



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

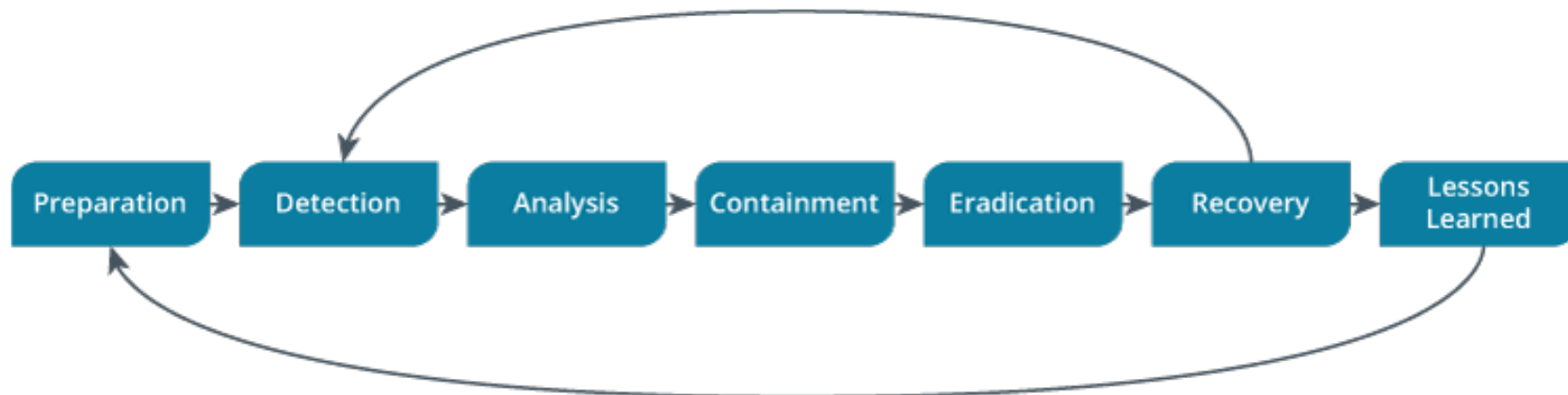
Lesson 12

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

The screenshot shows the Security Onion Alerts interface. At the top, it says "Security Onion" and "Alerts". There are "Options" and "Total Found: 30" indicators. A search bar is set to "Group By Name, Module". A "Fetch Limit" of 500 is shown. A clock icon is present with a tooltip: "Click the clock icon to change to absolute time". A context menu is open over the table, with options: "Include", "Exclude", "Only", "Drilldown", "Group By", "New Group By", "Clipboard", and "Actions". The "Drilldown" option is highlighted, and a tooltip says "Drilldown into this value".

Count	rule.name	event.module
1	New Windows Service Created	windows_eventlog
1	ET JA3 Hash - Possible Malware - Trickbot	suricata
2	Windows Defender: Antivirus real-time pro	windows_eventlog
2	Windows Defender: Antimalware scan was	windows_eventlog
8	ET MALWARE Possible Metasploit Payloa	PI (from server) suricata
8	ET HUNTING SUSPICIOUS SMTP EXE - EX	suricata

https://siem.ad.structureality.com/#/alerts?q=* | groupby rule.name event.module events...elds=rule.name&filterValue=ET JA3 Hash - Possible Malware - Trickbot&filterMode=DRILLDOWN

