Day#4

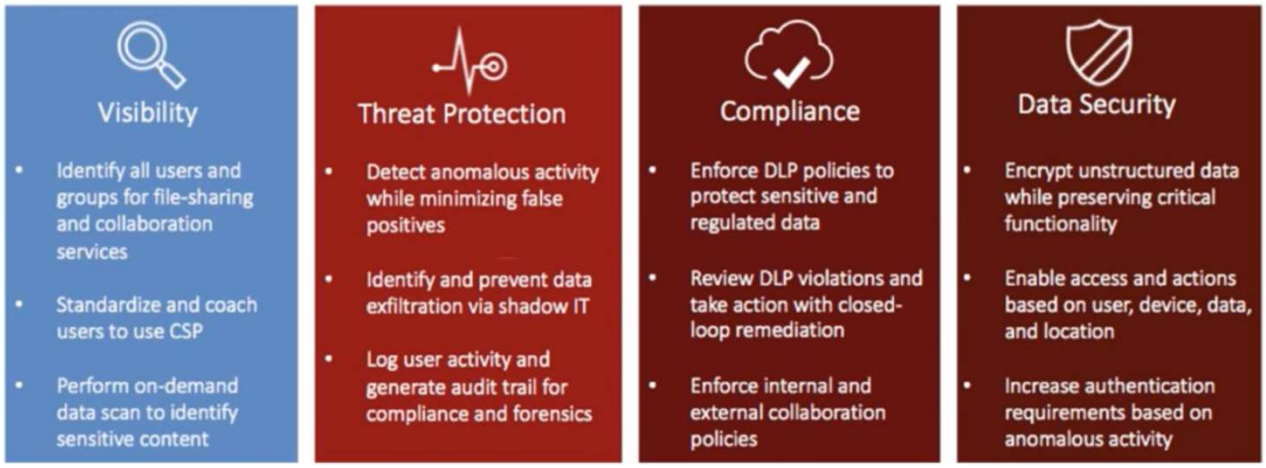
Operations and Incident Response

Syllabus Objectives Covered

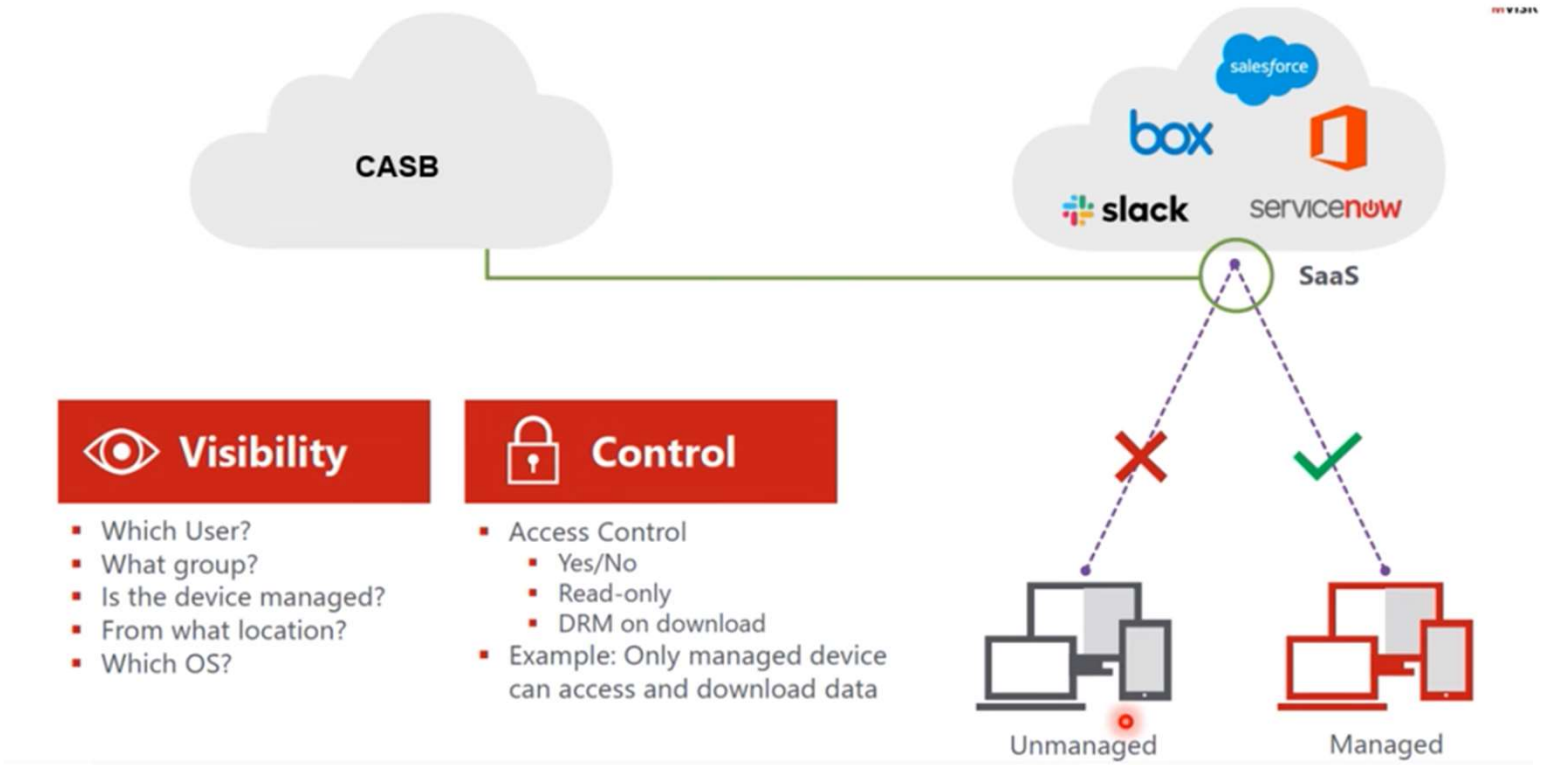
- 4.1 Given a scenario, use the appropriate tool to assess organizational security
- 4.2 Summarize the importance of policies, processes, and procedures for incident response
- 4.3 Given an incident, utilize appropriate data sources to support an investigation
- 4.4 Given an incident, apply mitigation techniques or controls to secure an environment
- 4.5 Explain the key aspects of digital forensics

Cloud Access Security Brokers (CASB)

Gartner defines the cloud access security broker (CASB) market as products and service that ***address security gaps in an organization's use of cloud services***, primarily for software