Netsecuris
Who's watching your network?

Data Driven Security – Framework to Success

Presented by Leonard Jacobs, MBA, CISSP, CSSA
Founder, President and CEO of Netsecuris Inc.

Netsecuris
Who's watching your network?

Topics

- The Explosion of Security Data
- Threat-centric Security vs. Vulnerability-centric Security
- Network Security Monitoring (NSM) Cycle
- Security Data Processing Concepts
- Security Data Visualization
- Threat-centric Security Data Framework

Netsecuris
Who's watching your network?

Opening Riddle

Win a Tee Shirt

- What goes fast?
- What is spelled the same in both directions?

Netsecuris
Who's watching your network?

The Explosion of Security Data

- How many of you can name all the sources of security data you have in your company?
- Can you name at least some sources?

Netsecuris
Who's watching your network?

The Explosion of Security Data

- Does your organization use any of the following cyber security measures?
  - Firewall
  - IDS/IPS
  - Security Incident and Event Management
  - Anti-malware/Anti-Bot
  - Internet Content Filtering

Netsecuris
Who's watching your network?

The Explosion of Security Data

- Do you know how many records of security data your organization collects every day?
- Every week?
- Every month?
- Every year?

Netsecuris
Who's watching your network?

The Explosion of Data

- Threat alerts grew 14 percent year over year; new alerts (not updated alerts) are on the rise.
- "Watering hole" attacks are targeting specific industry-related websites to deliver malware.

(Cisco 2014 Annual Security Report)

Netsecuris
Who's watching your network?

The Explosion of Data

- Kaspersky Lab products detected and neutralized a total of 6,167,233,068 threats during 2014
- A total of 1,910,520 attempts to launch banking malware on user computers were neutralized in 2014.

(Kaspersky Security Bulletin 2014 Overall Statistics for 2014)

Netsecuris
Who's watching your network?

The Explosion of Security Data

- Is your organization reviewing security data 24x7x365?
- Does your organization have alarms set for security events?
- Does your organization believe what the "machine" is telling it?

Netsecuris
Who's watching your network?

Threat-centric Security vs. Vulnerability-centric Security

- Vulnerability-centric security focuses on the "how".
- Threat-centric security focuses on the "who" and "why".

Netsecuris
Who's watching your network?

Threat-centric Security vs. Vulnerability-centric Security

Vulnerability Centric	**Threat Centric**
• Relies on prevention	• Prevention eventually fails
• Focus on detection	• Focus on collection
• Assumes universal view of all threats	• Knows that threats use different tools, tactics, and procedures
• Analyzes every attack in a vacuum	• Combines intelligence from every attack

Netsecuris
Who's watching your network?

Threat-centric Security vs. Vulnerability-centric Security

Vulnerability Centric	Threat Centric
• Heavy reliance on signature-based detection	• Utilizes all-source data
• Minimal ability to detect unknown threats	• Stronger ability to detect adversarial activities beyond known signatures
• Linear process	• Cyclical process

Netsecuris
Who's watching your network?