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



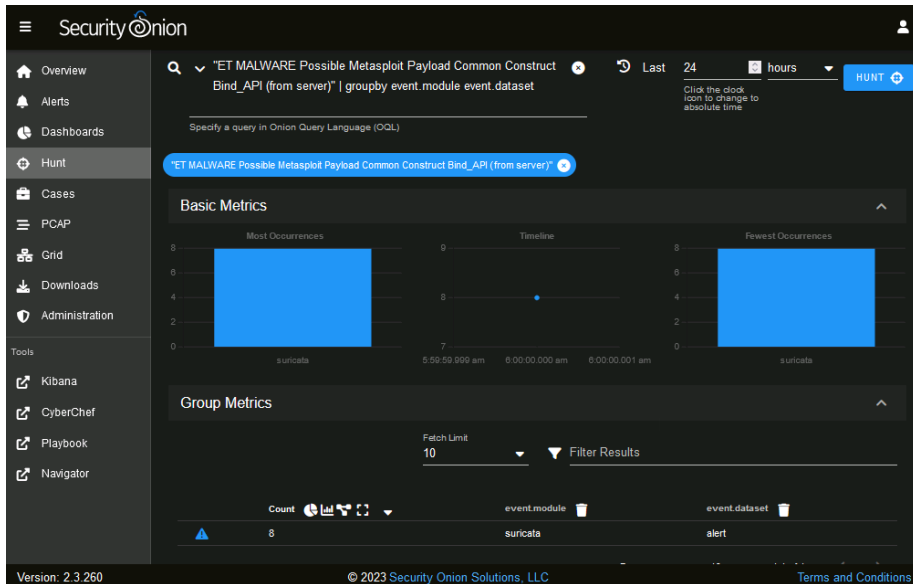
Members of the Kentucky and Alabama National Guard participate in a simulated network attack exercise.

(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

- 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



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.)

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=Win/SPIX64_23418 pslist
```

Volatility Foundation Volatility Framework 2.6	Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
	0xffffffff83020a7040	System	4	0	106	632	-----	0	2020-01-09 21:20:03	UTC+0000
	0xffffffff8303d6d1d0	smss.exe	308	4	2	29	-----	0	2020-01-09 21:20:03	UTC+0000
	0xffffffff83035f26a0	csrss.exe	396	388	8	370	0	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff83034fe060	wininit.exe	432	388	3	75	0	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff83036295e0	csrss.exe	444	424	8	293	1	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff8303716b30	winlogon.exe	492	424	3	109	1	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff83035fab30	services.exe	528	432	10	276	0	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff830373db30	lsass.exe	536	432	8	636	0	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff830373db30	lsass.exe	544	432	10	142	0	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff83037436a0	svchost.exe	652	528	10	349	0	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff83037e66a0	svchost.exe	716	528	7	235	0	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff83036566a0	svchost.exe	772	528	18	445	0	0	2020-01-09 21:20:05	UTC+0000
	0xffffffff83038bb060	svchost.exe	892	528	18	417	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff83038fcb30	svchost.exe	936	528	32	940	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff830393c060	svchost.exe	324	528	17	385	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff8303960060	svchost.exe	744	528	15	379	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff83039b7060	spoolsv.exe	1060	528	12	271	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff83039dd060	svchost.exe	1096	528	19	316	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff8303a58960	vmicsvc.exe	1192	528	5	126	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff8303a70b30	vmicsvc.exe	1216	528	7	217	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff8303a8c060	vmicsvc.exe	1264	528	4	78	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff8303accb30	vmicsvc.exe	1296	528	5	92	0	0	2020-01-09 21:20:06	UTC+0000
	0xffffffff8303b32920	vmicsvc.exe	1340	528	3	82	0	0	2020-01-09 21:20:07	UTC+0000
	0xffffffff8302ab3210	svchost.exe	1436	528	10	179	0	0	2020-01-09 21:20:07	UTC+0000
	0xffffffff8303bcf800	svchost.exe	1528	528	3	43	0	0	2020-01-09 21:20:08	UTC+0000
	0xffffffff8303c963a0	svchost.exe	1816	528	5	99	0	0	2020-01-09 21:20:08	UTC+0000
	0xffffffff8303ac5b30	svchost.exe	1976	528	14	323	0	0	2020-01-09 21:20:10	UTC+0000
	0xffffffff8303155b30	taskhost.exe	1964	528	9	157	1	0	2020-01-09 21:20:14	UTC+0000
	0xffffffff83031c3830	sppsvc.exe	2072	528	7	158	0	0	2020-01-09 21:20:14	UTC+0000
	0xffffffff8303262060	dwm.exe	2352	892	3	70	1	0	2020-01-09 21:20:18	UTC+0000
	0xffffffff8303238060	explorer.exe	2376	2344	24	784	1	0	2020-01-09 21:20:18	UTC+0000
	0xffffffff83033a2b30	jusched.exe	2520	2456	8	233	1	1	2020-01-09 21:20:18	UTC+0000
	0xffffffff8303ba0b30	SearchIndexer.exe	2568	528	11	656	0	0	2020-01-09 21:20:24	UTC+0000
	0xffffffff830326a060	procexp64.exe	2900	2376	8	382	1	0	2020-01-09 21:20:45	UTC+0000
	0xffffffff83036406a0	WmiPrvSE.exe	3024	652	7	118	0	0	2020-01-09 21:20:51	UTC+0000
	0xffffffff8303703190	Tcpview.exe	916	2376	6	139	1	1	2020-01-09 21:21:27	UTC+0000
	0xffffffff8302839b30	salter.exe	1808	2376	6	134	1	1	2020-01-09 21:23:49	UTC+0000
	0xffffffff8303818230	WMIADAP.exe	380	936	5	85	0	0	2020-01-09 21:24:08	UTC+0000

Screenshot: Volatility Framework volatilityfoundation.org

Disk Image Acquisition

- 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

