OT SIEM

GLOSSARY - V1.0

BY

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

OT SIEM LEVELING GUIDE 1-60
GENERAL SKILLS
GLOSSARY
VERSION 1.0

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

INTRODUCTION

HOW IT FITS WITH LEVELING GUIDE 1-60

Welcome to OT SIEM Glossary, a foundational resource designed to complement the OT SIEM Leveling Guide 1-60.

This document organizes terms into the 3 main categories:

[>] Industrial

[>] Security

[>] Documentation

to help you build a clear understanding of OT SIEM.

Like networks, devices, protocols, security concepts and standards.

Mastering these terms will provide the language and knowledge needed to advance through the guide and apply OT SIEM concepts effectively.

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

INDUSTRIAL - NETWORK

NETWORK COMPONENTS & ARCHITECTURE

ethernet - common wired network connection

mac address - media access control identifier

mac filtering - controlling network access

ip address - internet protocol identifier

packets - basic network data units

vlan - virtual local area network

dmz - demilitarized zone

level 3 switch - managed layer 3 network devices

level 2 switch - unmanaged layer 2 network devices

router - connect two networks with different IP addresses

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

INDUSTRIAL - DEVICES

ICS DEVICES & ROLES

field devices - end devices like sensors and actuators

ows - operator workstation

ews - engineering workstation

scada - supervisory control & data acquisition

historian - centralized database for data

hmi - human machine interface

dcs - distributed control system

plc - programmable logic controller

rtu - remote terminal unit

sis - safety instrumented system

jump host - secure intermediary for remote access

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

INDUSTRIAL - PROTOCOLS

COMMUNICATION METHODS IN ICS

ftp/sftp - file transfer protocol / secure

telnet/ssh - remote access protocols / secure

http/https - web communication protocols / secure

modbus - communication protocol for ICS

opc da - open platform communications data access

opc ua - open platform communications unified architecture

iec 101/104/61850 - standards for power automation

profinet/profibus - industrial ethernet protocols

dnp3 - distributed network protocol

tcp - transmission control protocol

udp - user datagram protocol

syslog - logging standard for devices

snmp - simple network management protocol

ntp - network time protocol

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

INDUSTRIAL - CONFIGURATION

PROGRAMMING AND SYSTEM SETUP

discrete/analog signals - signal types in field devices

coil/register - memory elements in modbus

commands - read, write, control modes

plc program - ladder logic, structured text, etc

scada project - overall system design & configuration

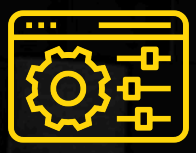
ld - ladder logic

il - instruction list

st - structured text

fbd - function block diagram

sfc - sequential function chart



predictive maintenance - monitoring equipment to predict failures

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

INDUSTRIAL - PHYSICAL

HARDWARE & SENSORS

24v dc - common power standard in ics

actuator - device for moving or controlling a mechanism

cycle/ms - plc cycle time / milliseconds

sensors - field devices for data collection

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

SECURITY - CONCEPTS

SECURITY PRINCIPLES AND TERMS

siem - security information & event management

av - antivirus software

edr - endpoint detection and response

xdr - extended detection and response

firewall - device for traffic filtering

traffic filtering - controlling inbound/outbound network flows

dpi - deep packet inspection

certificate - digital certificate for authentication and encryption

tls - transport layer security for encryption

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

SECURITY - THREATS

RISKS & ATTACK METHODS

attack - unauthorized actions targeting a system

threat - potential dangers to ICS systems

cve - common vulnerabilities and exposures

vulnerability - weaknesses in systems or configurations

exploit - malicious code or technique targeting vulnerabilities

payload - malicious code delivered during an attack

zero-day - vulnerabilities exploited before patches are available

rce - remote code execution

reconnaissance - information gathering about a target

privilege escalation - gaining higher access rights

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

SECURITY - TOOLS

SECURITY TOOLS & TECHNIQUES

pentest - penetration testing to assess vulnerabilities

scanning - searching for vulnerabilities in systems

nmap - network mapping and scanning tool

sniffer - tool for capturing network packets

wireshark - packet analysis tool

tcpdump - command-line packet analysis tool

