SEC+
Lesson 12:
Explain Alerting and Monitoring Concepts

Objectives

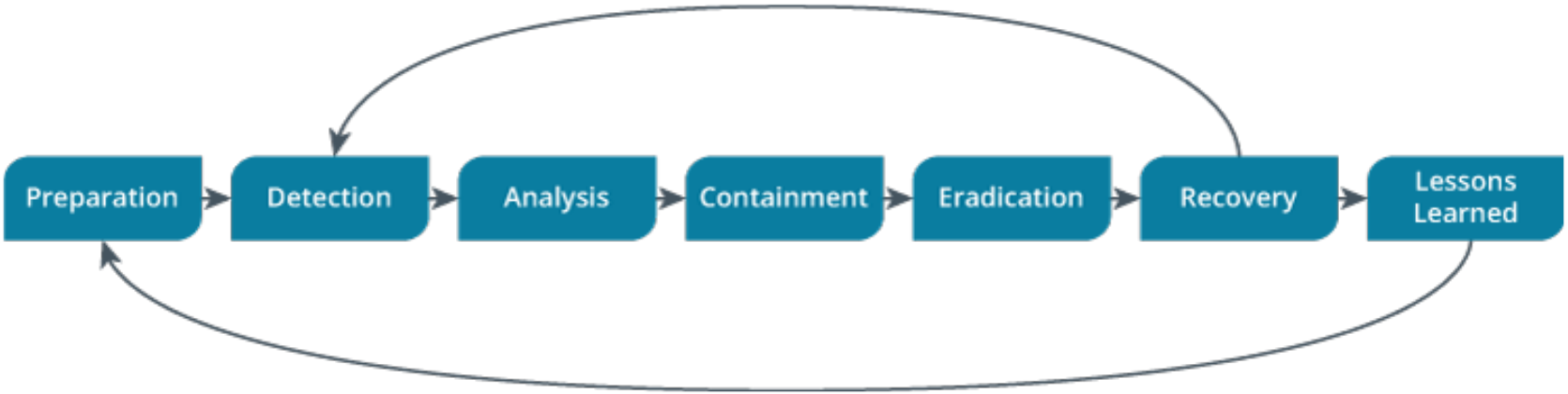
- Summarize incident response and digital forensics procedures
- Utilize appropriate data sources for incident investigations
- Explain security alerting and monitoring concepts and tools

Lesson 12

Topic 12A

Incident Response

Incident Response Processes



Preparation (1)

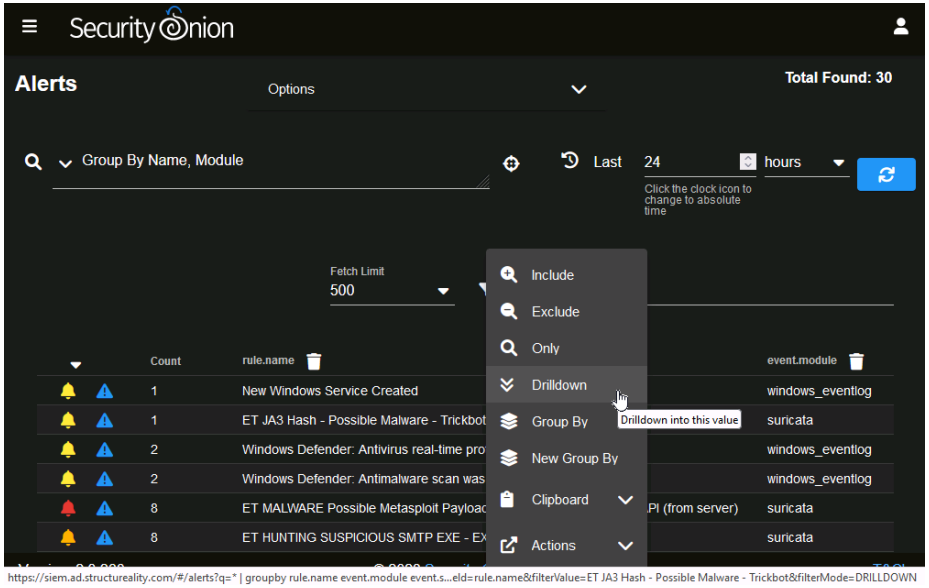
- Cybersecurity infrastructure
- Cyber Incident Response Team
  - Reporting, categorizing, and prioritizing (triage)
  - CIRT/CERT/CSIRT/SOC
  - Management/decision-making authority
  - Incident analysts
  - Roles beyond technical response
    - Legal, Human Resources (HR), Marketing

Preparation (2)

