MIDWEST RELIABILITY ORGANIZATION

MRO SAC Hosted Webinar

"Security Information and Event Management (SIEM)"

Justin Haar, Cyber Security Specialist, Minnkota Power Cooperative, MRO SAC Member

May 19, 2021

Disclaimer

The Midwest Reliability Organization (MRO) Security Advisory Council (SAC) is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging security topics. Subject Matter Experts (SMEs) develop materials, including presentations, through the MRO SAC from member organizations within the MRO Region and other government and industry security experts. The views in this presentation do not express the opinions and views of MRO.

MRO SAC/SACTF Tentative 2021 Meetings and Events

- **SACTF:**
  - Threat Call at 8:15 a.m. on Wednesday Mornings
  - COVID-19 Call at 8:15 a.m. on Thursday Mornings
- **SAC**
  - MRO SAC Quarter 2 Meeting on **June 23, 2021** (Registration is Open)
  - Security Technical Training on **October 5, 2021**
  - Security Conference on **October 6, 2021**
  - Regional Security Risk Assessment on **October 7, 2021**
  - MRO SAC Quarter 4 Meeting on **November 3, 2021** (Registration is Open)

"Security Information and Event Management (SIEM)"

Justin Haar

Minnkota Power Cooperative

MRO SAC

JUSTIN HAAR

Justin Haar is the Cyber Security Specialist for Minnkota Power Cooperative (MPC). In his current position, Justin is taking a leading role in the grown MPC's Cyber Security Program. Along with his position at MPC, Justin is also serving as a member of the MRO SAC. Justin has been in the IT Security industry since 2009. In that time he worked as an Information Security Consultant for small and medium-sized financial institutions. He also spent several years managing to IT Department of a mining company in northern Minnesota. Justin received a B.S. in Computer and Network Security and an M.S. in Information Assurance From Dakota State University. Justin also holds several industry certifications including the CISSP.

WHAT IS SIEM

What is a SIEM

- Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).

  - Gartner

Why is SIEM important

- Benefits of SIEM include:
  - Central Point of Information Collection
  - Increased efficiency
  - Detect and Identify potential security threats
  - Reducing the impact of security breaches
  - Improved and centralized reporting, log analysis, and retention
  - compliance

SIEM IN A WORD

- Correlation!
  - A SIEM makes it easier then ever to correlate events that occur across different systems and reporting sources, making it easier to identify potential issues.

GETTING STARTED

Why did Minnkota implement a SIEM

- Above and beyond compliance
- Correlation of data across silos
- View into the entire enterprise, not just small subsets.

Getting Started

- Identification of Needs \ Requirements
  - New SIEM / Upgrade\replace an existing SIEM
  - Identify environments you wish to have reporting to the SIEM
  - Identify the number and type of devices you will want sending logs to the SIEM
  - Identify your retention requirements
  - Network Flow Traffic
  - Cloud vs On Premises systems.
  - Staffing Needs
  - Licensing
  - Financial objectives

Identify environments you wish to have reporting to the SIEM

- IT
- OT
- Substation
- Distribution
- Transmission
- Generation

- Getting Data Out of Sensitive Environments

Retention Needs

- How long do you need data for?
- How long does that data need to be searchable?
- Do you have a need to store a subset of data for a longer period of time?
- On Premises System
  - Hot Storage
  - Warm Storage
  - Cold Storage
- Cloud
  - Variable
  - Retention may be fixed the vendor.

Cloud vs On Prem.

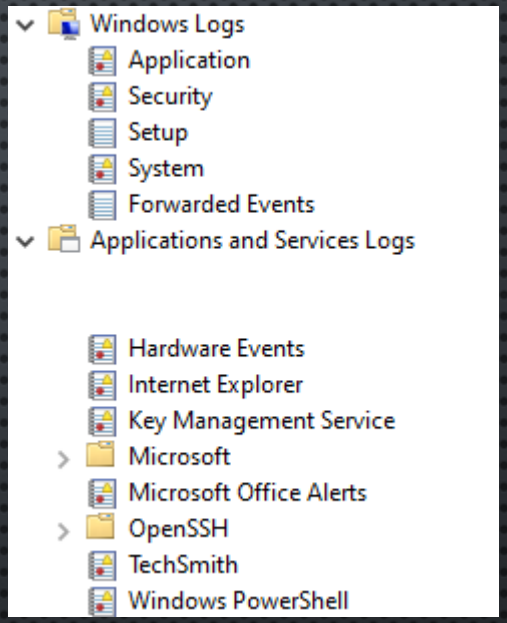
- Cloud Advantages
  - Op Ex Cost
  - No need / limited need to on site equipment
  - Backend maintenance handled by vendor
  - Scalable
  - Low Startup Costs
- Cloud Disadvantages
  - Op Ex Cost
  - Limited Retention Period
  - Requires larger internet pipe,
  - Variable billing costs based on utilization
  - Confidentiality challenges

Cloud vs On Prem.

