SANS

Mark @ Northern Kentucky University

15 Oct 2020

Mark Jeanmougin, Security Engineer at SAP Concur
SANS Community Instructor

Disclaimer

The information presented here is not intended for use by anyone. If you try to follow along at home and get a hangnail, instantiate global thermonuclear war, or have other adverse side effects: You’re on your own. Mark, as well as his past, current, or future employers, family members, and pets disclaim any and all responsibility from now until the end of the Universe.

Zoom Etiquette

DISABLE YOUR CAMERA

DISABLE YOUR MICROPHONE

Don’t give feedback

Confuse the presenter

Don’t let the presenter know what you want to learn

Quietly be frustrated that the presenter isn’t talking about things you care about

Don’t take steps to improve your position in life

Zoom Etiquette FOR REALZ!

Give feedback! Non-Verbal or verbal

Let the presenter know what you want to learn

Let the presenter know when he talks about things you care about

Take steps to improve your position in life!

Bad Day?

Fraud

Public Facing Web Server

SIEM? Be glad logging was enabled

SOC: When you have an interesting day, someone else is having a bad day.

Agenda

✓ Intro

❑ whoami

❑ Stages of Incident Response

❑ Common Techniques for Incident Detection

❑ Incident Response

❑ Forensics?

❑ How to Read

❑ Q&A

Ask Questions!

$ whoami

- Mark Jeanmougin (markjx@gmail.com / @markjx01)
  - mark.jeanmougin@sap.com
- Always Blue Team (SOC / CFC)
- SANS Community Instructor
- Digital Forensics & Incident Response
  - Inappropriate Internet Use & Academic Fraud
- IT for >20 years. Security since 2000.

Stages of Incident Response

Preparation

Identification

Containment

Eradication

Recovery

Lessons Learned

Engineers: Preparation & Lessons Learned

Analysts: Identification (Another attack? Reinfection? Or incomplete Identification?)

Containment, Eradication, & Recovery: Everyone

* Lock the doors & call KFC

Incident Response

When people think about IR, they usually mean:

Containment, Eradication, Recovery

But, the whole PICERL process applies. If you start pulling pieces out of the whole, it falls apart.

Proper Identification is key. EVERYTHING else builds on it

Detection: Alerts

Many tools generate alerts drawing Analyst attention:

- Anti-Virus
- IDS
- Web Proxy / Firewall

Contextual Information

Other tools generate information about what’s going on in your environment.

  - “Past you” configures them to record & ignore certain event types.
  - What’s interesting is left for “future you”.

Examples:

- Event Logs / CloudTrail / EDR (sysmon)
- Security Onion / Bro / Zeek
- Web Proxy / DNS Logs / DoH / Firewall

Incident Detection Data Sources

Detection Tools?

- Intrusion Detection System (IDS)
  - Snort / Suricata
- Security Incident & Event Management (SIEM)
- Event Detection & Response (EDR)
  - sysmon

Incident Detection Data Sources – I got P on it

Preventative Tools?

