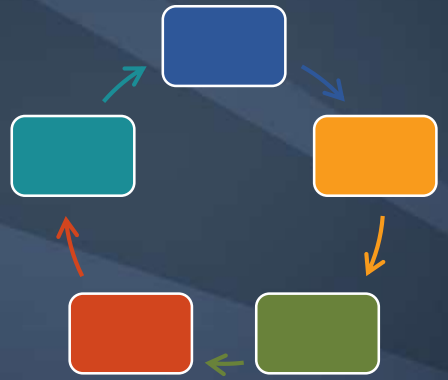
FIREEYE™

Tuning ICS Security Alerts:

An Alarm Management Approach



Chris Sistrunk, PE

Technical Manager, ICS/OT Security

SA x20

Overview

Remember: Threats and Risks aren't going away, so they should guide detection and response goals

- Detection
  - Engineering the system: Philosophy and Tuning
    - **Security alert engineering** is similar to ICS alarm engineering
    - **ISA 18.2** & **EEMUA 191** Alarm Management Standards
    - **NIST SP 800-94** Guide to Intrusion Detection & Prevention Systems

- Response
  - Incident response playbooks
  - Following the plan

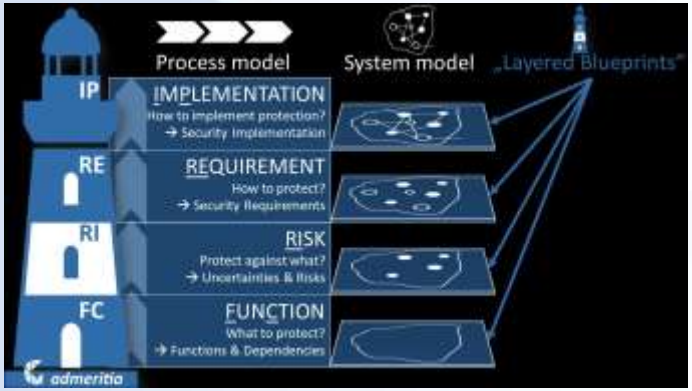
Know your Systems

Knowledge is the most powerful tool
to operate and defend your system.

- How does my system work?
- What are my threats / risks?
- Do I have enough visibility?
- Do I practice my plans?

Recap: Security Engineering

- S4x19 Sarah Fluchs: Layered Blueprints for OT Security

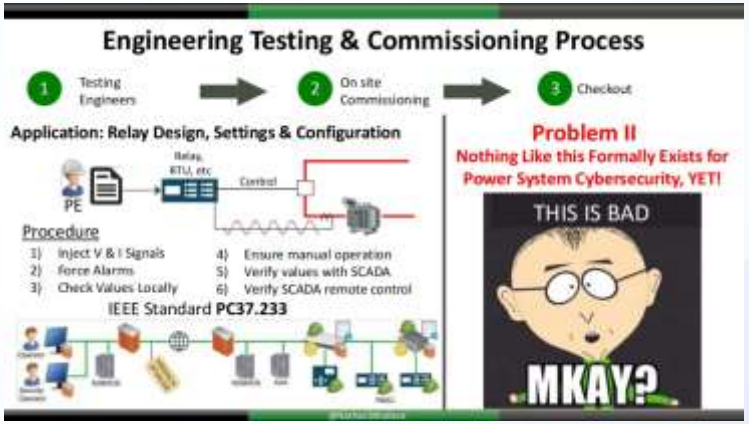


https://www.youtube.com/watch?v=bBjMZnoSYUs

https://www.controlglobal.com/articles/2019/making-ot-security-engineering-deserve-its-name

- S4x19 Nathan Wallace:
  Making Power System Cybersecurity Part of the Engineering Process

https://www.slideshare.net/NathanWallacePhDCSSA/s4x19-stage-2-making-power-system-cybersecurity-part-of-the-engineering-process



ICS Security Alert Management

Problem:

There is little published about ICS security alert management. Asset owners have to learn by doing things the hard way without a guide.

Theory:

- ICS Alarm management is well-defined
- IT security alert management is well-defined
- ICS security alert management must be *engineered*

Solution:

Create a reference that combines the key concepts from both philosophies to empower ICS security teams and asset owners.