- On Premises Advantages
  - Cap Ex Cost
  - Hardware can be scaled to meet your needs
  - Accessible to sensitive internal networks
- On Premises Disadvantages
  - Cap Ex Cost
  - Larger up front costs
  - Only scalable to a point before more purchases are needed

LICENSING

- Per Device
- Per Log Source
- Rate of data
- Combination



Financial Objectives

- Cap Ex vs Op Ex
- Vendor Hours needs
- SOC (Security Operation Center) as a Service
- Staffing Impacts
  - Care and Feeding

Right Size for your Organization

- Long Term Investment
- Capable of Growing to meet your long term needs
- What are your staffing availability and commitments?

TIPS AND TRICKS

Logging Configuration

- Systems log a lot of things and most of it is junk.
- Determine What you want to Log and don't want to Log
  - CIS Standards for different operating systems (OS)
  - OS Hardening Standards
  - Manufacturer recommendations

Other Log Sources

- Anti-Virus Software
- Application Logs
- SQL Logs
- Exchange Logs
- SAS applications

- Always ask, "How is this logged?"

Object Level Logging in Windows

- Highly detailed change logging for targeted objects
- Avoid global level Object Level Auditing
- Use targeted settings where needed.

Data Normalization / Noise Reduction

- Identify a log that is generating a lot of activity
- Figure out why that log is generating that activity
- Determine a response
  - Stop the logging
  - Drop / do not index the log
  - Ignore the log
  - Retain the log
- Track
- Repeat!

PowerShell

- Transcript Logs
  - In all versions of PowerShell
  - You get all the commands and all the outputs for each session
  - Cannot Always see enf-to-end activities (subscripts
  - Only works for current user's host sessions
- Script Block Logging
  - Records Everything PowerShell does
    - Starting in Windows 10 Protected Event Logging features added to hide PII and sensitive data
- Module Logging
  - Targeted to specific modules, but is more verbose.

Terminology

- Log – Raw Information
- Event – Indexed object, could contain a single log or a count of logs
- Alarm – An alert based on certain event criteria
  - Response Process
    - Who
  - Playbooks

Common Windows Event ID's

- 4624 – Account Login
- 4625 – Failed Logon
- 4720 – User was Created
- 4722 – User was Enabled
- 4724 – Privileged User Changed this Users Password
- 4738 – Account Changed
- 4740 – Account Locked
- 4767 – Account Unlocked
- 4728 – Member Added to a Global Security Group
- 4732 – Member Added to a Local Security Group

Common Windows Event ID's

- 1102 – Clear Event Log
- 7045 – New Windows Service
- 1022, 1033 – New MSI File Installed
- 903, 904 – New Application Installed
- 905, 906 – Updated Application
- 907, 908 – Removed application
- 4688 – New Process Created
- 4697 – New Service Installed
- 4698 – New Scheduled Task
- 43 – New Device Information
- 400, 410 – New Mass Storage Installation

USER LOGON / FAILED LOGON INDICATORS

Logon Types	
2	Interactive
3	Network (i.e. mapped drive)
4	Batch (i.e. schedule task)
5	Service (service startup)
7	Unlock (i.e. unnattended workstation with password protected screen saver)
8	Network Cleartext (Most often indicates a logon to IIS with “basic authentication”)
10	Remote Desktop
11	Logon with cached credentials

Logon Failure Codes	
0xC0000064	User name does not exist
0xC000006A	User name is correct but the password is wrong
0xC0000234	User is currently locked out
0xC0000072	Account is currently disabled
0xC000006F	User tried to logon outside his day of week or time of day restrictions
0xC0000070	Workstation restriction
0xC00000193	Account expiration
0xC0000071	Expired password
0xC0000133	Clocks between DC and other computer too far out of sync
0xC0000224	User is required to change password at next logon
0xC0000225	Evidently a bug in Windows and not a risk
0xC000015b	The user has not been granted the requested logon type (aka logon right) at this machine

https://www.ultimatewindowssecurity.com/securitylog/quickref/default.aspx

Closing Tips

- Keep an eye out for systems that should be reporting in, but are not.
- A shared accurate time source is essential.
- Refine your alerts.
- Identify Roles and Responsibilities, especially for response actions.
- Tie your response to your Incident Response Plan
- Google is your most powerful tool

QUESTIONS

Your feedback is very important to us. Please provide your feedback using the link or QR Code below or the link below:

https://www.surveymonkey.com/r/6JT5DHY

Thank You!