port forwarding - redirecting traffic through specific ports

pivoting - using compromised systems to attack others

reverse shell - remote shell from target to attacker

fuzzer - sending random inputs

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

SECURITY - MALWARE

MALICIOUS SOFTWARE & EXPLOITS

exe - executable file format

dll - dynamic link library used in malware

registry - windows os configuration database for persistence

rat - remote access trojan

trojan - malicious software disguised as legitimate

ransomware - malware that encrypts data for ransom

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

SECURITY - LOGGING

EVENT COLLECTION & ANALYSIS

security log - records of security-related events

agent - software for log collection

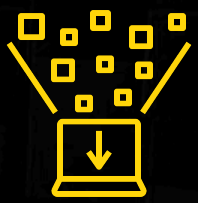
cef - common event format

csv - comma-separated values log format

json - data format for logs

winevent - windows event logs

eventid - unique identifier for events in logs



ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

SECURITY - SCRIPTING

HACKING & AUTOMATION

python - programming language for automation and exploits

powershell - scripting language for windows

bash - unix/linux shell scripting language

compilation - converting source code to machine code

disassembly - breaking down machine code for analysis

obfuscation - hiding code to evade detection

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

DOCUMENTATION - ADVERSARY

ATTACK METHODS & STAGES

adversary - entity conducting malicious activities

c2 - command & control

enumeration - identifying and listing target resources

reconnaissance - information gathering about a target system

scanning - probing networks or systems for vulnerabilities

remote access - ability to control a system remotely

initial access - first stage of an attack, gaining entry

persistence - maintaining access to a system over time

evasion - avoiding detection by security systems

lateral movement - spreading within a network

impact - final stage causing damage or disruption

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

DOCUMENTATION - STANDARDS

FRAMEWORKS & BEST PRACTICES

mitre attack - framework for categorizing adversary behavior

nist - national institute of standards and technology

cyber kill chain - framework describing the stages of a cyber attack

iec 62443 - standard for industrial cybersecurity

playbook - pre-defined response steps for incidents

taxonomy - classification system for cyber threats

use case - specific scenario for detection or response

cis controls - best practices for cybersecurity

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

DOCUMENTATION - DETECTION

IDENTIFYING & ANALYZING THREATS

alert - notification triggered by detection systems

false positive - non-malicious activity flagged as a threat

tactics - high-level goals of an adversary

techniques - specific methods used to achieve tactics

behavioral analysis - detecting anomalies based on behavior

signature-based detection - matching known attack patterns

anomaly detection - identifying unusual behavior

ioc - indicators of compromise, clues of malicious activity

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

DOCUMENTATION - RESPONSE

INCIDENT HANDLING & RECOVERY

soc - security operations center

incident - identified security event requiring response

forensics - analyzing evidence from security incidents

correlation - linking events across systems to detect patterns

response plan - predefined steps for handling incidents

remediation - fixing issues after an incident

reporting - documenting incidents for stakeholders

timeline - chronological sequence of events during an attack

ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

DOCUMENTATION - ASSETS

TRACKING & MANAGING RESOURCES

asset - physical or digital resource in a network

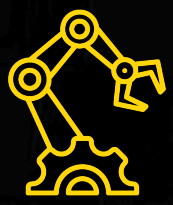
inventory - list of all assets in the system

configuration baseline - standard settings for devices

version control - tracking changes to system configurations

firmware - low-level software running on hardware

patching - applying updates to fix vulnerabilities



ZAKHAR BERNHARDT
LINKEDIN.COM/IN/ZAKHARB

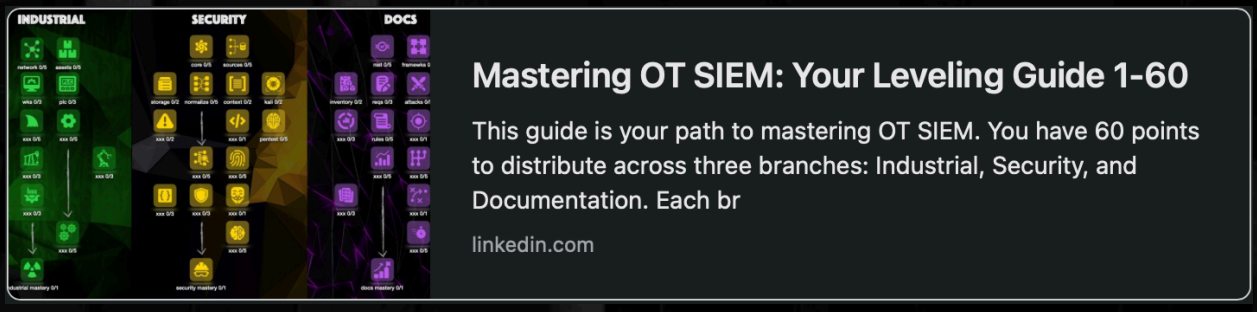
CONCLUSION

SUMMARY & KEY TAKEAWAYS

This glossary is your first step in mastering OT SIEM concepts, providing a solid foundation for understanding the terminology used in industrial networks, security practices, and documentation standards. As you progress through the OT SIEM Leveling Guide, refer back to these terms to deepen your knowledge and confidently apply them in real-world scenarios.

THANKS A LOT
YOURS
ZAKHAR BERNHARDT
FOLLOW ME ON
LINKEDIN.COM/IN/ZAKHARB

YOU CAN USE OT SIEM LEVELING GUIDE FOR MORE INFO



https://www.linkedin.com/pulse/ot-siem-leveling-guide-0-60-zakhar-bernhardt-7fczf/