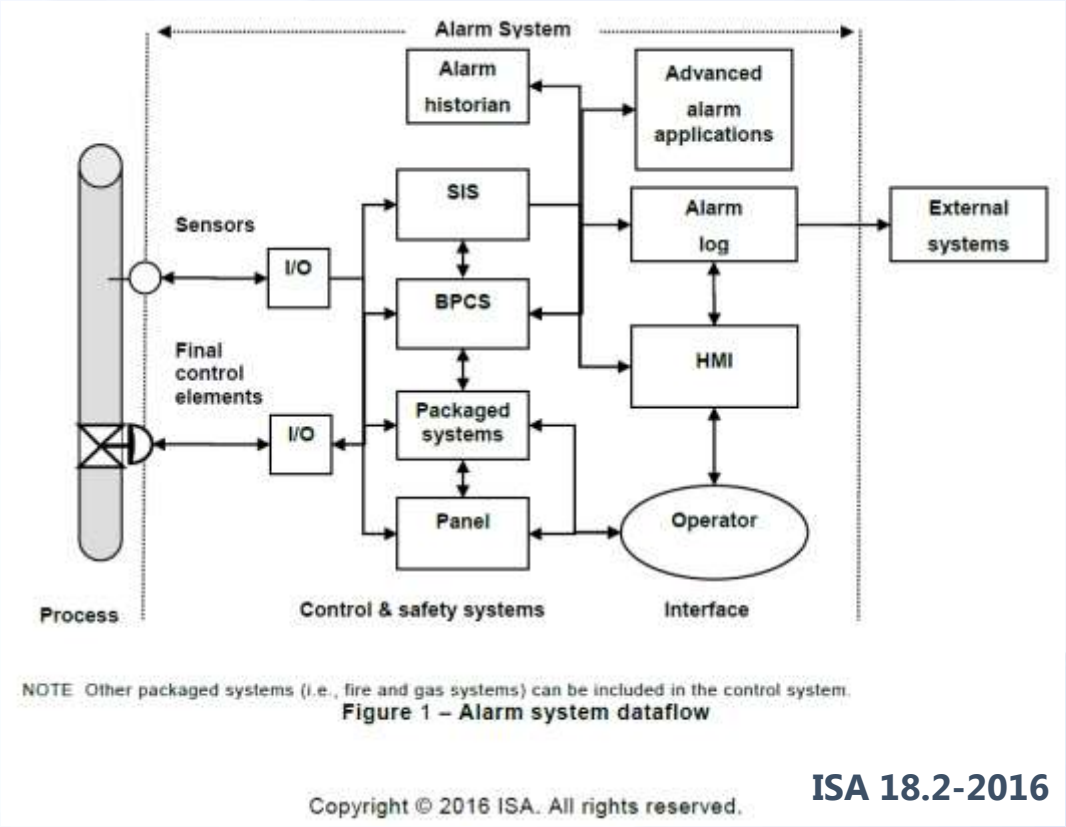
https://twitter.com/_LittleBobby_/status/1211340859091947520

ISA 18.2-2016

"The primary function within the alarm system is to notify operators of abnormal process conditions or equipment malfunctions and support the response."

NIST SP 800-94

(Feb 2007)
"Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices."