as a service (SaaS) applications. This technology is the result of the need to provide access to cloud services from users inside and outside the traditional enterprise perimeter, to control cloud-to-cloud plus connected app access, and to secure data stored in cloud services.

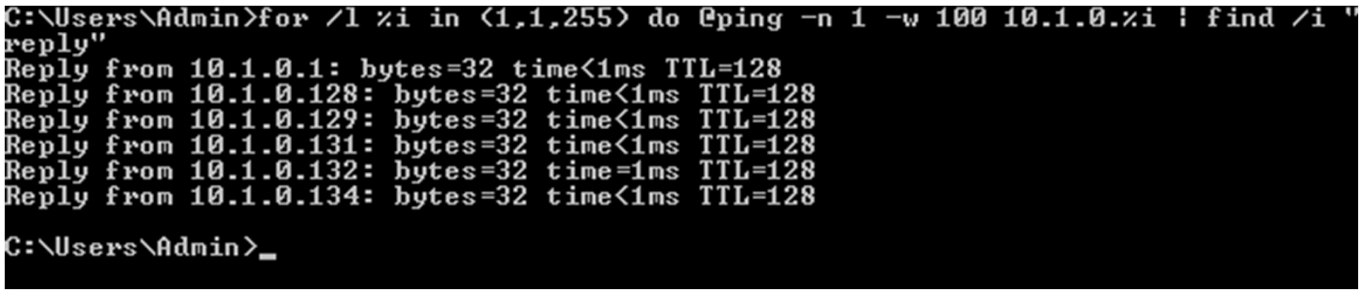


Cloud Access Security Brokers (CASB)



ipconfig, ping, and arp

- Footprinting the network layout and rogue system detection
- `ipconfig/ifconfig/ip`
  - Report the local IP configuration
- `ping`
  - Test connectivity with a host
  - Use a ping sweep to detect live hosts on a subnet
- `arp`
  - Address Resolution Protocol (ARP) cache
  - Shows IP to Media Access Control (MAC) address mapping
  - Detect spoofing (validate MAC of default gateway)