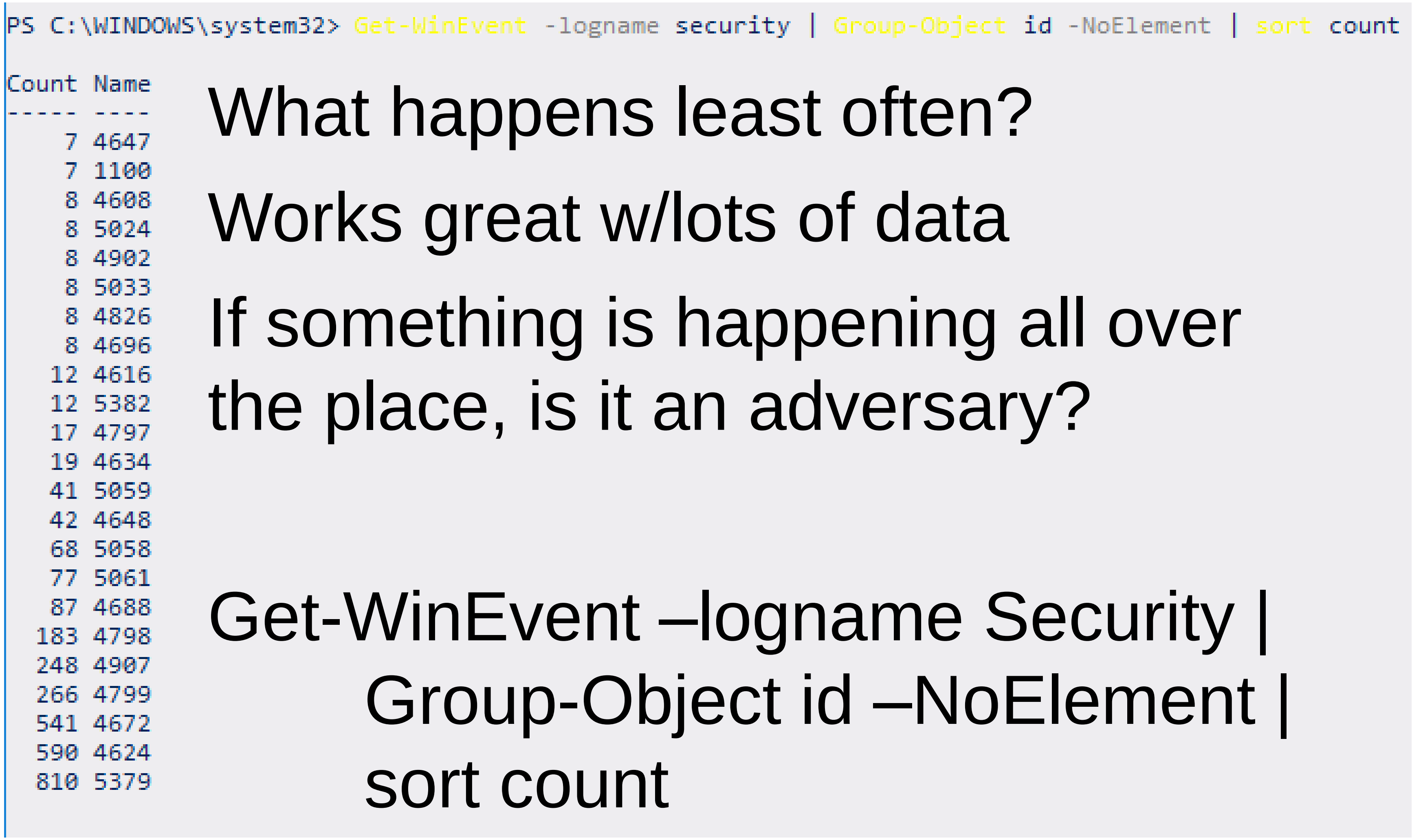
- Anti-Virus
- Firewall
- IPS
  - Why is an IPS fundamentally different from an IDS?

- Risk = (Threat * Vuln) – Mitigations
  - Businesses don’t exist to “be secure”

Incident Detection – SIEM Alerts

True Positive	If a SIEM alert fires, it should require corrective action
False Positive?	Tweak rule so you never see that again

Stack Ranking



```
PS C:\WINDOWS\system32> Get-WinEvent -logname security | Group-Object id -NoElement | sort count

Count Name
----- ----
    7 4647
    7 1100
    8 4608
    8 5024
    8 4902
    8 5033
    8 4826
    8 4696
   12 4616
   12 5382
   17 4797
   19 4634
   41 5059
   42 4648
   68 5058
   77 5061
   87 4688
  183 4798
  248 4907
  266 4799
  541 4672
  590 4624
  810 5379
```

What happens least often?

Works great w/lots of data

If something is happening all over the place, is it an adversary?

Get-WinEvent –logname Security |
        Group-Object id –NoElement |
        sort count

Works with:

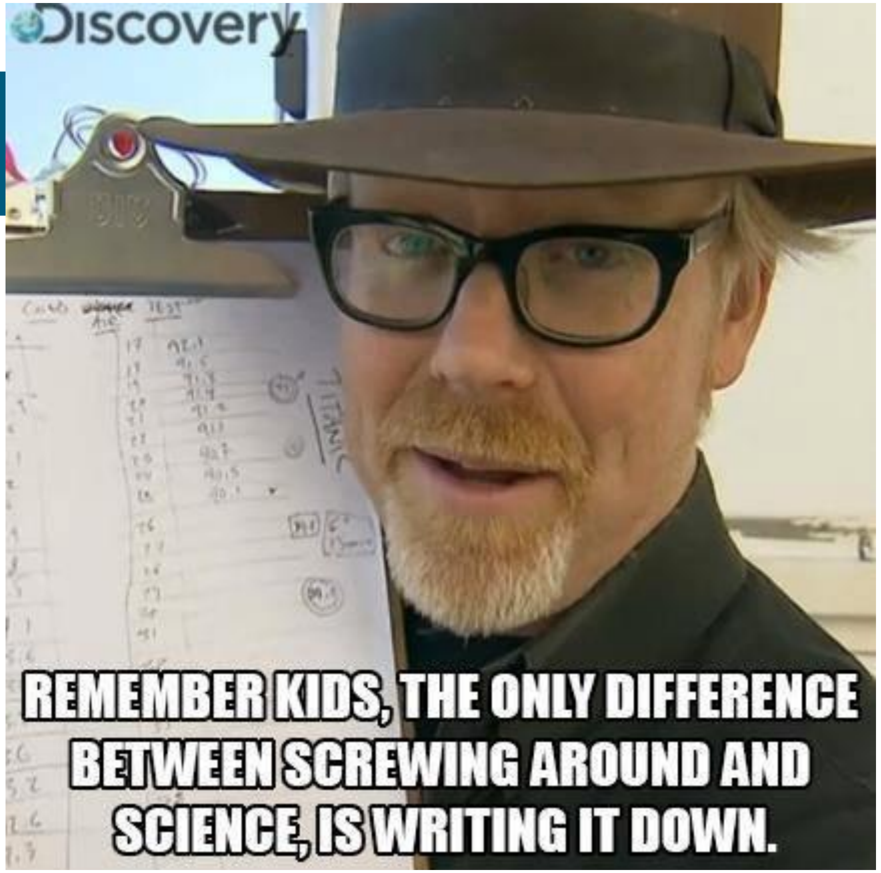
- Web Logs
- DNS Logs
- EDR sha1’s
- email From:
- Log: Event ID