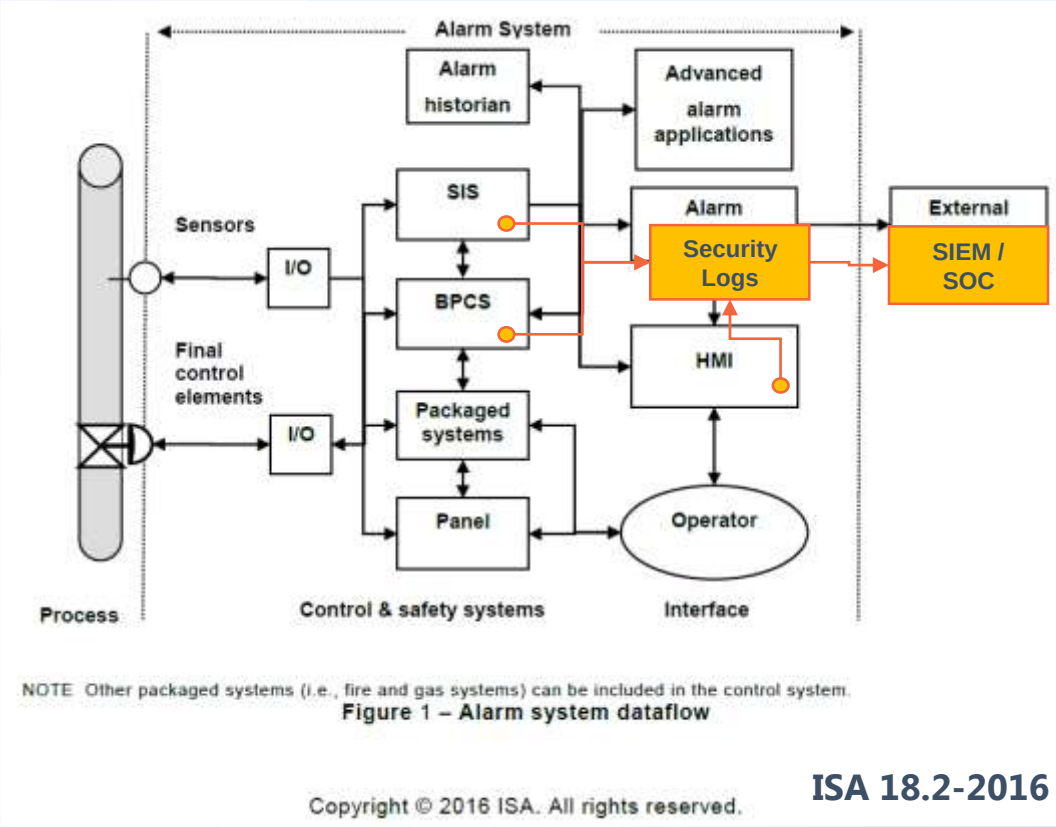


ISA 18.2-2016

"The primary function within the alarm system is to notify operators of abnormal process conditions or equipment malfunctions and support the response."

NIST SP 800-94

(Feb 2007)
"Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices."



Where/what should we collect and detect?

Threats and Risks define goals and ultimately drive your Security Alert Philosophy

Operations
Monitor the process & assets, KPIs, safety, regulatory, etc

Security
Monitor the network & assets for malicious activity, safety, regulatory, etc

You can't see where you aren't looking!

You can't do forensics either.

Engineering Forensics
"Root Cause Analysis"

Digital Forensics

Alert Philosophy

ISA 18.2

"The **philosophy** starts with the **basic definitions** and extends them to **operational definitions**. The criteria for alarm prioritization and the definition of alarm classes, performance metrics, performance limits and reporting requirements are **based on the objectives and principles for alarm systems**."

Create/Document ICS Security Alert Philosophy

- Define security operations for ICS
- Define ICS specific alert categories and priorities
- Define and measure metrics
- Align with existing philosophies (IT alert, ICS alarm)

Philosophy Checklist – EEMUA 191

1.	Clearly define the intention of the alarm system.
2.	Indicate the goals/performance targets of alarm systems (which will be reflected in any relevant engineering specification).
3.	Define how the design and operation of alarm systems will be appropriately executed, monitored and audited.
4.	Define any technical terms used (e.g. eclipsing, suppression, etc.).
5.	Clearly lay out the methodology for managing the alarm systems, including: • the management of change, • the setting of alarm priorities, • guidance on the selection of alarm settings, • other items (specify) .....
6.	Define the management of change mechanisms.
7.	Define the mechanisms for addressing Human Factors issues.
8.	Define the training requirements.
9.	Define the auditing mechanism.

alert
alert
alert
IoC, network attack, Sandworm
alert
incident
rule

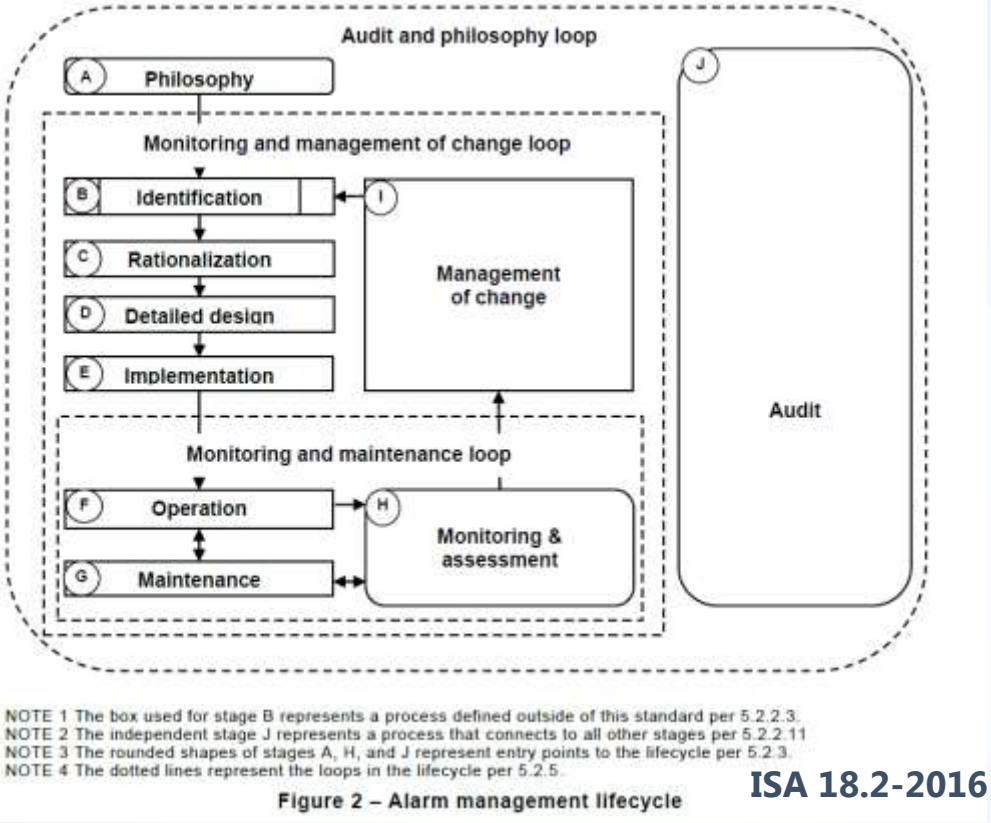
Engineering Equipment and Materials Users Association