Screenshot used with permission from Microsoft.

route and traceroute

- `route`
  - Show the local routing table
  - Identify default route and local subnet
  - Check for suspicious entries
- `tracert/traceroute`
  - Test the path to a remote host
- `pathping/mtr`
  - Measure latency

```
[centos@lx1 ~]$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.1.0.254      0.0.0.0         UG    100    0        0 eth0
10.1.0.0        0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

IP Scanners and Nmap

- Host discovery
  - Test whether host in IP range responds to probes
- Port scan
  - Test whether TCP or UDP port allows connections

```
C:\Program Files (x86)\Nmap>nmap 10.1.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-06 10:13 Pacific Standard Time
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.00s latency).
Not shown: 986 filtered ports
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
443/tcp  open  https
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:01:CA:AB (Microsoft)
```

Screenshot used with permission from nmap.org.

Service Discovery and Nmap

- Service discovery
  - Scan custom TCP/UDP port ranges
- Service and version detection
  - Fingerprinting each port
  - Protocol
  - Application/version
  - OS type
  - Device type

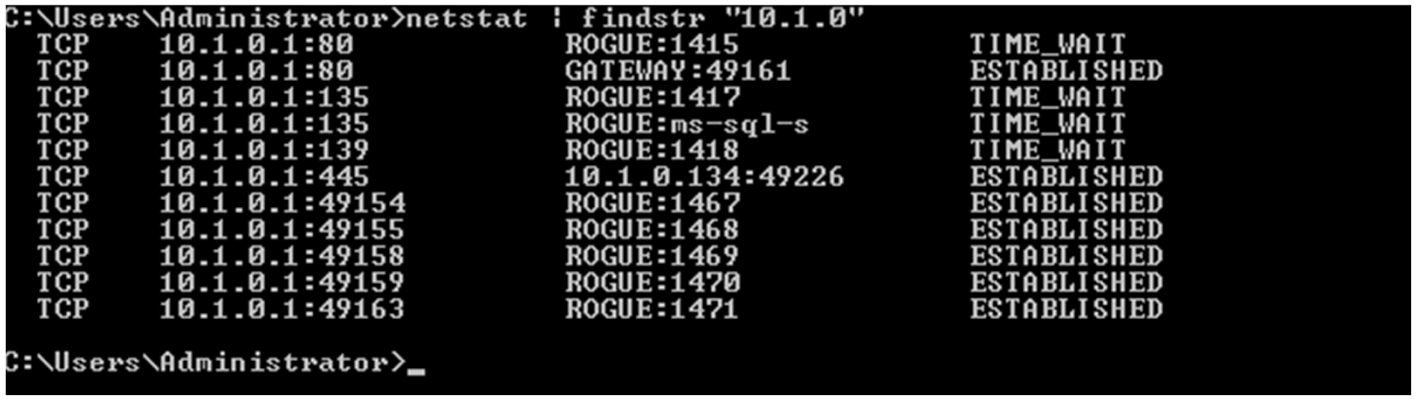
```
C:\Program Files (x86)\Nmap>nmap 10.1.0.1 -A
Starting Nmap 7.70 ( https://nmap.org ) at 2020-01-06 10:41 Pacific Standard Time
Nmap scan report for DC1.corp.515support.com (10.1.0.1)
Host is up (0.000083s latency).
Not shown: 986 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
...
1 service unrecognized despite returning data. If you know the service/version, please sul
SF-Port53-TCP:V=7.70%I=7%D=1/6%Time=5E137F54%P=i686-pc-windows-windows%r(D
SF:NSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07versi
SF:on\x04bind\0\0\x10\0\x03");
MAC Address: 00:15:5D:01:CA:AB (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|2012 (98%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2012:r2
Aggressive OS guesses: Microsoft Windows Server 2016 (98%), Microsoft Windows Server 2012
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: DC1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Screenshot used with permission from nmap.org.

netstat and nslookup

- `netstat`
  - Report port status on local machine
  - Switches to filter by protocol
  - Display process name or PID that opened port
- `nslookup` and `dig`
  - Query name servers
  - Zone transfers

Screenshot used with permission from Microsoft.

