Security Through Data Analysis : Harnessing The Power Of Feedback

Introduction

Chapter 1: Unleashing The Securing Power Of Data

Standing on the shoulders of giants

Looking at other industries that have made a conversion from little-to-no data to being data-driven.

**Use Case**: Agriculture -> Agri-infomatics

**Use Case:** Biology -> Bioinformatics/Epidemiology

Shifting from security Shaman to data Sherpa

Linking information security with other pre-data-driven industries

Data analysis assists our thinking, it does not replace it

Chapter 2: Finding Your Inner Security Data Scientist

No shirt, no shoes, no degree? No problem!

Performing basic analysis without advanced statistics using the “ABC” (Arithmetic, Bucketing & Comparing) simplification method

**Use Case:** Discovering anomalous firewall traffic

**Use Case:** Identifying the cost of two-factor authentication

Obtaining the essential skills & ingredients

Discussion of skills: curiosity, statistics, programming, scripting, database management and visualization techniques

Getting real benefit from combining with domain knowledge in information security

Chapter 3: Learning The “Hello World” Of Security Data Analysis

Deciphering the not-so-secret secret of data analysis: Data munging

How to acquire and prepare security data

Creating a repeatable data analysis toolkit and workflow

**Use Case:** Swimming the river of log data (CLF)

Exploring the dark art of data munging

The importance of timestamps and handling time series data

Combining multiple data sources

Using more than just “security data” to solve security problems

**Use Case**: Normalizing NetFlow Data

**Use Case**: Analyzing Windows Event Logs

**Use Case**: Helping The Help Desk

Chapter 4: Tuning The Right Frequency: Security Analysis By The Numbers

Learning from our frequentist forefathers

Shifting from descriptive to inferential statistics and outgrowing the ABC method (ch. 2)

Separating correlation from causation

Seeing attack patterns that do not exist

**Use Case**: Productivity in proxy logs

**Use Case**: Whitehat statistics report

**Use Case**: Security event correlation

Chapter 5: Knowing When 35 == 37: Finding The True Messages In Security Data

Measuring the “power” of sample size

Strong versus weak messages in the data

**Use Case**: Vulnerability counts

**Use Case**: Security patch coverage

Being secure in your uncertainty

Embracing hypothesis testing and confidence intervals with open eyes

**Use Case**: Trustwave’s industry report: trending year-over-year

**Use Case**: Malware gone wild (using inferential statistics to detect a malware outbreak *before* it gets crazy)

Chapter 6: Breaking Up With Your Relational Database

Realizing the container has constraints

**Use Case**: MySQL memory (and other) tables

Managing non-relational data (saying “Yes” to NoSQL)

Explaining alternative data stores and their strengths:

Hadoop/PacketPig, MongoDB, Couch, Redis, etc

**Use Case**: Storing and accessing netflow data (continuing ch.3 data)

Chapter 7: Visualizing Your Security Data

Building the foundation of security data visual analysis and communication

How-to examples each in in Excel, Python and R

**Use Case**: Graphing trends in netflow data (expansion of ch 3 & 6 analysis)

**Use Case**: Improving visual defaults

**Use Case**: Visualizing system logs (expansion from ch 3)

Chapter 8: Mapping Security Data

Realizing that spatial data may not be special data

Performing Geo-IP mapping (and the gotchas in doing so)

**Use Case**: Generic geo-location of IP addresses

**Use Case**: Mapping Botnets

Mapping outside the continents

Discovering patterns and clusters with mapping tools

**Use Case**: Mapping malicious ASN.1 data

Chapter 9: Making The Machine Learn For You

De-mystifying machine learning

Basics of ML with the necessary background for the next section

Understanding the (security) potential of machine learning

**Use Case**: Discovering account takeovers (with “supervised learning”)

**Use Case**: Detecting and classifying malware with Naïeve Bayes networks

Chapter 10: Making The Machine Read For You

Introduction to textual analysis (NLP)

Using NLP in security

**Use Case**: Using NLP in DLP (Data Loss Prevention)

**Use Case**: Who Wrote That? (Attribution of anonymous blog/forum posts)

Chapter 11: Predicting The Future With Security Data

Can you do better than a groundhog?

The hype and hopes of predictive analytics

How to perform basic predictive analysis

**Use Case**: Modeling growth in centralized security logging systems

**Use Case**: Predicting rogue behavior (insider misuse)

Chapter 12: Keeping It Simple

Putting security data analysis into perspective

Comparing a “drilling for oil” approach to a “pan for gold” approach

Understanding the reality of our environments

Reiterating that data analysis assists our thinking, it does not replace it