- Communication plan
  - Prevent inadvertent disclosure
  - Call list identifying trusted parties
  - Share data on a need to know basis
  - Out-of-band communications—avoid alerting intruder
- Stakeholder management
  - Communication with internal and external stakeholders
  - Notification and reporting
- Incident response plan (IRP)

Detection

- Detection channels
  - Monitoring and alerting from logs and other data sources
  - Deviation from baseline metrics
  - Manual inspection
  - Notification procedures
  - Public reporting and whistleblowing
- First responder
  - Member of CIRT taking charge of a reported incident



Analysis

- Analysis and incident identification
  - Classify and prioritize
  - Downgrade low priority alerts to log-only
- Impact
  - Data integrity, downtime
  - Economic/publicity
  - Scope
  - Detection time, recovery time
- Category
  - Kill chains and threat intelligence
- Playbooks

Containment

- Issues
  - Loss control
  - Countermeasures available
  - Preserving evidence
- Isolation-based containment
- Segmentation-based containment

Eradication and Recovery

- Reconstitution of affected systems
- Reaudit security controls
- Ensure that affected parties are notified

Lessons Learned

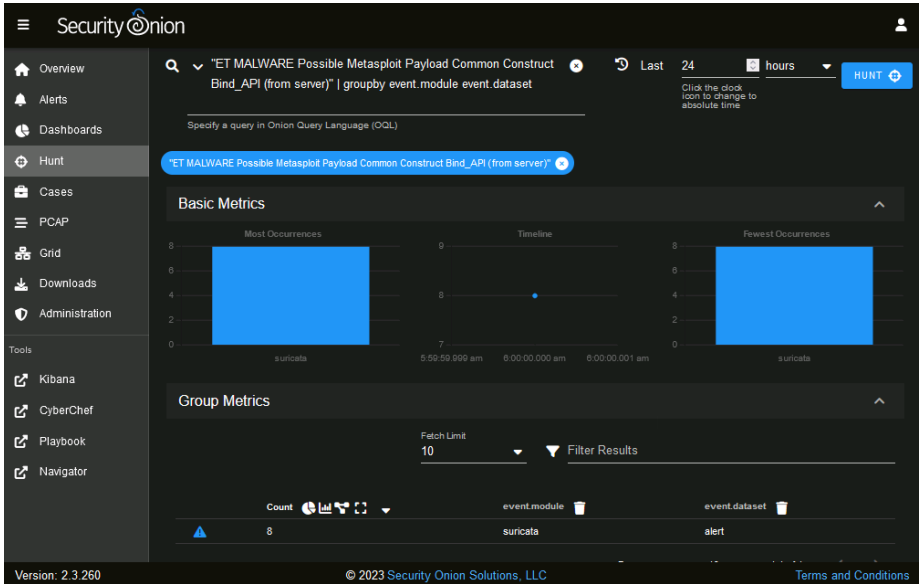
- Meet and report
- Root cause analysis
  - Five whys
  - Drill through incident with questions: Who, why, when, where, how, what
  - Walkthrough timeline

Testing and Training

Members of the Kentucky and Alabama National Guard participate in a simulated network attack exercise.
(Photo by Kentucky National Guard Maj. Carla Raisler.)

- Testing
  - Tabletop
    - Facilitator presents a scenario
    - Does not involve live systems
  - Walkthroughs
    - Responders demonstrate response actions
  - Simulations
    - Red team performs a simulated intrusion
- Training

Threat Hunting



The Hunt dashboards in Security Onion can help to determine whether a given alert affects a single system only (as here), or whether it is more widespread across the network. (Screenshot courtesy of Security Onion securityonion.net.)

- Proactive process compared to reactive incident response
- Warning of new threat types
- Intelligence fusion and threat data
- Maneuver
  - Awareness that threat actor might take countermeasures

Incident Response

- Incident response processes
  - Preparation
  - Detection
  - Analysis
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
- Testing and training
- Threat hunting

Lesson 12

Topic 12B

Digital Forensics

Due Process and Legal Hold

- Digital forensics
  - Collecting evidence from computer systems to a standard that will be accepted in a court of law
- Evidence, documentation, and admissibility
  - Latent evidence
  - Collection must be documented
- Due process
  - Evidence collection and analysis procedures that ensure fairness
- Legal hold
  - Right to seize systems as evidence

Acquisition

- Legal seizure and search of devices
- Computer on/off state
- Order of volatility
  - CPU registers, cache memory, and non-persistent system memory (RAM)
  - Data on persistent storage
  - Remote logging and monitoring data
  - Physical configuration and network topology
  - Archival media