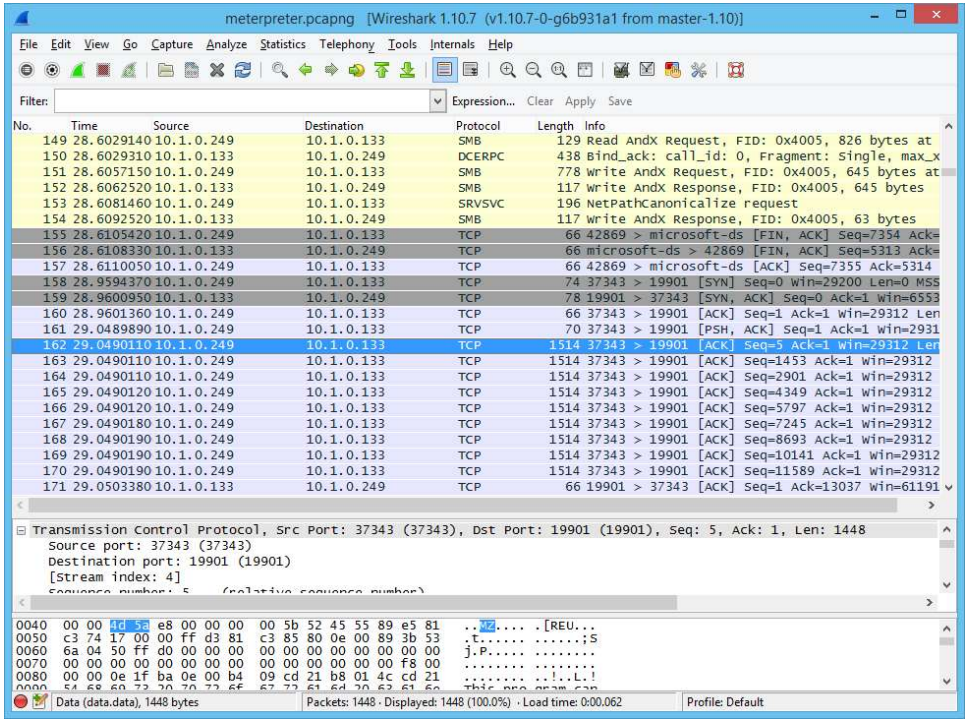


Packet Capture and tcpdump

- Packet analysis versus protocol analysis
- Sniffer—tool for capturing network frames
  - Use software to interact with host network driver (libpcap/winpcap)
  - Mirrored ports/switched port analyzer (SPAN)
  - Use a test access port (TAP) device to read frames from network media
  - Placement of sensors
- tcpdump
  - Write to pcap
  - Read from pcap
  - Filters

```
tcpdump -i eth0 "src host 10.1.0.100 and
(dst port 53 or dst port 80)"
```