UK based
51 member companies
O&G and Chem

https://www.eemua.org/Products/Publications/Checklists/EEMUA-alarms-checklist.aspx

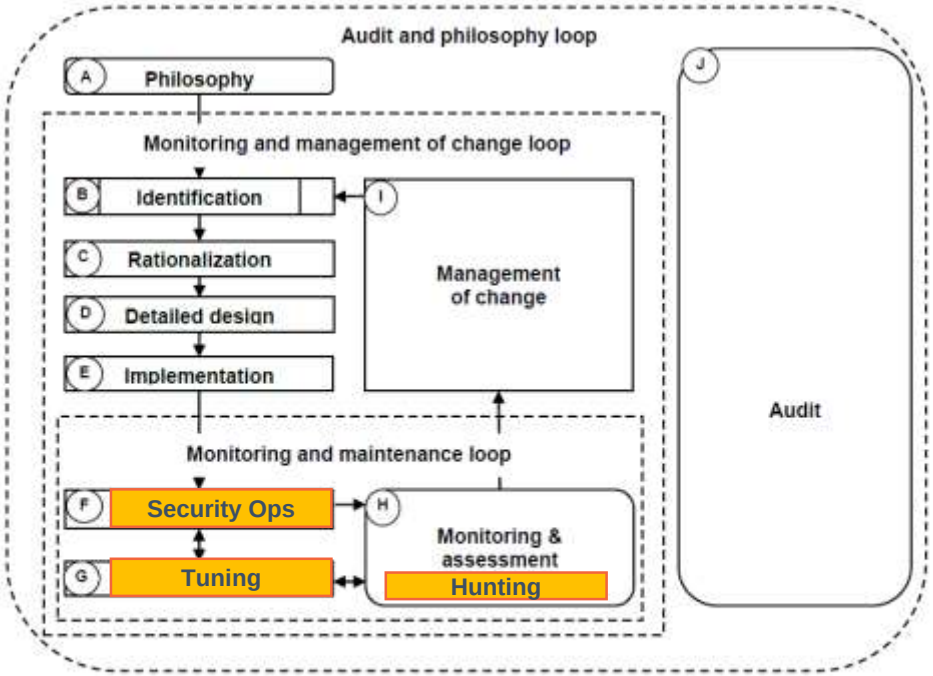
FREE

Security Alert Management



ISA 18.2-2016

Security Alert Management



NOTE 1 The box used for stage B represents a process defined outside of this standard per 5.2.2.3.
NOTE 2 The independent stage J represents a process that connects to all other stages per 5.2.2.11
NOTE 3 The rounded shapes of stages A, H, and J represent entry points to the lifecycle per 5.2.3.
NOTE 4 The dotted lines represent the loops in the lifecycle per 5.2.5.

Figure 2 – Alarm management lifecycle

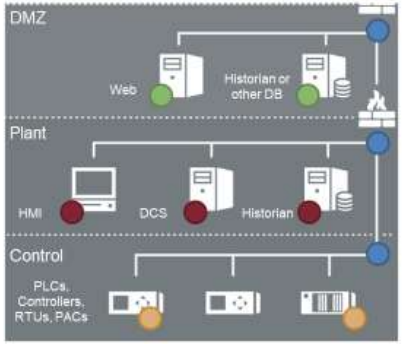
ISA 18.2-2016

Recap: Where/what will we detect?