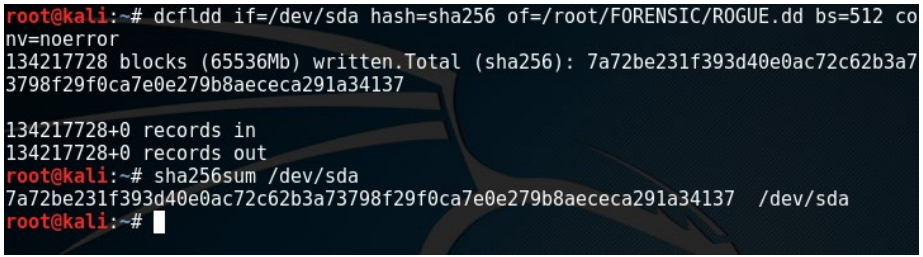
System Memory Acquisition

- Evidence recovery from non-persistent memory
  - Contents of temporary file systems, registry data, network connections, cryptographic keys, …
- Live acquisition
  - Pre-install kernel driver

```
c:\Users\James\Downloads>volatility_2.6_win64_standalone.exe -f c:\dumps\memory.dmp --profile=Win7SP1x64_23418 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----
0xfffffa83020a7040 System                    4      0    106      632 ------      0 2020-01-09 21:20:03 UTC+0000
0xfffffa8303d6d1d0 smss.exe                308      4      2       29 ------      0 2020-01-09 21:20:03 UTC+0000
0xfffffa83035f26a0 csrss.exe               396    388      8      370      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83034fe060 wininit.exe             432    388      3       75      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83036295e0 csrss.exe               444    424      8      293      1      0 2020-01-09 21:20:05 UTC+0000
0xfffffa8303716b30 winlogon.exe            492    424      3      109      1      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83035fab30 services.exe            528    432     10      276      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa8303732b30 lsass.exe               536    432      8      636      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa830373db30 lsm.exe                 544    432     10      142      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83037436a0 svchost.exe             652    528     10      349      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83037e66a0 svchost.exe             716    528      7      235      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83036566a0 svchost.exe             772    528     18      445      0      0 2020-01-09 21:20:05 UTC+0000
0xfffffa83038bb060 svchost.exe             892    528     18      417      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa83038fcb30 svchost.exe             936    528     32      940      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa830393c060 svchost.exe             324    528     17      385      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303960060 svchost.exe             744    528     15      379      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa83039b7060 spoolsv.exe            1060    528     12      271      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa83039dd060 svchost.exe            1096    528     19      316      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303a58960 vmicsvc.exe            1192    528      5      126      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303a70b30 vmicsvc.exe            1216    528      7      217      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303a8c060 vmicsvc.exe            1264    528      4       78      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303accb30 vmicsvc.exe            1296    528      5       92      0      0 2020-01-09 21:20:06 UTC+0000
0xfffffa8303b32920 vmicsvc.exe            1340    528      3       82      0      0 2020-01-09 21:20:07 UTC+0000
0xfffffa8302ab3210 svchost.exe            1436    528     10      179      0      0 2020-01-09 21:20:07 UTC+0000
0xfffffa8303bcf800 svchost.exe            1528    528      3       43      0      0 2020-01-09 21:20:08 UTC+0000
0xfffffa8303c963a0 svchost.exe            1816    528      5       99      0      0 2020-01-09 21:20:08 UTC+0000
0xfffffa8303ac5b30 svchost.exe            1976    528     14      323      0      0 2020-01-09 21:20:10 UTC+0000
0xfffffa8303155b30 taskhost.exe           1964    528      9      157      1      0 2020-01-09 21:20:14 UTC+0000
0xfffffa83031c3830 sppsvc.exe             2072    528      7      158      0      0 2020-01-09 21:20:14 UTC+0000
0xfffffa8303262060 dwm.exe                2352    892      3       70      1      0 2020-01-09 21:20:18 UTC+0000
0xfffffa8303238060 explorer.exe           2376   2344     24      784      1      0 2020-01-09 21:20:18 UTC+0000
0xfffffa83033a2b30 jusched.exe            2520   2456      8      233      1      1 2020-01-09 21:20:18 UTC+0000
0xfffffa8303ba0b30 SearchIndexer.         2568    528     11      656      0      0 2020-01-09 21:20:24 UTC+0000
0xfffffa830326a060 procexp64.exe          2900   2376      8      382      1      0 2020-01-09 21:20:45 UTC+0000
0xfffffa83036406a0 WmiPrvSE.exe           3024    652      7      118      0      0 2020-01-09 21:20:51 UTC+0000
0xfffffa8303703190 Tcpview.exe             916   2376      6      139      1      1 2020-01-09 21:21:27 UTC+0000
0xfffffa8302839b30 salter.exe             1808   2376      6      134      1      1 2020-01-09 21:23:49 UTC+0000
0xfffffa8303818230 WMIADAP.exe             380    936      5       85      0      0 2020-01-09 21:24:08 UTC+0000
```

Screenshot: Volatility Framework volatilityfoundation.org.)