Threat Hunting

Go out and look for bad guys

Scientific Method

- Create Hypothesis
- Gather Data
- Tweak Hypothesis
- Occam’s Razor


Discovery
REMEMBER KIDS, THE ONLY DIFFERENCE BETWEEN SCREWING AROUND AND SCIENCE, IS WRITING IT DOWN.

Incident 1

8 Figure Deductible

Incident 2

Rekall
Forensics

We can remember it for you wholesale!

Jobs Right out of College

SOC Analyst

Security Engineer

Compliance

Identity & Access Management (IAM)

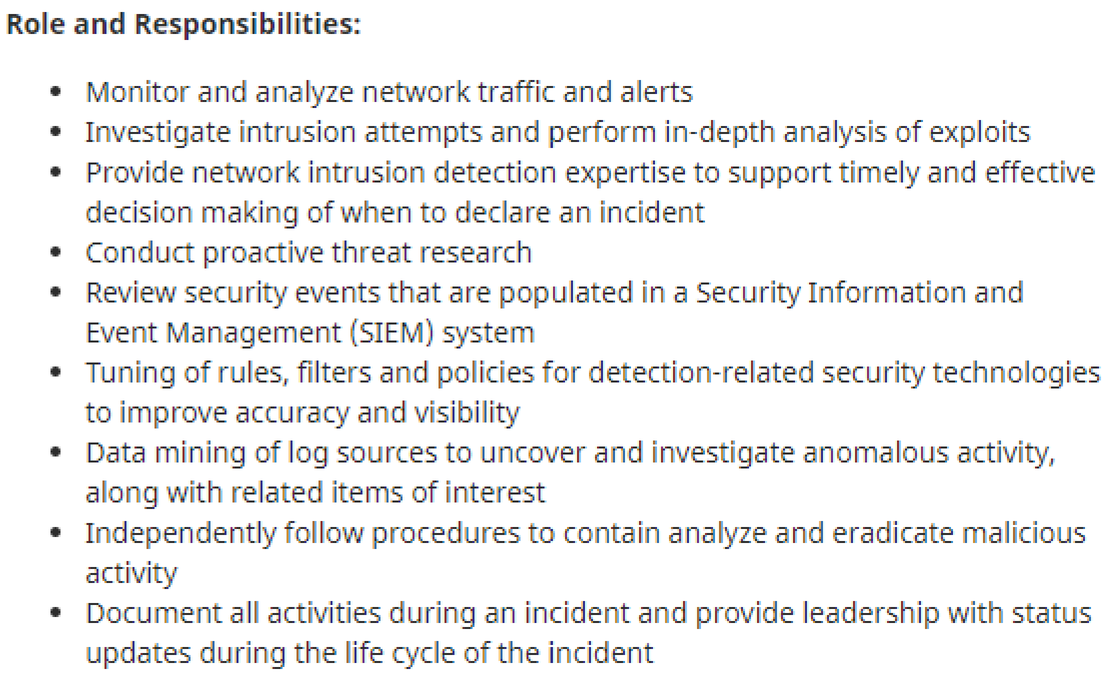
Cloud

“Consultant” (SkyMiles & Marriott Points)