- S4x15 Talk

NSM Collection

Enterprise technology collectors
Logs and/or Agent
Network sensors
Logs only

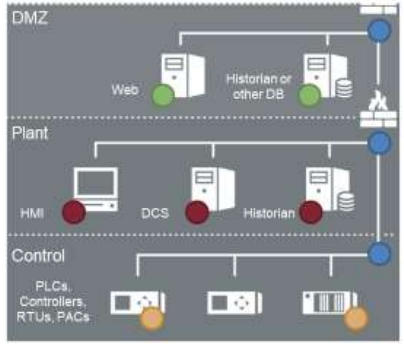


- Firewall Logs
- Netflow Data
- NIDS/HIDS
- Full packet capture or NetFlow
- Windows Logs and syslog
- SNMP (CPU % etc.)
- Alerts from security agents (AV, whitelisting, etc.)

17

NSM Detection

Analyst looks at detected anomalies or alerts then escalates to IR

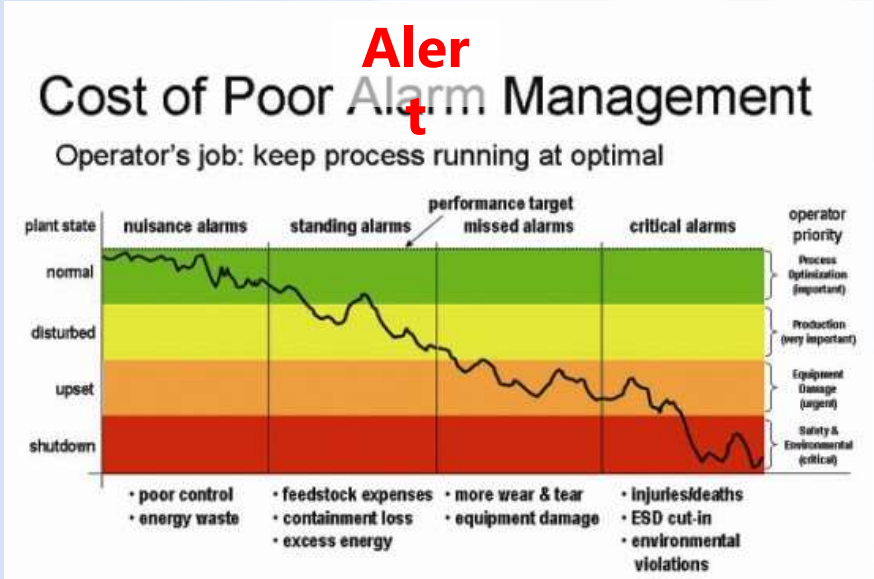


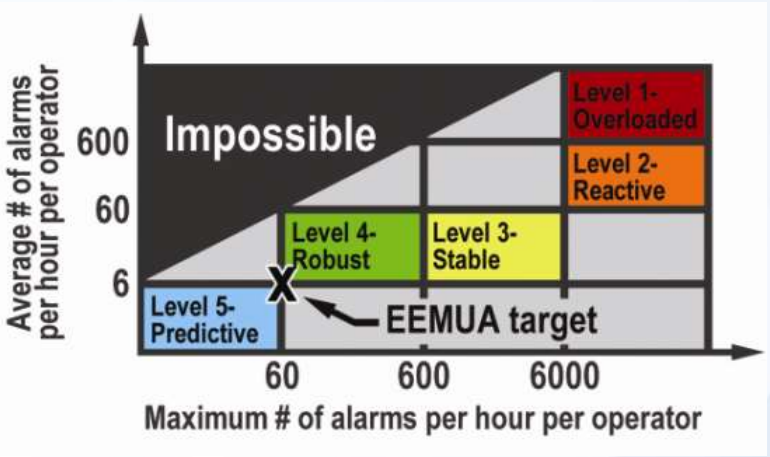
- IDS alerts
- Anomaly detection
- Firmware updates, other commands
- Login with default credentials
- High CPU or network bandwidth
- Door alarms when nobody is supposed to be working
- Devices going off-line or behaving strangely

19

Tuning

- **Create** and **Refine** reliable IDS rules
- **Actively Manage** your ICS network sensors