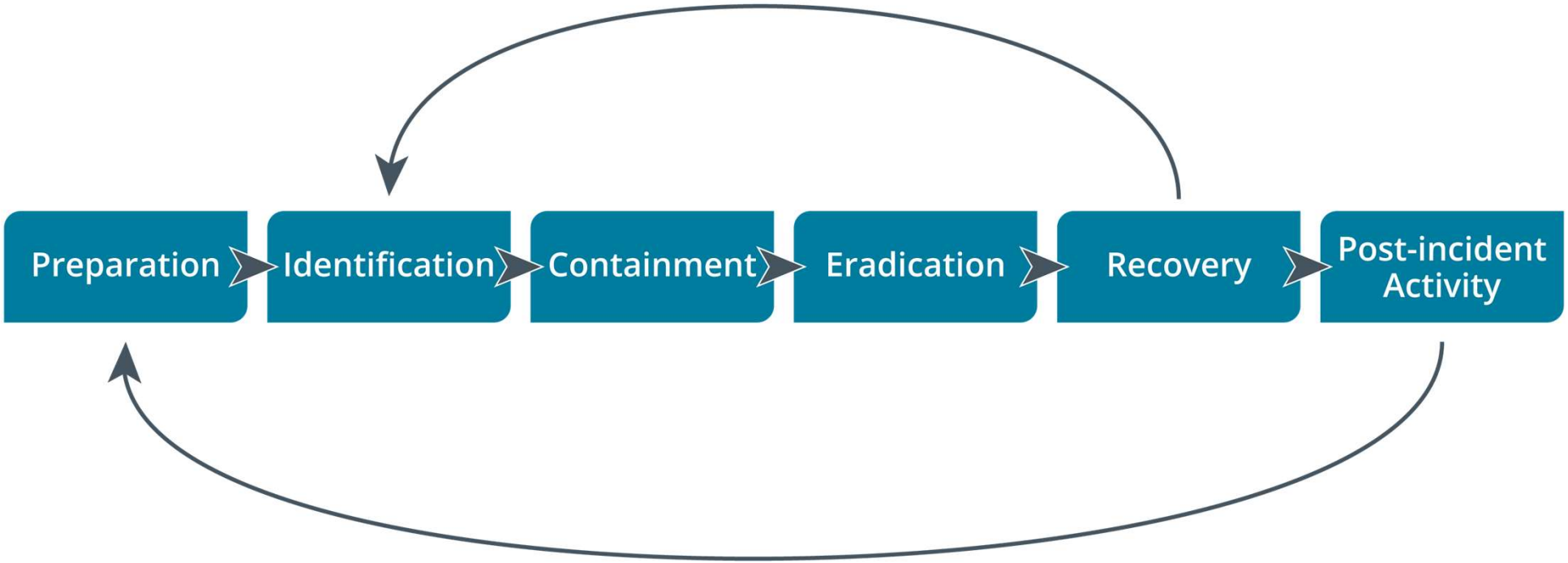
Packet Analysis and Wireshark



Screenshot used with permission from wireshark.org.

- Output panes
  - Packet list
  - Packet details (headers and fields)
  - Packet bytes (hex and ASCII)
- Capture and display filters
- Coloring rules
- Follow TCP Stream

Incident Response Process



Cyber Incident Response Team

- Reporting, categorizing, and prioritizing (triage)
- CIRT/CERT/CSIRT/SOC
- Management/decision-making authority
- Incident analysts
- 24/7 availability
- Roles beyond technical response
  - Legal
  - Human Resources (HR)
  - Marketing

Image credit: John Mattern/Feature Photo Service for IBM.

Incident Response Plan

- Lists the procedures, contacts, and resources available to responders for various incident categories
- Playbooks and runbooks
- Incident categorization
- Prioritization factors
  - Data integrity
  - Downtime
  - Economic/publicity
  - Scope
  - Detection time
  - Recovery time