```
root@kali:~# dcfldd if=/dev/sda hash=sha256 of=/root/FORENSIC/ROGUE.dd bs=512 co
nv=noerror
134217728 blocks (65536Mb) written.Total (sha256): 7a72be231f393d40e0ac72c62b3a7
3798f29f0ca7e0e279b8aececa291a34137

134217728+0 records in
134217728+0 records out
root@kali:~# sha256sum /dev/sda
7a72be231f393d40e0ac72c62b3a73798f29f0ca7e0e279b8aececa291a34137 /dev/sda
root@kali:~# █
```

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

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

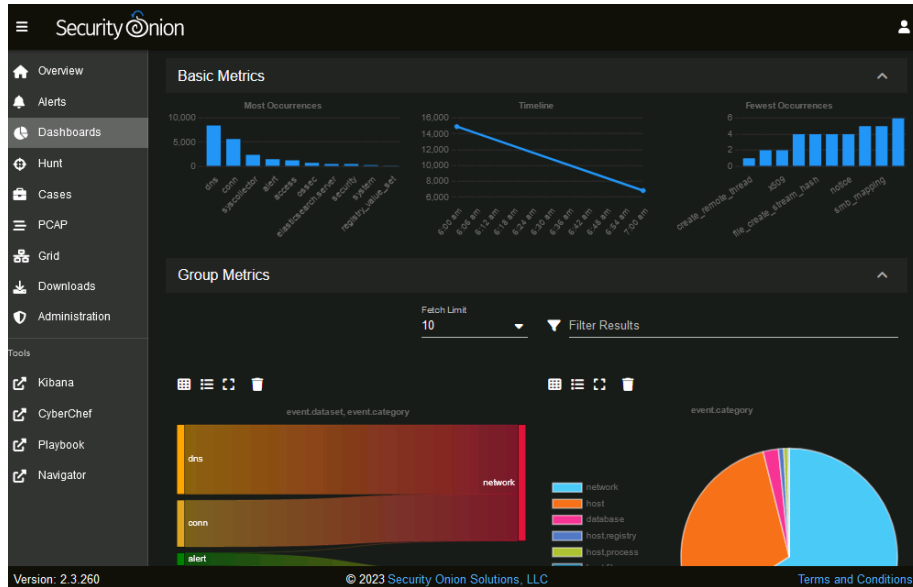


Data Sources, Dashboards, and Reports (1)

- 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)

- 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



Screenshot courtesy of Security Onion (securityonion.net.)

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 LX1 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 LX1 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

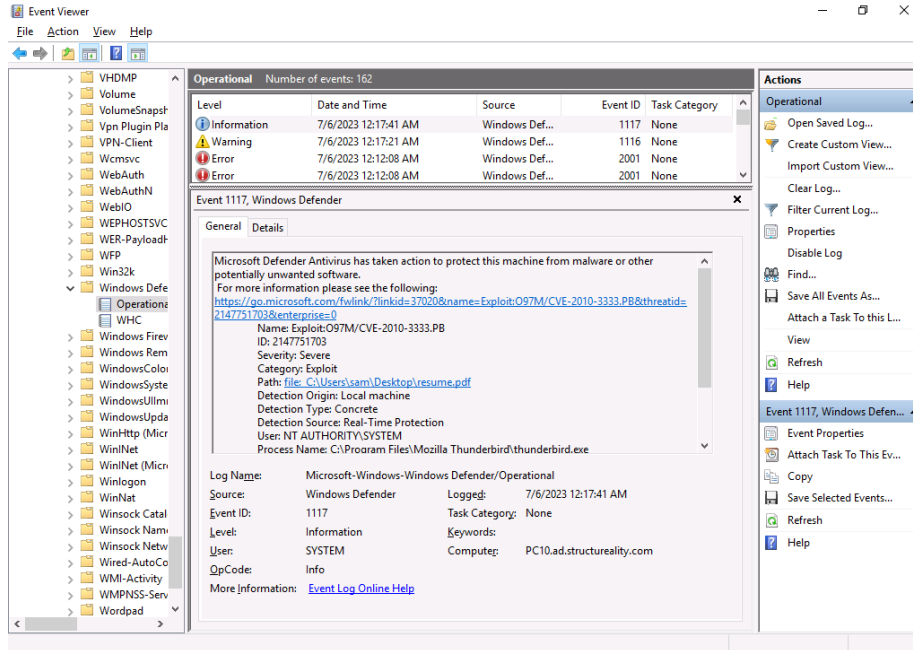
```
00:01:57 lamp sshd[453]: Server listening on 0.0.0.0 port 22.
00:01:57 lamp sshd[453]: Server listening on :: port 22.
00:17:01 lamp CRON[744]: pam_unix(cron:session): session opened for user root(uid=0) by (ui
00:17:01 lamp CRON[744]: pam_unix(cron:session): session closed for user root
00:26:47 lamp login[415]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0
00:26:51 lamp login[415]: FAILED LOGIN (1) on '/dev/tty1' FOR 'root', Authentication failur
00:26:59 lamp login[415]: FAILED LOGIN (2) on '/dev/tty1' FOR 'root', Authentication failur
00:27:05 lamp login[415]: FAILED LOGIN (3) on '/dev/tty1' 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=tty1 ; 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

