My Perspective

Information security metrics do not show us how we need to improve our defenses.
Tim Howard
US Goalie
World Cup 2014

Measure:
16 World Cup Saves

Metrics:
Avg .89 saves / goal
Avg .97 claim success
Avg 2 saves per game

Many believe:
The.Best.Goalie.Ever

What’s missing?

How was the other team able to get the ball into the back of our net?

Belgium  2
USA    1
You keep using that word...

- **Measure**: The size, amount, or degree of something
- **Metric**: Meta-data derived from analyzing measurements of a given variable over time, or against a specific baseline or target
- **Correlation**: The appearance of statistical dependence between measured events, without a causal relationship
- **Causation**: The direct effect of one measured event on another (cause and effect relationship)
- **Threat**: A malicious attempt to compromise the confidentiality, integrity, availability, authenticity, utility, or possession of a given information asset*
- **Risk**: The probability of loss due to a given threat

---

We’ve got to ask ourselves a question

1) CIS Security Benchmarks
   • Number of applications
   • Mean time to complete changes
   • IS Budget as % of IT Budget

2) GIAC / SANS
   • Unauthorized devices
   • Total count, avg hours online/device
   • Infrastructure configurations
   • # of insecure configs, mean time to repair
   • User admin accounts
   • Total, %, mean time to remediate
   • Incident Response
   • Mean time to detect, remediate

3) 5 Strategic Security Metrics
   • Comparative spend
   • Mean time to compliance
   • % of emergency changes

Are we measuring the right stuff?
Identify the threats

- Identify **causally significant** metrics
  - Marginal threat levels – immediate feedback
  - Threat volumes and types – long term
- Leverage immediate feedback to address current threat levels
- Use long term metrics to refine and improve security posture
- Select tools that can best help your team
One more generic note

What does Breach Detection address?

Residual Risk

It's time to start considering these sorts of technologies, and the intel they can provide as part of the whole equation.
Top Level Classifications

- **Recon:** find a vulnerability
- **Initial Exploit:** take advantage of recon
- **Compromise:** privilege escalation, spread, etc.
- **C&C:** check in with HQ
- **Actions:** steal, corrupt, interrupt, etc.
- **Compliance:** policy/procedure violations
- **Hygiene:** misconfigured apps, etc.

Advanced, targeted, it's all the same stuff. The difference comes in the type of recon – specific, or how to hit the most targets.
Threat Identification Tools
Network Behavior Analysis

- Volume, Direction, Frequency, and Scale
  + Ubiquitous, easy to scale
  + Encryption not an issue
  + Typically allows asset classification / valuation
  + Statistical analysis baselines and identifies “abnormal behavior” from various measures
  + Adds significant troubleshooting, performance analysis capabilities (budget / resource sharing)

- May miss smaller attacks or compromises
- No packet level analysis
- Requires some care and feeding
Network Behavior

Anomaly Identification - > Actions
• Scales well (netflow is everywhere)
• Built-in metrics with anomaly detections
• Build groups to prioritize assets
• Build alerts to monitor compliance
• Integrate with authentication, network gear to immediately identify affected users and devices

What Sorts of Metrics?
• Session count
• Volume by port, app, device
• Drill down by group, port, application, or device
• Malware propagation
• Typical connection peers
Behavior Clues

Netflow and Packet Analysis
• Add application specific data points
• Visually significant anomalies with drill down capabilities allow for quick investigation

Identify credible threats via Volumetric Analysis
• DNS
  • CnC traffic from malware outbreak?
  • External? -> Block outbound DNS
  • Internal? -> Check Server
• ICMP
  • DOS, DDOS ?Botnet?
  • External? -> Block ICMP
  • Internal? -> Investigate
• SMTP
  • Identify hosts & targets
  • External? -> Block SMTP
  • Internal? -> Check policies and reqs
• Data Breach
  • Should that critical asset be communicating with remote countries?
  • Why did Alice’s salesforce connection volume increase by 400%?
• HTTP Session Count
  • Increase by 200%? Adware, Click Fraud?
  • User Ed? Content filtering?
  • Bad headers? Stealth C&C?
Network Breach Detection

+ Typically combine IDS type functions with advanced malware id
  C&C / DGA analysis, obfuscated comm. channels, etc.
+ Able to correlate multiple attacks to a single host over time
+ Able to track small threats as well as more obvious ones
- Can combine with other tools for SSL analysis
- May require larger investments in architecture for full coverage
- Performance reqs. may limit deployment options
- Direct remediation available
Breach Analysis

Aggregate Measures

Risk Based Prioritization
Threat Categorization

Alerts by threat type leads to immediate possibilities for focusing remediation.
Suspicous Details

Packet captures that show the offending traffic for detailed human and forensic, as well as potentially for prosecution.

Details for advanced and/or proprietary alerts are a must to start.
Asset View

Alerts by Asset Category

Built In Metrics
Intelligent Alert Management

Filter and quickly address multiple alerts to minimize information overload.
Threat Analysis

Alert correlation and detailed threat assessment
Major Challenges

- Focus on the unknown
  - No CVE, focus is on behavior
  - Requires understanding of malware communications channels

- Scope and Breadth of analysis
  - Aggregation of metrics, reporting
  - 500 “breaches” are just as difficult to manage as 500 SIEM events

- Still immature market & too much FUD
Challenge Accepted

Breach Detection - Sans Top 20!

- Use behavioral analysis as top incident risk identification
  - As a front end tool, then leverage with SIEM, etc.
  - Or pipe detections into existing SIEMs

- Review data
  - Fine detail for individual, credible threats
  - 10km view for general insight into your network
  - Combine with other tools for more context
    - Threat feeds, reputations lists, etc.
    - Firewall / IDS / Sandbox / Server logs
"The ideal scenario is that everyone and every vendor uses the same format for indicators of compromise," he says. "You can use it to share threat data, so all of us can benefit."

Jaime Blasco
Director, AlienVault
Ways to help the transition

- Integrate Breach Detection
  - Apply new technologies to mitigate risks before it’s a tool for residual risk

- Reporting
  - 500 discrete “Credible Threats” can be much more painful to deal with than 10,000 identified CVEs

- Integration of external intel
  - The more the merrier

- Asset Valuation
  - Prioritize alerts based on value of involved assets

- Open Integration
  - IOCs, Observables, Veris, etc.
## Malware Types by Remediation

<table>
<thead>
<tr>
<th>Veris threat sources</th>
<th>Remediation Ideas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware, click fraud, browser attacks, etc.</td>
<td>Better user education, additional content controls</td>
</tr>
<tr>
<td>Recon, brute force, SQLi</td>
<td>Tighten admin controls</td>
</tr>
<tr>
<td>Command &amp; Control</td>
<td>Leverage threat intel</td>
</tr>
<tr>
<td>Spam, DGA, DOS</td>
<td>Tighten Outbound controls</td>
</tr>
<tr>
<td>Policy Violation</td>
<td>Address violation, training</td>
</tr>
</tbody>
</table>

http://veriscommunity.net
Asset Classification

- A realistic asset classification system is a must (at least 3 priorities)
  - Preferably custom groupings to allow Risk based prioritization as well as group based reporting for remediation focus

- Even better – ability to tie into existing asset value frameworks
Aggregate Metrics

How bad are things today?
Conclusion

- We’re losing everyday because we tend to focus on the attacks that we stop – looking at the known issues.

- We need to start learning from the new, existing, and evolving threats that are already in our networks and leverage that data to improve across the field of information security.

Thanks for your time!