Cyber Kill Chain Attack Framework

Incident Response Exercises

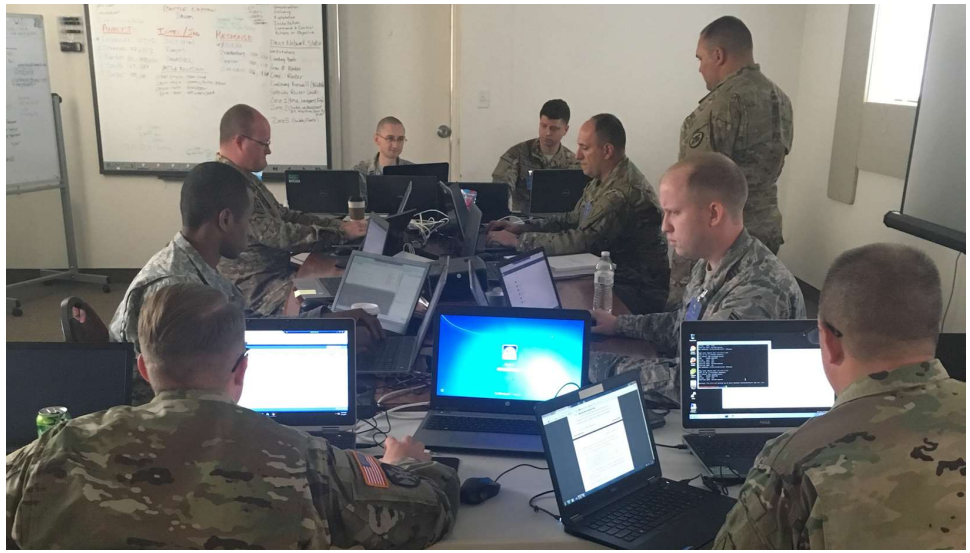
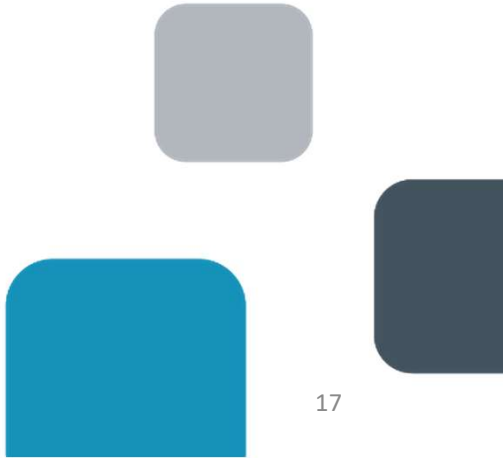


Image © 2017 Kentucky National Guard.

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

Incident Response, Disaster Recovery, and Retention Policy

- Incident response versus disaster recovery and business continuity
  - Disaster recovery plan
    - Response and recovery planning for major incidents
  - Business continuity plan
    - Making business procedures resilient
  - Continuity of operation planning (COOP)
- Incident response, forensics, and retention policy
  - Digital forensics requirements
  - Retention policies for evidence preservation