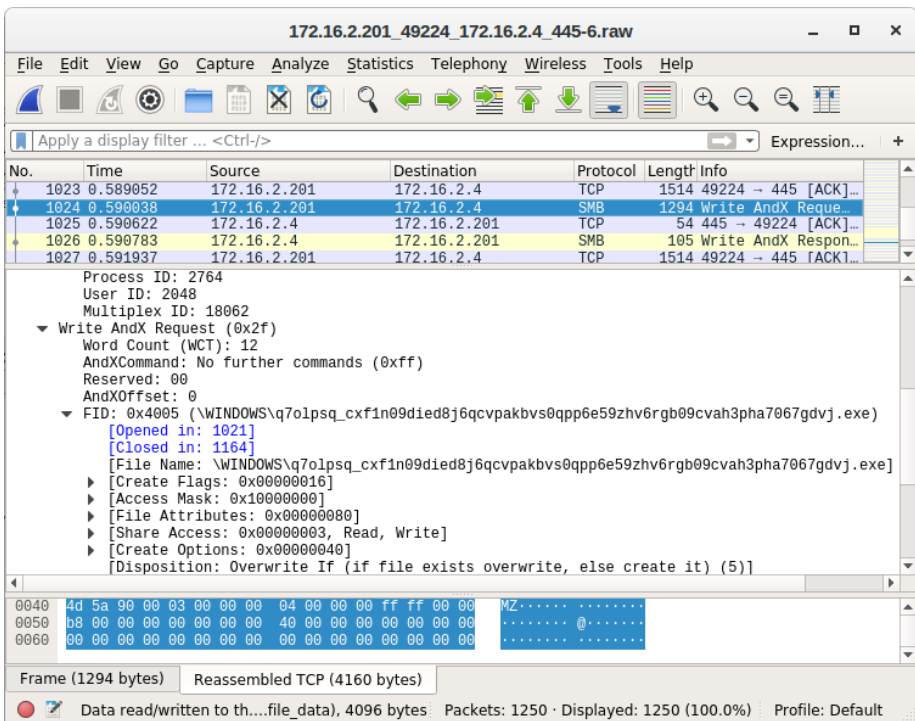
- Application logs
- Endpoint logs
 - Security software running on hosts
 - Summarize volume of detection incidents to indicate threat levels
 - Incident attribution and threat intelligence
- Vulnerability scans