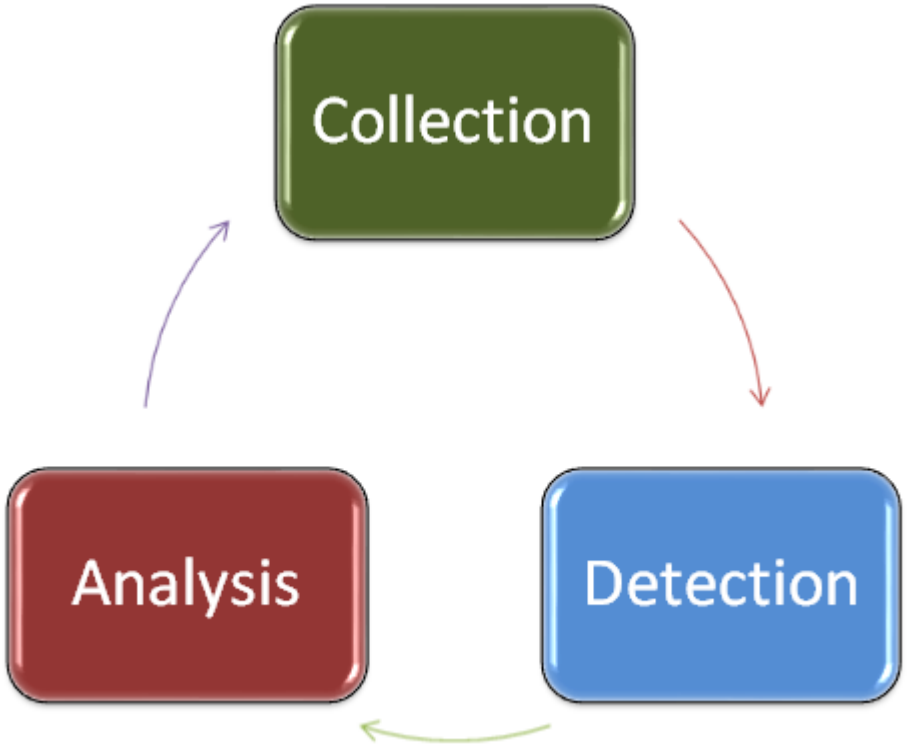
Network Security Monitoring Cycle

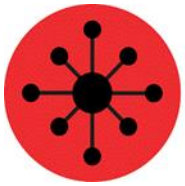
- NSM is based on the collection, detection, and analysis of network security data.

Netsecuris
Who's watching your network?

Network Security Monitoring Cycle

NSM is a cyclical process.





Network Security Monitoring Cycle

- Collection
  - Focuses on:
    - Generation of security data.
    - Organization of the security data.
    - Storage of the security data.

Netsecuris
Who's watching your network?

Network Security Monitoring Cycle

- Collection
  - Tasks:
    - Defining where the largest amount of risk exists in the organization.
    - Identifying threats to organizational goals.
    - Identifying relevant data sources.
    - Refining collection portions of data sources
    - Configuring data collection mechanisms
    - Building storage for security data retention

Network Security Monitoring Cycle

- Detection
  - Based upon:
    - Observed events.
    - Data that is not expected.
  - Focuses on:
    - Examination of collected data.
    - Generation of alerts.

Netsecuris
Who's watching your network?

Network Security Monitoring Cycle

- Analysis
  - Focuses on:
    - Human investigation of alerts.
    - Human interpretation of alerts.

Network Security Monitoring Cycle

- Analysis
  - Tasks can include:
    - Packet Analysis
    - Network Forensics
    - Host Forensics
    - Malware Analysis
    - Open Source Intelligence

Security Data Processing Concepts

- "Good" Data vs. "Bad" Data
  - "Good" Data is data that can be organized in a meaningful way and can be efficiently analyzed.

Netsecuris
Who's watching your network?

Security Data Processing Concepts

- Examples of "Bad" Data

Emp ID	1	2	3	4	5
10240	P	P	H	P	P
10355	P	P	H	P	P
10371	P	P	H	P	P
10444	A	A	H	A	A

Month	Base	Actual	Total
Jan	1966	905	2871
Feb	1953	905	2858
Mar	1956	905	2861
Apr	1937	935	2872
May	1934	905	2839

Netsecuris
Who's watching your network?

Security Data Processing Concepts

- Example of "Good" Data

Customer Name	Due date	Amount
CXQ	Monday, August 01, 2005	140497
HEC	Tuesday, December 22, 2009	19421
QYD	Monday, June 08, 2009	22143
JVJ	Tuesday, December 08, 2009	13742
BMJ	Sunday, September 10, 2006	15563

Netsecuris
Who's watching your network?

Security Data Processing Concepts

- What does "Good" security messages look like?
  - Descriptive
  - Relatable
  - Complete

Netsecuris
Who's watching your network?

Security Data Processing Concepts

- Descriptive Messages
  - Not Descriptive

    Mar 29 11:22:45.221 myhost sshd[213]: Failed login attempt
  - More Descriptive

    Mar 29 11:22:45.221 myhost (192.168.2.2) sshd[213]: Failed login attempt from host 192.168.3.1 as 'admin' , incorrect password

Netsecuris
Who's watching your network?

