bad**
  - They are wrong.
  - The bad guys use exploits and social engineering.
- **Understanding the risk of using exploit code**
  - Will hackers use this code against you?
  - Will you bring down your network?
  - How do you do it safely?

Summary

- **We suck at predicting things**
  - So you better be able to REACT FASTER
- **Monitoring at all levels of the stack is imperative**
  - Look for anomalies
- **You can fake it (sort of) with reputation and testing**
- **Make sure you have a containment plan**