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

Packet Captures

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



The screenshot shows the Wireshark interface with a packet capture of a file transfer. The packet list pane shows several packets, with packet 1024 selected. The packet details pane shows the structure of the selected packet, including a Write AndX Request and a File ID. The packet bytes pane shows the raw data of the selected packet, which is a file named \WINDOWS\q7olpsq_cxf1n09died8j6qcvpakbvs0qpp6e59zhv6rgb09cvah3pha7067gdvj.exe.

No.	Time	Source	Destination	Protocol	Length	Info
1023	0.589052	172.16.2.201	172.16.2.4	TCP	1514	49224 → 445 [ACK]...
1024	0.590038	172.16.2.201	172.16.2.4	SMB	1294	Write AndX Reque...
1025	0.590622	172.16.2.4	172.16.2.201	TCP	54	445 → 49224 [ACK]...
1026	0.590783	172.16.2.4	172.16.2.201	SMB	105	Write AndX Respon...
1027	0.591937	172.16.2.201	172.16.2.4	TCP	1514	49224 → 445 [ACK]...

Process ID: 2764
User ID: 2048
Multiplex ID: 18062
▼ Write AndX Request (0x2f)
Word Count (WCT): 12
AndXCommand: No further commands (0xff)
Reserved: 00
AndXOffset: 0
▼ FID: 0x4005 (\WINDOWS\q7olpsq_cxf1n09died8j6qcvpakbvs0qpp6e59zhv6rgb09cvah3pha7067gdvj.exe)
[Opened in: 1021]
[Closed in: 1164]
[File Name: \WINDOWS\q7olpsq_cxf1n09died8j6qcvpakbvs0qpp6e59zhv6rgb09cvah3pha7067gdvj.exe]
▶ [Create Flags: 0x00000016]
▶ [Access Mask: 0x10000000]
▶ [File Attributes: 0x00000080]
▶ [Share Access: 0x00000003, Read, Write]
▶ [Create Options: 0x00000040]
[Disposition: Overwrite If (if file exists overwrite, else create it) (5)]

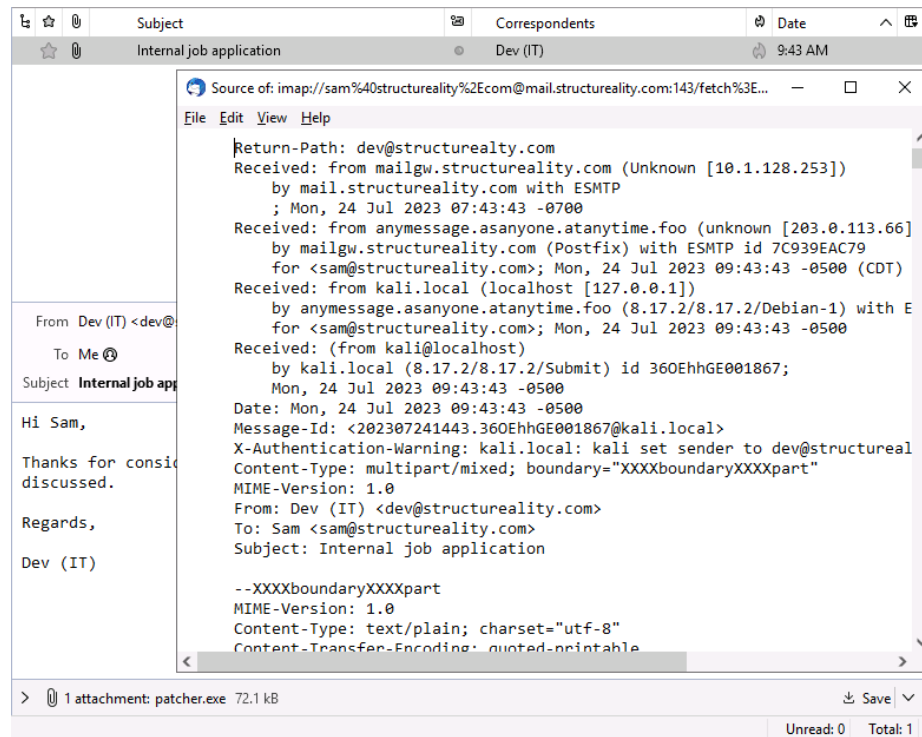
0040 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
0050 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00@.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00@.....