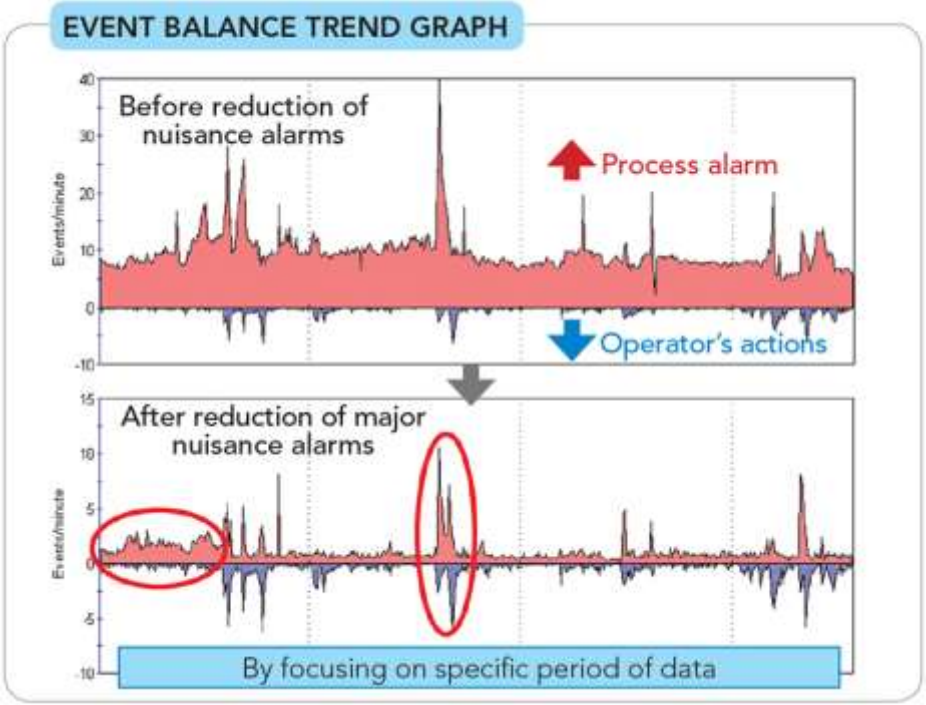




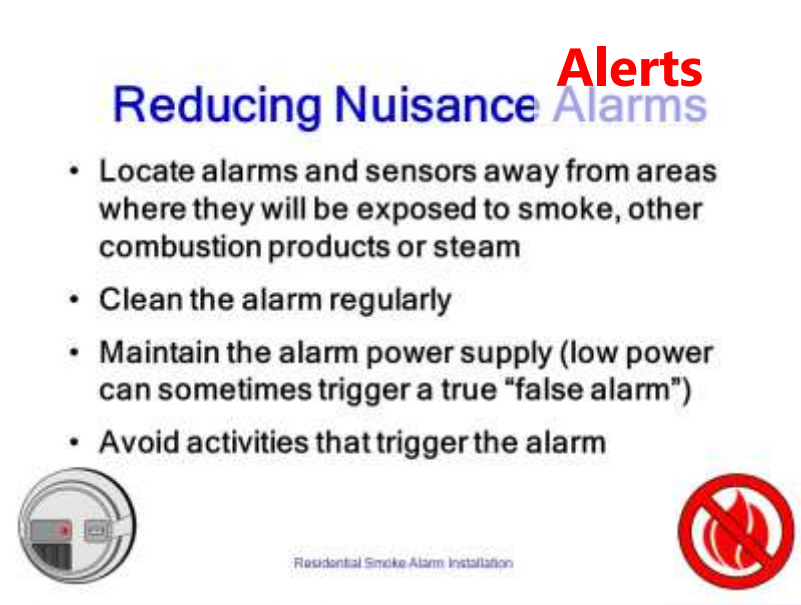
Is a critical alert lost in a mountain of nuisance alerts?

https://www.automation.com/library/articles-white-papers/alarm-monitoring-management/keeping-the-peace-and-quiet

Reducing Nuisance Alerts



https://www.chemicalprocessing.com/articles/2018/optimize-alarm-management/



http://www.mc.uky.edu/kiprc/fire/Residential%20Smoke%20Alarm%20Installation.ppt

Examples when you don't tune

- [insert favorite IDS or ICS NSM sensor here]
- You installed it, it is collecting data, but soon…

- There are 800,000 active security alerts and baselining feature wasn't used
  - Mesh radios like to change IP addresses: could have added their MAC's to the asset list to prevent alerts
- Bro/Zeek by default alerts on every function code for each ICS protocol


Richard Bejtlich
@taosecurity

To all the academic security teachers: please stop giving your students assignments to run "Bro" to generate alerts and find "bad traffic." @Zeekurity is inherently policy-neutral. Vern built it to generate transaction logs for network traffic, not decide what is good or bad.

12:18 PM · Nov 27, 2019 · Twitter Web App

Collect them all???

https://www.wsj.com/articles/sorry-collectors-nobody-wants-your-beanie-babies-anymore-1519234039

NEWS

False positives still cause threat alert fatigue

How you set up and prioritize which alerts to look at and act on is the basis for an effective threat management strategy.

