Thank you for attending. Our webinar will begin shortly.
ResearchSOC

NSF-funded security operations center designed to make scientific cyberinfrastructure resilient to cyberattacks and capable of supporting trustworthy, productive research.

A suite of technologies, services, training, and a community of practice specifically designed for research and education projects.
Housekeeping

- All participants are on mute.
- Ask your questions via the Q&A feature.
- We will record this webinar and provide a link.
- Slides will also be made available.
- Tech troubles? Sign out and back in.
How to select and use cybersecurity metrics to make cybersecurity operations more effective

Susan Sons
Deputy Director, ResearchSOC
Center for Applied Cybersecurity Research
Indiana University
HERE WE GO...

YOU ARE HERE.

1. Metrics with Purpose
2. Selecting Metrics
3. Using Metrics
4. Keeping it Sane: The Evolution of Security Metrics Over Time
SECTION 1

METRICS WITH PURPOSE
WHAT IS A METRIC?

N., A SYSTEM OR STANDARD OF MEASUREMENT

--Oxford’s American Dictionary
THE PERILS OF BAD SECURITY METRICS

- PERVERSE INCENTIVES
- INTENSIFIES “MAGIC BOX” SYNDROME
- FALSE SENSE OF SECURITY
- SPEND RESOURCES IN THE WRONG PLACES

- CONFUSE METRICS WITH SUBJECTIVE OR QUALITATIVE MEASUREMENTS
- USE METRICS TO TALK ABOUT THE PAST, NOT THE FUTURE
- “UP AND TO THE RIGHT” SYNDROME
WHAT SOMEONE ASKED FOR

Jan  | Feb  | Mar  | Apr  | May  | Jun  | Jul  | Aug  

Line graph showing an increase from Jan to Aug.
HOW RESEARCHSOC GOT HERE:

HAVE YOU EVER TRIED TO FIGURE OUT WHETHER YOUR WORK WAS ACCOMPLISHING ANYTHING?

HAVE YOU EVER WONDERED WHETHER IT WAS YOU OR THE CLIENT?

WE DID.
GOOD SECURITY METRICS WORK FOR YOU

- Understand and communicate security risk
- Understand how well current processes and controls are working
- Discover weaknesses in infrastructure
- Spot emerging threats
- Direct security dollars and effort to get more “bang for the buck”
- Decide what to do next, and what to stop doing
THE PURPOSE OF RISK MANAGEMENT IS TO IMPROVE THE FUTURE, NOT TO EXPLAIN THE PAST.

-- Andrew Jaquith
My short list of (mildly belligerent) vendor questions, therefore, include these:

- WHICH WOULD BE CONSIDERED “KEY INDICATORS”?
- HOW DO YOU USE THESE INDICATORS TO DEMONSTRATE IMPROVEMENT TO CUSTOMERS AND TO EACH CUSTOMER’S INVESTORS, REGULATORS, AND EMPLOYEES?
- COULD YOU, OR A MANAGEMENT CONSULTANT, GO TO DIFFERENT COMPANIES AND GATHER COMPARABLE STATISTICS?
- DO YOU BENCHMARK YOUR CUSTOMER BASE USING THESE KEY INDICATORS?

I want to see somebody smack these out of the ballyard, but somehow I think I will be waiting a while.
1 METRICS WITH PURPOSE

YOU ARE HERE.

2 SELECTING METRICS

3 USING METRICS

4 KEEPING IT SANE: THE EVOLUTION OF SECURITY METRICS OVER TIME
SECTION 2

SELECTING METRICS
A GOOD METRIC SHOULD BE:

- CONSISTENTLY MEASURED
- CHEAP TO GATHER
- EXPRESSED AS A CARDINAL NUMBER OR PERCENTAGE
- EXPRESSED USING AT LEAST ONE UNIT OF MEASURE
- ACTIONABLE
TWO WAYS TO LOOK AT YOUR METRICS

WHAT ARE WE MEASURING?
- Process
- Outcome
- Impact

WHAT ARE WE DOING WITH THE MEASURE?
- Target
- Heartbeat
- Compliance
WE HAVE IT HARDER THAN THE PRIVATE SECTOR.

Creating numbers connected to mission is astronomically simpler when your mission can be boiled down to dollars and cents than when your mission is discovery.