Frame (1294 bytes) Reassembled TCP (4160 bytes)
Data read/written to th...file_data, 4096 bytes Packets: 1250 · Displayed: 1250 (100.0%) Profile: Default

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

Metadata

- File
 - Date/time and security attributes
 - Extended attributes and properties
- Web
- Email
 - 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

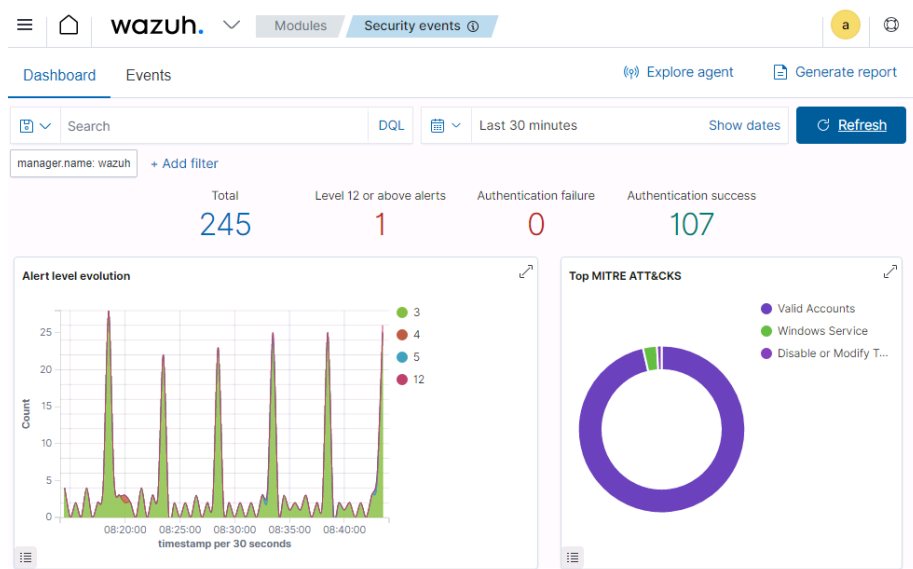
Lesson 12

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)

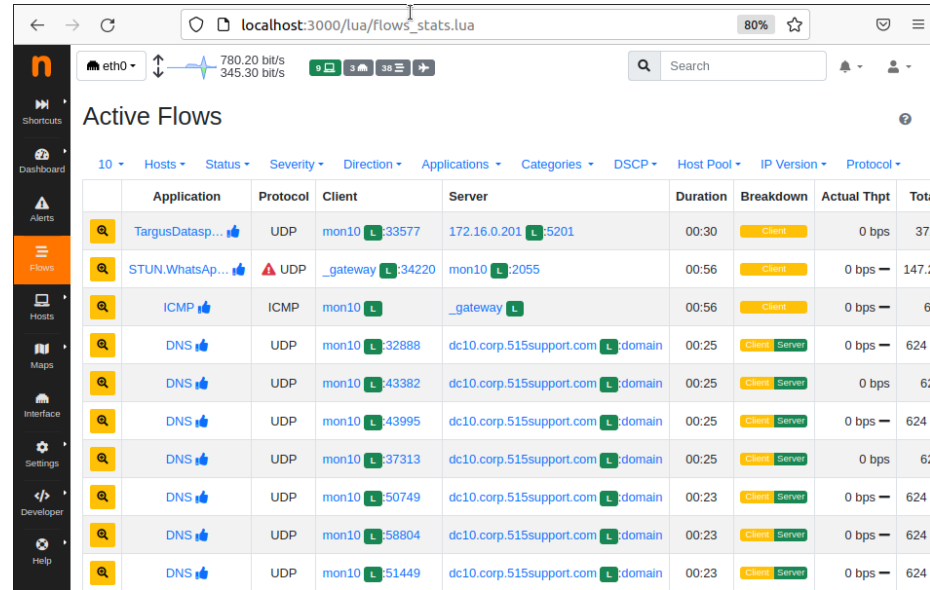
- Correlation action to log only, trigger alert, or trigger alarm
- Reduce false positives without increasing false negatives
 - False positives raise an alert when there is no actual malicious activity
 - False negatives do not raise an alert when there is malicious activity
 - True positives measure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