By Ryan Francis

Contributor, CSO | MAY 3, 2017 3:31 AM PDT

https://www.csoonline.com/article/3191379/false-positives-still-cause-alert-fatigue.html

MARKET NEWS MARCH 13, 2014 / 8:35 AM / 6 YEARS AGO

Target missed early alert of credit card data breach -report

https://www.reuters.com/article/target-breach/target-missed-early-alert-of-credit-card-data-breach-report-idUSL2N0MA0KF20140313

Confusion Matrix

True Positive (TP): • Reality: A wolf threatened. • Shepherd said: "Wolf." • Outcome: Shepherd is a hero.	**False Positive (FP):** • Reality: No wolf threatened. • Shepherd said: "Wolf." • Outcome: Villagers are angry at shepherd waking them up.
False Negative (FN): • Reality: A wolf threatened. • Shepherd said: "No wolf." • Outcome: The wolf ate all the sheep.	**True Negative (TN):** • Reality: No wolf threatened. • Shepherd said: "No wolf." • Outcome: Everyone is fine.

Hat tip to @mubix: https://twitter.com/mubix/status/1201923641979654146
Google: https://developers.google.com/machine-learning/crash-course/classification/true-false-positive-negative

Recap: Where do we start?

- S4x19 On-ramp Talk

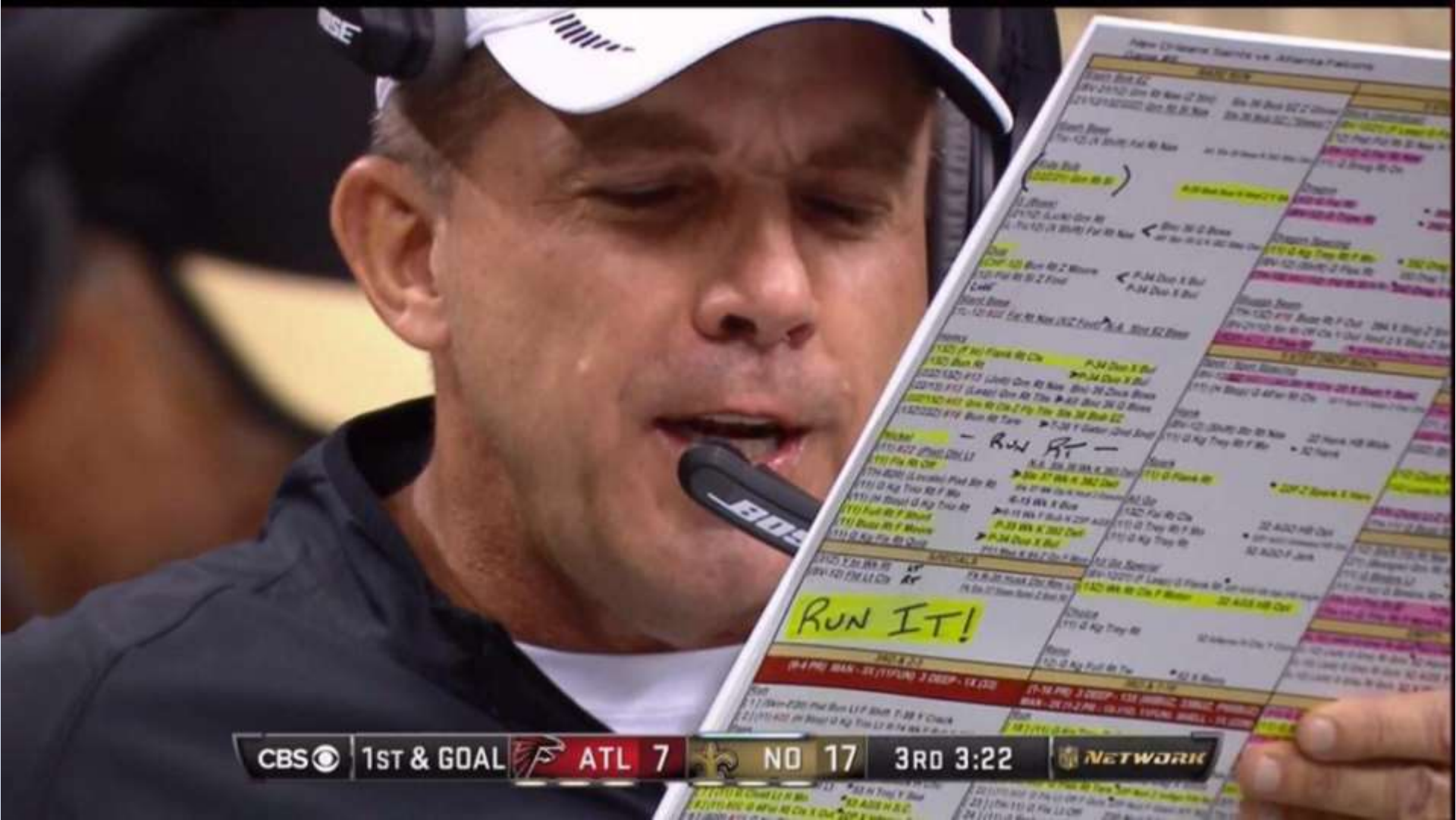
Start small
Use what and who you already have