WE NEED TO START BY UNDERSTANDING OUR SCIENCE DRIVERS’ METRICS, OR CREATING THEM.
The Scientific Awesome Facility of Excellence (SAFE) is tracking the following science metrics:

- Hours of availability to scientists per instrument
- Cost of providing each instrument/hour to scientists
- Success in embargoing raw data from instruments for 30-90 days (instrument dependent) for exclusive use of a particular project.
- Availability of the public data archive and associated science gateway to the general public, as measured in % uptime.
- Scientist satisfaction, as measured in a twice-annual survey of our two biggest target communities.
SAFE also tracks the following mission goals, not expressed as metrics:

• **REPUTATION**

• **ABILITY TO SECURE ONGOING FUNDING FROM NSF**
  • Sub-goal: keeping security budget low, because IT and security spending are considered “overhead”
  • Sub-goal: demonstrating that we are proactive with regard to ensuring data security and integrity

• **ABILITY TO SUPPORT CUTTING-EDGE AND TRANSFORMATIVE SCIENCE**

• **SUPPORT OF EARLY-CAREER RESEARCHERS THROUGH TRAINING AND ACCESSIBILITY OF OUR INSTRUMENTS AND DATA PRODUCTS**

• **OUTREACH TO THE PUBLIC TO HELP MORE YOUNG PEOPLE (K-12) BECOME PASSIONATE ABOUT STEM**
SAFE'S MANAGEMENT CAME CALLING:

- MANAGEMENT WANTS 2-5 METRICS THAT WILL DEMONSTRATE CONSISTENT “UP AND TO THE RIGHT”, DON'T SEEM TO CARE IF THEY MEAN ANYTHING.

- NO SECURITY METRICS SYSTEMATICALLY TRACKED AND RECORDED

- WE HAVE A ZEEK INSTALLATION, BUT WITH ONLY BASIC CONFIGURATION AND NO VISIBILITY TO SCIENCE DMZ...THIS IS OUR ONLY MONITORING
SAFE'S CISO TELLS THE TEAM IT'S TIME TO BRAINSTORM REAL, USEFUL METRICS

WE DON'T HAVE ANY COMPLIANCE REQUIREMENTS
That leaves target metrics and heartbeat metrics

WE CARE DEEPLY ABOUT PROCESS, OUTCOME, AND IMPACT
...but impact is unusually hard to measure in a scientific facility
<table>
<thead>
<tr>
<th>Network</th>
<th>Endpoints (E)</th>
<th>Endpoints (O)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>Email</td>
<td>Incident Response</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Program</td>
<td>Security Culture</td>
</tr>
<tr>
<td>Network</td>
<td>Endpoints (E)</td>
<td>Endpoints (O)</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Code</td>
<td>Email</td>
<td>Incident Response</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Program</td>
<td>Security Culture</td>
</tr>
</tbody>
</table>
EMAIL METRICS

- **%AGE OF STAFF ON OUR EMAIL SERVICE**
- **EMAIL VOLUME**
- **SPAM VOLUME**
- **SPAM & PHISH DETECTION**
  - Successful detection
  - False negatives
  - False positives

- **MALWARE DETECTION**
  - Successful detection
  - False negatives
  - False positives
  - Outgoing incidents

- **PHISHING EXERCISES**
  - Carried out
  - Users trained
  - Clicks
  - Conversions
**PROGRAM METRICS**

- **# OF SECURITY POLICIES**
  - Total # of policies
  - Total # of pages

- **%AGE OF POLICIES REVIEWED IN LAST 12 MONTHS**

- **SECURITY EXERCISES**
  - Total # of exercises last 12 month (rolling)
  - # last 12 months tabletop
  - # last 12 months live
  - # last 12 month with leadership participation
  - # of recommendations produced from security exercises
  - # of recommendations implemented within 3, 6, and 12 months of exercise

- **OFFBOARDING SUCCESS**

- **SHADOW IT**
  - Discoveries of shadow devices
  - Discoveries of policy violations
  - Requests from leadership for convenience exceptions

- **CONTRACTS WITH THIRD PARTIES THAT LAY OUT SECURITY REQUIREMENTS**

- **SYSTEMS REVIEWED FOR COMPLIANCE WITH ACCEPTED SECURITY POLICY**

- **STAFF TRAINED IN SECURITY RESPONSIBILITIES**
INCIDENT RESPONSE METRICS

- **MONITORED SYSTEMS AND NETWORKS**
  - % networks monitored to SEIM
  - % enterprise endpoints logging to SEIM
  - SEIM monitoring coverage (24/7/365? business hours?)
  - Manpower operating SEIM
  - Monitoring not connected to SEIM