Security Data Processing Concepts

- Relatable Messages
  - Not Relatable

    Mar 29 11:22:45.221 myhost (192.168.2.2) myspamapp[213]: Message <21394.283845@spam.com> title 'Herbal Remedies and Tiny Cars' from 'spammer@spam.com' rejected due to unsolicited commercial content
  - More Descriptive

    Mar 29 11:22:45.221 myhost (192.168.2.2) myspamapp[213]: Message <21394.283845@spam.com> title 'Herbal Remedies and Tiny Cars' from 'spammer@spam.com' at SMTP host 192.168.3.1:2034 rejected due to unsolicited commercial content

Netsecuris
Who's watching your network?

Security Data Processing Concepts

- Complete Messages
  - Incomplete

    Mar 29 11:22:45.221 myhost (192.168.2.2) myspamapp[213]:
    Received Message <21394.283845@spam.com> title
    'Herbal Remedies and Tiny Cars' from 'spammer@spam.com' at
    SMTP host 192.168.3.1:2034
    Mar 29 11:22:45.321 myhost (192.168.2.2) myspamapp[213]:
    Message <21394.283845@spam.com> passed reputation filter
    Mar 29 11:22:45.421 myhost (192.168.2.2) myspamapp[213]:
    Message <21394.283845@spam.com> FAILED Bayesian filter
    Mar 29 11:22:45.521 myhost (192.168.2.2) myspamapp[213]:
    Message <21394.283845@spam.com> Dropped
  - Complete

    Mar 29 11:22:45.521 myhost (192.168.2.2) myspamapp[213]:
    Received Message <21394.283845@spam.com> title
    'Herbal Remedies and Tiny Cars' from 'spammer@spam.com' at
    SMTP host 192.168.3.1:2034 reputation=pass Bayesian=FAIL decision=DROP

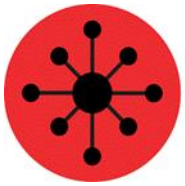
Netsecuris
Who's watching your network?

Security Data Visualization

- Advantages
  - Communicates complexity quickly.
  - Enables recognition of latent patterns.
  - Enables quality control on the data.
  - Can serve as a muse.

Security Data Visualization

- Exploratory Data Analysis (EDA)
  - The process of examining a dataset without pre-conceived assumptions about the data and its behavior.
  - EDA is a constant process.

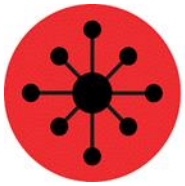


Security Data Visualization

- EDA Example
  - A simple, classic (Anscombe) example of the central role that graphics play in terms of providing insight into a data set starts with the following data set:

Data

X	Y
10.00	8.04
8.00	6.95
13.00	7.58
9.00	8.81
11.00	8.33
14.00	9.96
6.00	7.24
4.00	4.26
12.00	10.84
7.00	4.82
5.00	5.68



Security Data Visualization

- EDA Example
  - If the goal of the analysis is to compute summary statistics plus determine the best linear fit for Y as a function of X, the results might be given as:

N = 11

Mean of X = 9.0

Mean of Y = 7.5

Intercept = 3

Slope = 0.5

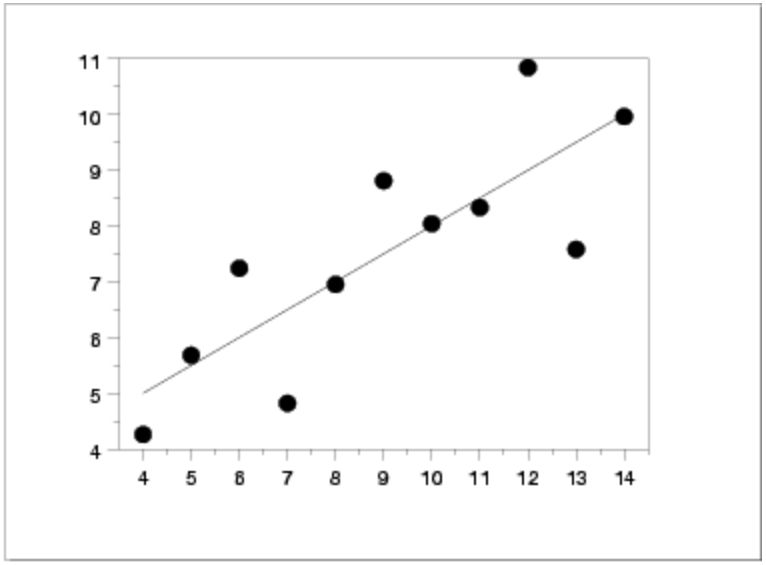
Residual standard deviation = 1.237

Correlation = 0.816

Netsecuris
Who's watching your network?

Security Data Visualization

- EDA Example
  - In contrast, the following simple scatter plot of the data



suggests the following:

Netsecuris
Who's watching your network?

Security Data Visualization

- EDA Example

- The data set "behaves like" a linear curve with some scatter;
- there is no justification for a more complicated model (e.g., quadratic);
- there are no outliers;
- the vertical spread of the data appears to be of equal height irrespective of the *X*-value; this indicates that the data are equally-precise throughout and so a "regular" (that is, equi-weighted) fit is appropriate.

Security Data Visualization

- The EDA approach of deliberately postponing the model selection until further along in the analysis has many rewards, not the least of which is the ultimate convergence to a much-improved model and the formulation of valid and supportable scientific and engineering conclusions.

Netsecuris
Who's watching your network?

Threat-centric Security Data Framework

- Applied Collection Framework (ACF)*
  1. Define and Identify Threats
  2. Quantify Risk
  3. Identify Data Feeds
  4. Narrow Focus

*Reference: Applied Network Security Monitoring, Chris Sanders and Jason Smith, 2014

Netsecuris
Who's watching your network?

Threat-centric Security Data Framework

1. Define and Identify Threats

   Always start with this question:

   What is the worst case scenario as it relates to the survivability of the organization?

   Gain buy-in from upper management in terms of the answer.

   Develop a set of questions that can be used to determine which assets within the network are most critical to protecting sensitive data.

Netsecuris
Who's watching your network?

Threat-centric Security Data Framework

2. Quantify Risk
   You could use:

   Risk (R) = Impact (I) x Probability (P)

   Impact is a scale of 1 to 5 with 1 meaning the threat has little impact and 5 meaning the threat has large impact.

   Probability is a scale of 1 to 5 with 1 meaning low probability and 5 meaning high probability of occurring.

   Risk is a scale of 1 to 25 with

   0-9: Low Risk

   10-16: Medium Risk

   17-25: High Risk

Netsecuris
Who's watching your network?

Threat-centric Security Data Framework

3. Identify Data Feeds that might provide NSM detection and analysis value.

   Start with the technical threat with the highest risk weight.

Netsecuris
Who's watching your network?

Threat-centric Security Data Framework

4. Narrow Focus
   - The most technically in-depth step.
   - Review every data source to gauge its value.

Netsecuris
Who's watching your network?

Threat-centric Security Data Framework

4. Narrow Focus

- You might want to answer the following example questions to help in narrowing focus:
  - What can you filter out of PCAP traffic from a specific network segment?
  - Which system event logs are the most important?
  - Do you need to retain both firewall permits and denies?
  - Which portions of the web application do you really need web logs for?
- Begin to define the amount and duration of each data type you would desire to retain.

Netsecuris
Who's watching your network?

Consider these tips

- Cyber security program balance is paramount.
- Accept the fact that, to some extent, your networks and computer systems will be breached repeatedly.
- Work hard to make breaches hard to do. Attack containment is the mantra.
- Ensure that your cyber security program provides sufficient detection and response capability for when the inevitable occurs.

Netsecuris
Who's watching your network?

Contact Information

Leonard Jacobs, MBA, CISSP, CSSA

Email: ljacobs@netsecuris.com

Office: (952)641-1421 ext. 20

Thank you