Disk Image Acquisition



Using dcfldd (a version of dd with additional forensics functionality created by the DoD) and generating a hash of the source-disk data (sda).

- Non-volatile storage media and devices
- Acquisition types
  - Live acquisition
  - Static acquisition by shutting down the host
  - Static acquisition by pulling the plug
- Imaging utilities
  - Forensic software suites and file formats

Preservation

- Timeline and provenance
  - Record process of evidence acquisition
  - Use a write blocker
- Evidence integrity and non-repudiation
  - Cryptographic hashing and checksums
  - Take hashes of source device, reference image, and copy of image for analysis
- Chain of custody
  - Integrity and proper handling of evidence from collection, to analysis, to storage, and finally to presentation
  - Secure tamper-evident bagging
  - Secure storage facility and protection against environmental hazards

Reporting

- Summarizes contents of the digital data
- Conclusions from the investigator's analysis
- Professional ethics
  - Analysis must be performed without bias
  - Analysis methods must be repeatable
  - Evidence must not be changed or manipulated
- E-discovery
  - Electronically Stored Information (ESI)
  - Identify and de-duplicate files and metadata and facilitate search and tagging
  - Protect access and make tamper-evident
  - Facilitate disclosure

Digital Forensics

- Due process and legal hold
- Acquisition
  - Order of volatility
- System memory acquisition
- Disk image acquisition
- Preservation
  - Evidence integrity, reference hash, chain of custody
- Reporting
  - E-discovery

Lesson 12

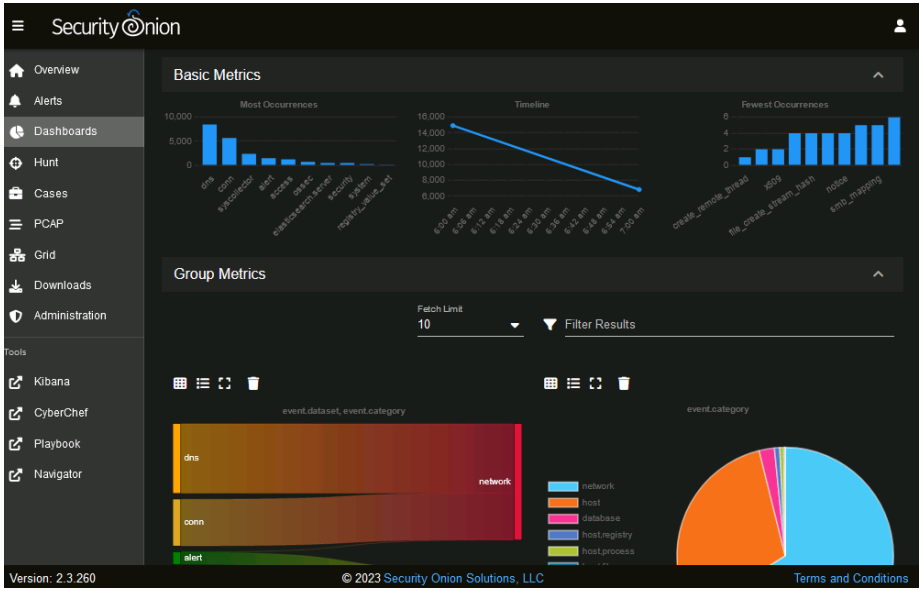
Topic 12C

Data Sources

Data Sources, Dashboards, and Reports (1)

- System memory and media device file system data and metadata
- Log files generated by network appliances
- Network traffic captured by sensors and/or intrusion detection systems
- Log files and alerts generated by network-based vulnerability scanners
- Log files generated by the OS components of client and server hosts
- Log files generated by applications and services running on hosts
- Log files and alerts generated by endpoint security software installed on hosts

Data Sources, Dashboards, and Reports (2)



Screenshot courtesy of Security Onion (securityonion.net.)