Mark’s Personal Views

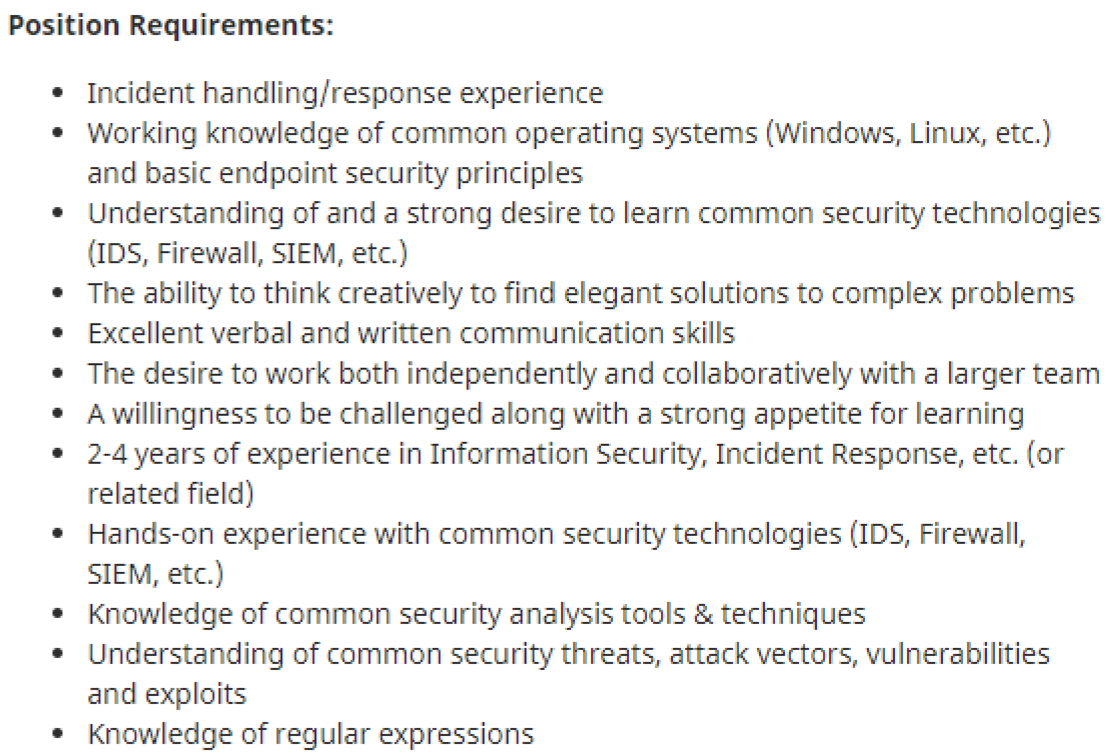
How to read… a Job Description

https://www.indeed.com/viewjob?jk=9526535853d391ae&tk=1eki22db4p94m800&from=serp&vjs=3



Role and Responsibilities:

- Monitor and analyze network traffic and alerts
- Investigate intrusion attempts and perform in-depth analysis of exploits
- Provide network intrusion detection expertise to support timely and effective decision making of when to declare an incident
- Conduct proactive threat research
- Review security events that are populated in a Security Information and Event Management (SIEM) system
- Tuning of rules, filters and policies for detection-related security technologies to improve accuracy and visibility
- Data mining of log sources to uncover and investigate anomalous activity, along with related items of interest
- Independently follow procedures to contain analyze and eradicate malicious activity
- Document all activities during an incident and provide leadership with status updates during the life cycle of the incident



Position Requirements:

- Incident handling/response experience
- Working knowledge of common operating systems (Windows, Linux, etc.) and basic endpoint security principles
- Understanding of and a strong desire to learn common security technologies (IDS, Firewall, SIEM, etc.)
- The ability to think creatively to find elegant solutions to complex problems
- Excellent verbal and written communication skills
- The desire to work both independently and collaboratively with a larger team
- A willingness to be challenged along with a strong appetite for learning
- 2-4 years of experience in Information Security, Incident Response, etc. (or related field)
- Hands-on experience with common security technologies (IDS, Firewall, SIEM, etc.)
- Knowledge of common security analysis tools & techniques
- Understanding of common security threats, attack vectors, vulnerabilities and exploits
- Knowledge of regular expressions

Position Requirements

- Incident handling/response experience
- Working knowledge of common operating systems (Windows, Linux, etc.) and basic endpoint security principles
- Understanding of and a strong desire to learn common security technologies (IDS, Firewall, SIEM, etc.)
- The ability to think creatively to find elegant solutions to complex problems
- Excellent verbal and written communication skills
- The desire to work both independently and collaboratively with a larger team
- A willingness to be challenged along with a strong appetite for learning
- 2-4 years of experience in Information Security, Incident Response, etc. (or related field)
- Hands-on experience with common security technologies (IDS, Firewall, SIEM, etc.)
- Knowledge of common security analysis tools & techniques
- Understanding of common security threats, attack vectors, vulnerabilities and exploits
- Knowledge of regular expressions

Hacker Lifestyle

© GETTY IMAGES /

Wrap Up

Q&A

https://sap.com/careers

My Contact Info:

markjx@gmail.com @markj01

aws

DigitalOcean

Azure

Webinars

Teach Yo Self

Homelab