- Detection is a continuum > use capability you have until you need more
- Don’t overwhelm yourself right off the bat
- Measure your success

Focus on the Basics

- SOC analysts > buy donuts for the ICS Engineers & SMEs
  - Work together to define the ICS Alert Philosophy
  - Use your existing ICS alarm and SOC alert standards as the reference
    - If you don't have them, use ISA 18.2, EEMUA 191, and NIST SP 800-94
- Start with the ICS DMZ firewall or other ingress/egress points
- Choose from existing firewall logs, Windows logs, switch logs – not all
- Tune IDS or ICS NSM sensors (leverage your vendors during install)

- DON'T put ICS Security Alerts on the HMI
- Operators don't need extra burden > leave it to the SOC analysts


RUN IT!
CBS
1ST & GOAL
ATL 7
NO 17
3RD 3:22
NFL NETWORK

Playbooks and Use Cases

1. Commodity Malware
   - Conficker, Ramnit
2. Credential Compromise
   - Ukraine Power Grid, ladder logic change (Aurora)
3. Destructive Attack
   - KillDisk, overwriting firmware (Ukraine)
4. "Stop the bleeding" if it's a serious situation
   - Wiper malware (NotPetya) or ransomware spreading

Remediation for each play:

- Restore backups, reset passwords, etc

"RUN IT!"

Run it!

- Design plays for each phase
- Practice those drills
- Use your players' strengths
- Exploit their weaknesses
- Finish strong!

Knowledge is the most powerful tool

1

Know and harden the network

- Review what you already have (tighten rules, accounts, backups, etc)
- Identify critical assets and ingress/egress points

2

Know and tune the network visibility

- Review your existing alarm/alert standards
- Philosophy > implementation > monitoring > metrics

3

Know what to do when an incident occurs

- Review your disaster recovery and incident response plans
- Run it! > Practice your playbooks

ICS Alarm Management

References

- **ISA18.2-2016** Alarm Management Standard > aka **IEC 62682**
- https://www.isa.org/intech/201606standards/
- **ISA-TR18.2.2-2016** Alarm Identification and Rationalization
- https://www.isa.org/intech-plus/2017/november/beyond-alarm-management/
- https://www.rockwellautomation.com/resources/downloads/rockwellautomation/pdf/events/automation-fair/2011/psug/afpsug11_ed16.pdf - **excellent**
- https://en.wikipedia.org/wiki/Alarm_management
- https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/white-papers/pas-understanding-and-applying-ansi-isa-18-2-alarm-management-standard/
- https://www.automation.com/library/articles-white-papers/alarm-monitoring-management/keeping-the-peace-and-quiet
- **EEMUA Publication 191** Alarm systems - a guide to design, management and procurement
- https://www.eemua.org/Products/Publications/Print/EEMUA-Publication-191.aspx
- *The Alarm Management Handbook, 2nd Ed.,* Hollifield and Habibi, PAS Inc. 2010.

Security Alert Management

References

- **NIST SP 800-94**, Guide to Intrusion Detection and Prevention Systems (IDPS)
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
  - Tuning, 2-3, 3-3, 3-4, 4-11, 5-10, 6-5, 7-6
- https://securityonion.readthedocs.io/en/latest/tuning.html
- https://securityonion.readthedocs.io/en/latest/alerts.html
- https://www.zeek.org/current/slides/2016_educause_configuration_and_tuning.pdf
- https://developers.google.com/machine-learning/crash-course/classification/true-false-positive-negative
- *Applied Network Security Monitoring: Collection, Detection, and Analysis.* Sanders and Smith. Syngress, 2013.

Security Engineering

- https://www.controlglobal.com/articles/2019/making-ot-security-engineering-deserve-its-name

Thank you!

chris.sistrunk@mandiant.com
@chrissistrunk
Technical Manager, ICS/OT