- Analyst dashboard
  - Console of alerts that require prioritization and investigation
- Manager dashboard
  - Overall status indicators
- Automated reports
  - Alerts and alarms
  - Status reports for response team, business managers, business owners, and compliance

Log Data

- Event
  - Format and source (local or redirected over network)
  - Event data versus metadata
- Windows Event Viewer
- Syslog
  - PRI – facility and severity
  - Header with timestamp and host
  - Message part

```
<5>Mar 12 05:11:40 LX1 kernel: [ 8399.702841] netfilter - ACCEPT
  IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=10.1.0.102 DST=10.1.0.10
  LEN=88 TOS=0x00 PREC=0x00 TTL=128 ID=11507 DF PROTO=TCP SPT=1901 DPT=22 WINDOW=32767 RES=0x00 ACK PSH URGP=0
<5>Mar 12 05:11:46 LXI kernel: [ 8404.945586] netfilter - ACCEPT
  IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=10.1.0.102 DST=10.1.0.10
  LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=11510 DF PROTO=TCP SPT=1906 DPT=80 WINDOW=65535 RES=0x00 SYN URGP=0
<4>Mar 12 05:12:07 LXI kernel: [ 8426.739265] netfilter - DROP
  IN=eth0 OUT= MAC=00:15:5d:01:ca:55:00:15:5d:01:ca:ad:08:00 SRC=10.1.0.102 DST=10.1.0.10
  LEN=52 TOS=0x00 PREC=0x00 TTL=128 ID=11613 DF PROTO=TCP SPT=1911 DPT=21 WINDOW=64240 RES=0x00 SYN URGP=0
```

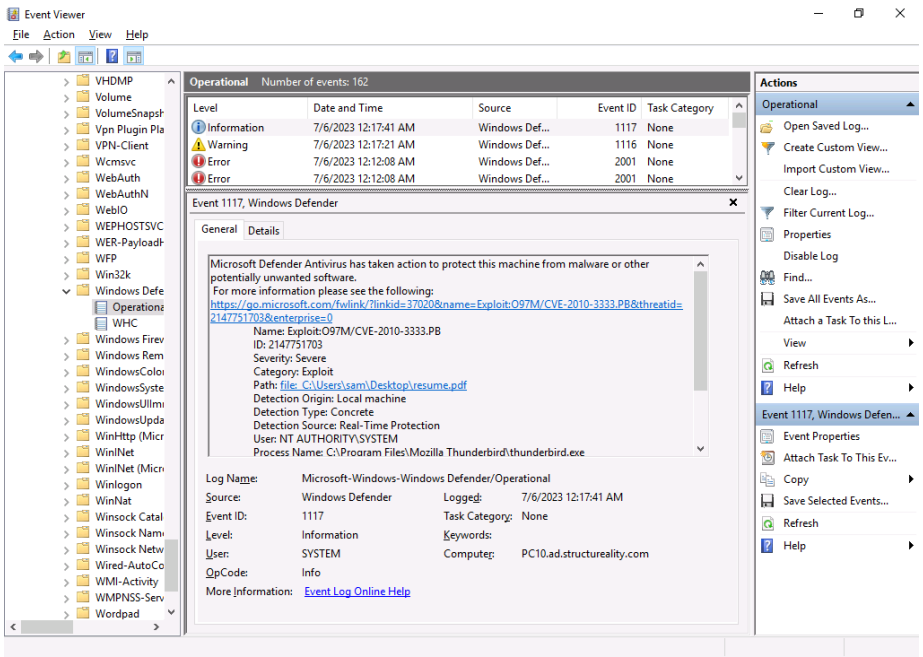
Host Operating System Logs

```
00:01:57 lamp sshd[453]: Server listening on 0.0.0.0 port 22.
00:01:57 lamp sshd[453]: Server listening on :: port 22.
00:17:01 lamp CRON[744]: pam_unix(cron:session): session opened for user root(uid=0) by (ui
00:17:01 lamp CRON[744]: pam_unix(cron:session): session closed for user root
00:26:47 lamp login[415]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0
00:26:51 lamp login[415]: FAILED LOGIN (1) on '/dev/ttyl' FOR 'root', Authentication failur
00:26:59 lamp login[415]: FAILED LOGIN (2) on '/dev/ttyl' FOR 'root', Authentication failur
00:27:05 lamp login[415]: FAILED LOGIN (3) on '/dev/ttyl' FOR 'root', Authentication failur
00:27:11 lamp login[415]: pam_unix(login:session): session opened for user lamp(uid=1000) b
00:27:11 lamp systemd-logind[396]: New session 3 of user lamp.
00:27:11 lamp systemd: pam_unix(systemd-user:session): session opened for user lamp(uid=100
00:29:26 lamp sudo:     lamp : TTY=ttyl ; PWD=/home/lamp ; USER=root ; COMMAND=/usr/bin/cat
00:29:26 lamp sudo: pam_unix(sudo:session): session opened for user root(uid=0) by lamp(uid
```

Linux authentication log showing SSH remote access is enabled, failed authentication attempts for root user, and successful login for lamp user.

- Security/audit logs
  - Authentication and authorization events
  - File system events
- Windows
  - Application, security, and system
- Linux
  - Syslog versus Journald
  - Common log files
- macOS unified logging

Application and Endpoint Logs



Windows Defender logging detection and quarantine of malware to Event Viewer. (Screenshot used with permission from Microsoft.)