- **TIME TO EVALUATE SEIM ALERTS OR INTERNAL NOTIFICATION**

- **TIME FOR STAFF TO NOTIFY SECURITY TEAM OF POSSIBLE INCIDENT**

- **NTP COMPLIANCE**
  - Systems synchronizing clocks via NTP
  - Systems synchronizing clocks via internal NTP

- **VULNERABILITY MANAGEMENT**

- **PROCESS ADHERENCE IN INCIDENTS AND EXERCISES**

- **INCIDENTS AND SEVERITY**
<table>
<thead>
<tr>
<th>Network</th>
<th>Endpoints (E)</th>
<th>Endpoints (O)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code</td>
<td>Email</td>
<td>Incident Response</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Program</td>
<td>Security Culture</td>
</tr>
</tbody>
</table>
1 METRICS WITH PURPOSE

2 SELECTING METRICS

YOU ARE HERE.

3 USING METRICS

4 KEEPING IT SANE: THE EVOLUTION OF SECURITY METRICS OVER TIME
SECTION 3

USING METRICS
STEPS TO EFFECTIVE METRICS:

1. START WITH THE CHEAP AND EASY
2. SYSTEMATICALLY ELIMINATE UNKNOWNS AND MATURE YOUR PROGRAM
3. ENLIST OTHER TEAMS IN IMPROVING SECURITY
4. FIND EFFICIENCIES, MAKE VENDORS PROVE THEIR VALUE
5. OLD METRICS DON'T RETIRE, THEY JUST GO FROM TARGET TO HEARTBEAT
AVOID THE BIG TRAPS

WATCH FOR ABSOLUTISM
Don't chase metrics to extremes, watch out for perverse incentives

WATCH FOR “WE’RE DONE”
Heartbeat metrics are essential.

SOME HARD-TO-MEASURE THINGS ARE STILL IMPORTANT.

SOME PEOPLE WILL EQUATE MEASUREMENT WITH BLAME.
NEVER COMMUNICATE METRICS WITHOUT PURPOSE, TARGETS, AND CONTEXT.
FIND OPPORTUNITIES TO CONNECT WITH PEER ORGANIZATIONS.
COMMUNICATE CONSISTENTLY.
METRICS WITH PURPOSE

SELECTING METRICS

USING METRICS

KEEPING IT SANE: THE EVOLUTION OF SECURITY METRICS OVER TIME

YOU ARE HERE.
WHERE METRICS CAN GET US

WHAT'S NEXT?
Organizations want to be “done” but we know the landscape changes. By systematizing and measuring what is known, we can equip ourselves to deal with the unknown.

OLD ASPIRATIONS ARE NEW DEFAULTS
Migrate target metrics to heartbeats...we've got this, so don't regress.

PUT RESOURCES IN THE RIGHT PLACES
Fix or get rid of what's not working, systematize what does.

GET YOUR ORGANIZATION MOVING
Pick something and mature it...most science orgs we work with haven't got all baseline controls in place yet.
WRAP UP

We covered a lot in a short time!

1. METRICS WITH PURPOSE
2. SELECTING METRICS
3. USING METRICS
4. KEEPING IT SANE: THE EVOLUTION OF SECURITY METRICS OVER TIME
Visit the ResearchSOC website: https://researchsoc.iu.edu/

Subscribe to the ResearchSOC announcements list: https://researchsoc.iu.edu/contact/index.html

Read the ResearchSOC Blog: https://blogs.iu.edu/researchsoc/

Join our Community of Practice: https://ask.cyberinfrastructure.org/c/rsoc

Follow ResearchSOC on Twitter @IUResearchSOC
Upcoming ResearchSOC Events

**Webinars:**
How to secure scientific data flows in research projects.
May 21, 2020 3pm EST

[https://researchsoc.iu.edu/webinars](https://researchsoc.iu.edu/webinars)

**Conferences:**
Educause SPC virtual presentations (TBD)
PEARC Virtual
July 26-30
Thank you!

We thank the National Science Foundation (grant 1840034) for supporting our work.

The views and conclusions herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.

Susan E. Sons
sesons@iu.edu
https://researchsoc.iu.edu