The screenshot shows the ntopng web interface displaying active network flows. The browser address bar shows 'localhost:3000/lua/flows_stats.lua'. The interface includes a sidebar with navigation options like Shortcuts, Dashboard, Alerts, Flows, Hosts, Maps, Interface, Settings, Developer, and Help. The main content area is titled 'Active Flows' and features a table with columns for Application, Protocol, Client, Server, Duration, Breakdown, Actual Thpt, and Tot. The table lists various traffic flows, including TargusDataSp..., STUN.WhatsAp..., ICMP, and multiple DNS entries.

	Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Tot
	TargusDataSp...	UDP	mon10 L:33577	172.16.0.201 L:5201	00:30	Client	0 bps	37
	STUN.WhatsAp...	UDP	_gateway L:34220	mon10 L:2055	00:56	Client	0 bps	147.7
	ICMP	ICMP	mon10 L	_gateway L	00:56	Client	0 bps	6
	DNS	UDP	mon10 L:32888	dc10.corp.515support.com L:domain	00:25	Client Server	0 bps	624
	DNS	UDP	mon10 L:43382	dc10.corp.515support.com L:domain	00:25	Client Server	0 bps	6;
	DNS	UDP	mon10 L:43995	dc10.corp.515support.com L:domain	00:25	Client Server	0 bps	624
	DNS	UDP	mon10 L:37313	dc10.corp.515support.com L:domain	00:25	Client Server	0 bps	6;
	DNS	UDP	mon10 L:50749	dc10.corp.515support.com L:domain	00:23	Client Server	0 bps	624
	DNS	UDP	mon10 L:58804	dc10.corp.515support.com L:domain	00:23	Client Server	0 bps	624
	DNS	UDP	mon10 L:51449	dc10.corp.515support.com L:domain	00:23	Client Server	0 bps	624

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

The screenshot shows the Wazuh dashboard interface. At the top, the 'wazuh.' logo is visible, along with navigation tabs for 'Controls', 'Dashboard', and 'Events'. A search bar is present with filters for 'manager.name: wazuh' and 'rule.nist_800_53: exists'. The main content area displays a 'Requirements' table for the NIST 800-53 framework. The table lists various requirements with their corresponding alert counts. A sidebar on the left shows the 'NIST 800-53' category with a total of 183 requirements.

Requirement ID	Alert Count
AC.7 - UNSUCCESS...	163
AU.6 - AUDIT REVIE...	7
AU.5 - RESPONSE T...	2
AC.2 - ACCOUNT M...	0
AC.6 - LEAST PRIVIL...	0
AC.12 - SESSION TE...	0
AU.8 - TIME STAMPS...	0
AU.9 - PROTECTION ...	0
AU.12 - AUDIT GENE...	0
CA.3 - SYSTEM INTE...	0
CM.1 - CONFIGURATI...	0
CM.3 - CONFIGURAT...	0
CM.5 - ACCESS RES...	0
IA.4 - IDENTIFIER M...	0
IA.5 - AUTHENTICAT...	0
IA.10 - ADAPTIVE IDE...	0
SA.11 - DEVELOPER ...	0
SC.2 - APPLICATION...	0
SC.7 - BOUNDARY P...	0
SC.8 - TRANSMISSI...	0

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

CompTIA Security+ Exam SY0-701

Lesson 12



Summary