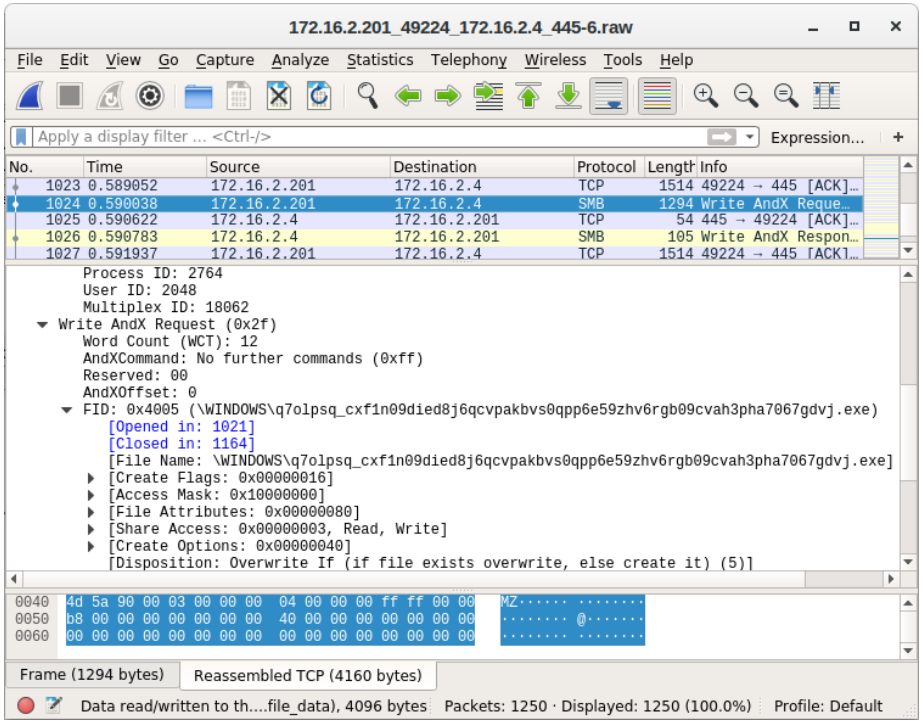
- Application logs
- Endpoint logs
  - Security software running on hosts
  - Summarize volume of detection incidents to indicate threat levels
  - Incident attribution and threat intelligence
- Vulnerability scans

Network Data Sources

- Network logs
  - Traffic and access data from network appliances
- Firewall logs
  - Correlate to malicious activity on hosts
- IPS/IDS logs
  - Summarize volume of detection incidents to indicate threat levels
  - Attribution and threat intelligence

Viewing the raw log message generated by a Suricata IDS alert in the Security Onion SIEM.

Packet Captures

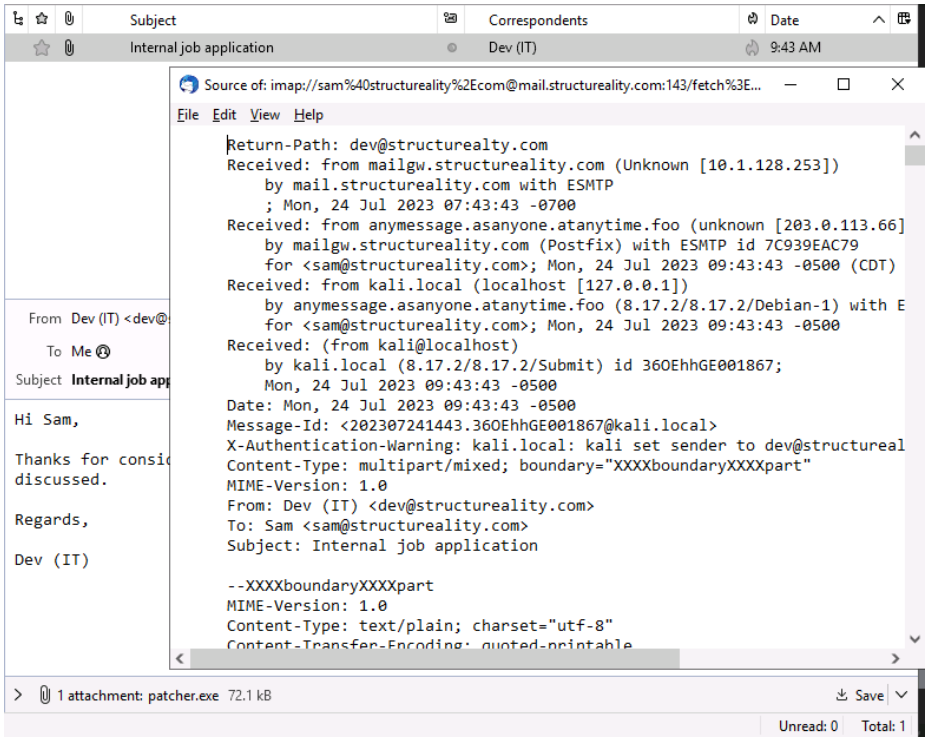


Using the Wireshark packet analyzer to identify malicious executables being transferred over the Windows file-sharing protocol. (Screenshot Wireshark wireshark.org.)

- Pivot from alert event to per-packet or frame analysis
- Extract binary data

Metadata

- File
  - Date/time and security attributes
  - Extended attributes and properties
- Web
  - Request and response headers
- Email
  - Internet header listing message transfer agents
  - Spam/security analysis



Analyzing headers in a phishing message: the sender is using typosquatting to hope the recipient confuses structureality.com with the genuine domain structureality.com.

(Screenshot courtesy of Mozilla)

Data Sources

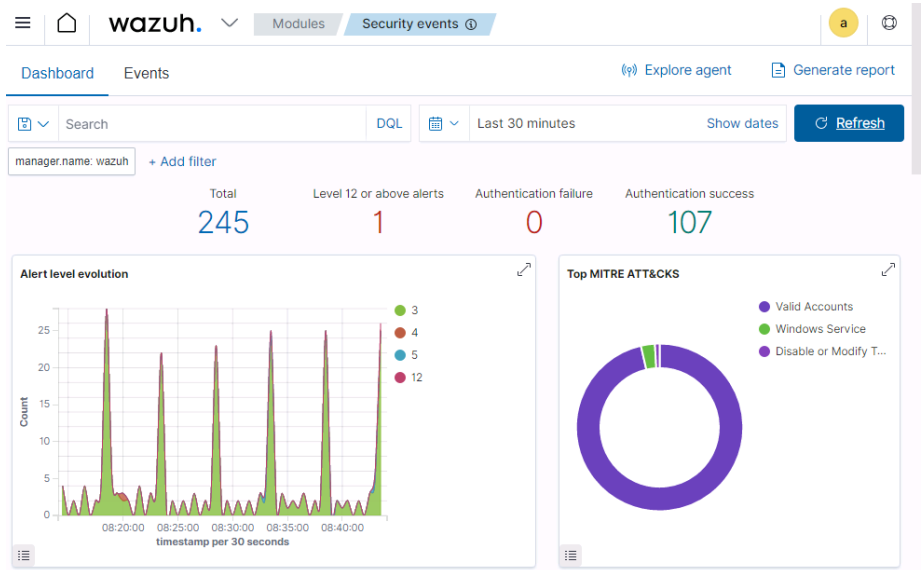
- Data sources, dashboards, and reports
- Log data
- Host operating system logs
- Application and endpoint logs
- Network data sources
  - Network appliance logs, firewall logs, IPS/IDS logs
- Packet captures
- Metadata

Lesson 12

Topic 12D

Alerting and Monitoring Tools

Security Information and Event Management



Wazuh SIEM dashboard—Configurable dashboards provide the high-level status view of network security metrics. (Screenshot used with permission from Wazuh Inc.)

- Log collection
  - Agent-based
    - Local agent to forward logs
  - Listener/collector
    - Protocol-based remote log forwarding (syslog)
  - Sensor
    - Packet capture and traffic flow data
- Log aggregation
  - Consolidation of multiple log formats to facilitate search/query and correlation
  - Normalization of fields
  - Time synchronization

Alerting and Monitoring Activities

- Alerting and correlation
  - Static rules and logical expressions
  - Threat intelligence feeds
  - Validation of alerts as true positives versus false positives
  - Quarantine for remediation
- Reporting
  - Executive, managerial, and compliance audiences
- Archiving
  - Preserve evidence of attack
  - Facilitate threat hunting and retrospective incident identification

Alert Tuning (1)

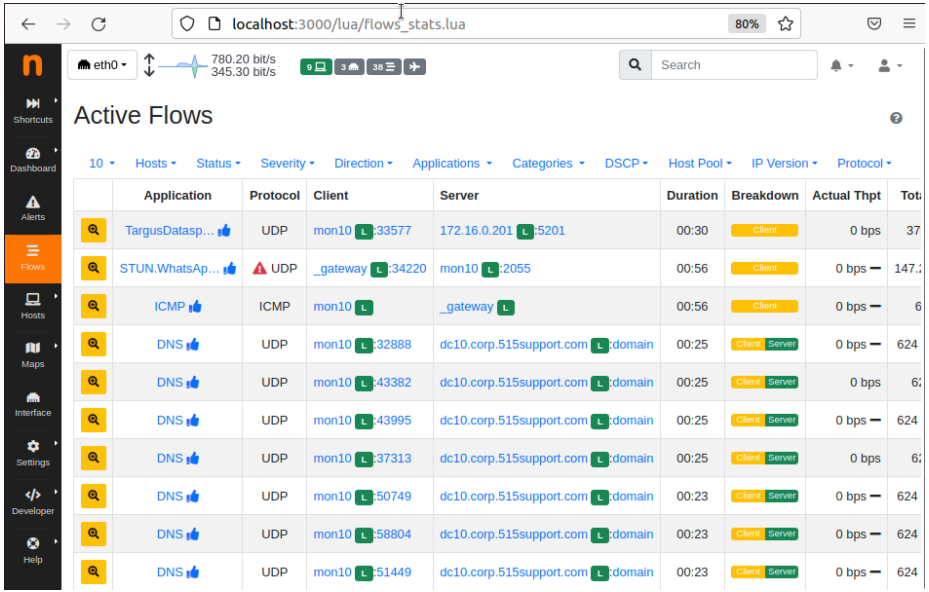
- Correlation action to log only, trigger alert, or trigger alarm
- Reduce false positives without increasing false negatives
  - False positives raise an alert when there is no actual malicious activity
  - False negatives do not raise an alert when there is malicious activity
  - True positives measure successful detection of incidents

Alert Tuning (2)

- Techniques for tuning
  - Refining detection rules and muting alert levels
  - Redirecting sudden alert “floods“
  - Redirecting infrastructure-related alerts
  - Continuous monitoring of alert volume and analyst feedback
  - Deploying machine learning (ML) analysis

Monitoring Infrastructure

- Network monitors
  - Appliance state data
  - Heartbeat availability monitoring
  - Simple Network Management Protocol (SNMP) traps
- Netflow/IPFIX
  - Records traffic statistics
  - Flows defined by endpoints and ports (keys)
  - Netflow exporters and collectors

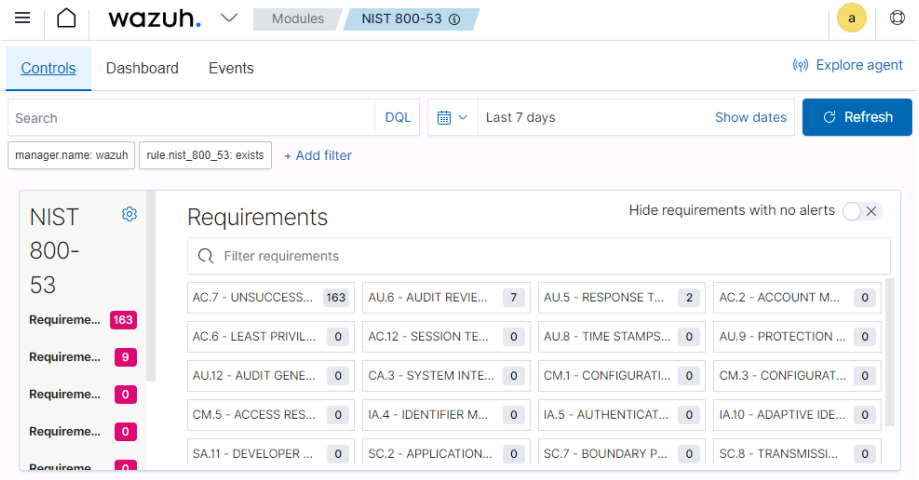


ntopng community edition being used to monitor NetFlow traffic data. (Screenshot used courtesy of ntop.)

Monitoring Systems and Applications

- System monitors and logs
  - System health reporting
  - System logs to diagnose availability issues
  - Security logs to audit access
- Application and cloud monitors
  - Application health monitoring
  - Cloud service health
- Vulnerability scanners
- Antivirus
- Data loss prevention (DLP)

Benchmarks



Monitoring template aligned to NIST 800-53 framework requirements.

- Scanning for configuration vulnerabilities
  - Lack of controls
  - Improper configuration
- Security content automation protocol (SCAP)
  - Language to enable scanners to load configuration benchmarks and scan for deviations

Alerting and Monitoring Tools

- Security Information and Event Management
  - Collection and aggregation
- Alerting and monitoring activities
  - Correlation, reporting, archiving
- Alert tuning
  - False positives, false negatives, alert fatigue
- Monitoring infrastructure
  - Network monitors, NetFlow
- Monitoring systems and applications
- Benchmarks
  - SCAP, OVAL, XCCDF configuration baseline scanning

Lesson 12

Summary