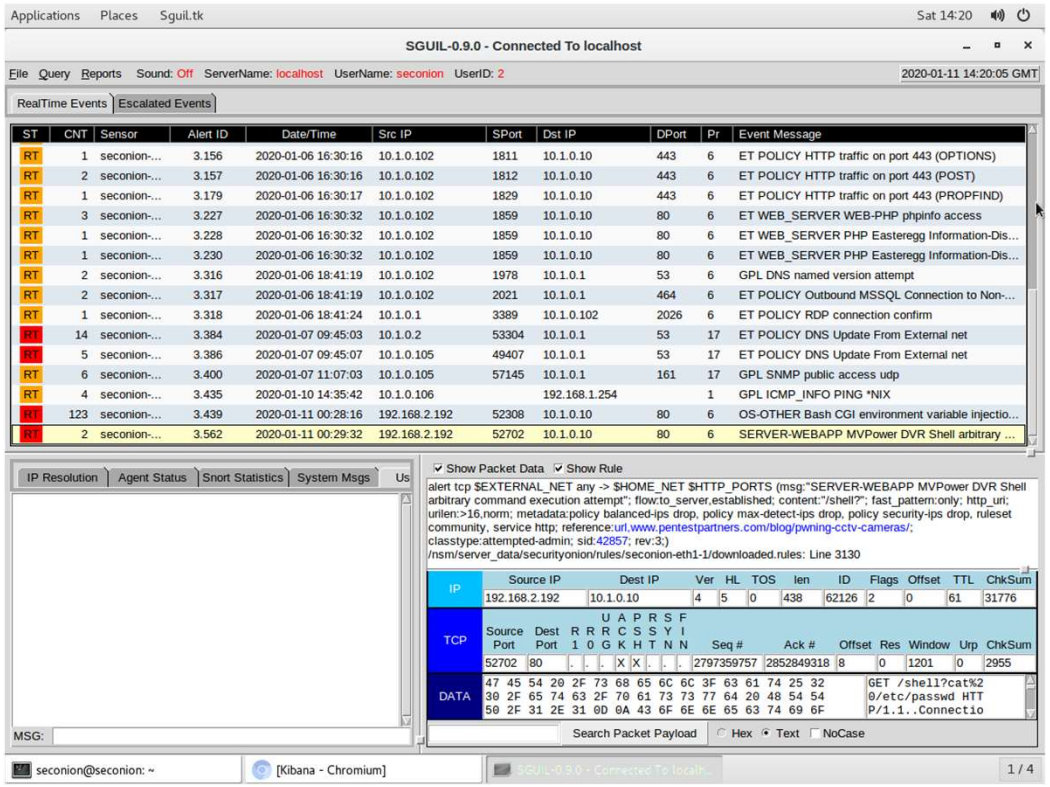
Incident Identification

- Precursors and detection channels
  - Security mechanisms (IDS, log analysis, alerts)
  - Manual inspections
  - Notification procedures
  - Public reporting
  - Confidential reporting/whistleblowing
- First responder
  - Member of CIRT taking charge of a reported incident
- Analysis and incident identification
  - Classify and prioritize → [illegible] take action

Security and Information Event Management

- Correlation
  - Static rules and logical expressions
  - Threat intelligence feeds
  - AI-assisted analysis
- Retention
  - Preserve evidence of attack
  - Facilitate threat hunting and retrospective incident identification

SIEM Dashboards

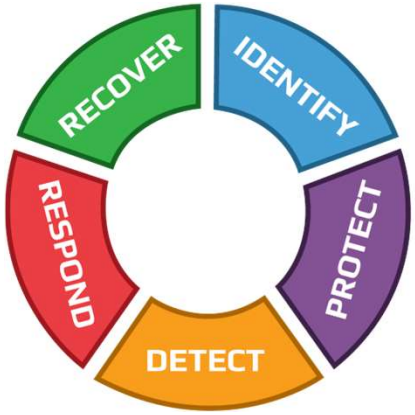


Screenshot courtesy of Security Onion (securityonion.net.)

- Analyst dashboard
  - Console of alerts that require prioritization and investigation
- Manager dashboard
  - Overall status indicators
- Sensitivity and alerts
  - Log only/alert/alarm
- Sensors
  - Source for network traffic data
  - Aggregate data under one dashboard
  - Per-sensor dashboards

Best Practice NIST CSF for dealing with threats .

Function	Objective
Identify	Develop the organisational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Protect	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.



The NIST Cybersecurity Framework

Function	Category	How to	Information
Idetify	Asset Management	- Asset & Inventory information of device or server or IP register including in charge person and installation location - Contact information of in charge person involved including to support MA information	- Asset Information - Contact Information
	Business Environment	- Identify critical systems and develop management plans such as backups. and plans for recovery - Communication plan	- BCP Plan
	Governance	- Develop Information Security Policy - Define duties and responsibilities related to Cyber Security	- IS Policy
	Risk Assessment	- Risk Assessment (Internal / External) - Risk response and prioritized	
	Risk Management Strategy	- Risk Management process - Organizational risk tolerance	
	Supply Chain Risk Management	- Response and recovery planning and testing are conducted with suppliers and third-party providers	- Plan BCP or IR

Function	Category	How to	Information
Protect	Identity Management and Access Control	- Having access control system that comply according to the IS Policy such as AD. - Define Access Control Policy on devices	- AD for Authentication - IS Policy
	Awareness and Training	- IT Staff & Operation Team - Non-IT Staff	
	Data Security	- Data Classification / Protect Data in transit / Against Data loss - Capacity planning / Availability / Integrity Check - Separate environment (Production / POC)	- ISO define topic Data Classification, Data in transit but do not have Data loss - Capacity Planning
	Information Protection Processes and Procedures	- Baseline & Security baseline, Life cycle on device or Product - Process (Incident and IRP, Change, Backup/Restore) - Personal screening	- Security Baseline
	Maintenance	- MA / PM Schedule, Backup/Restore/Failover Testing	- Backup/Restore/Failover testing
	Protective Technology	- Implement High Availability Technology (Load balance, …) - Review configuration / log and optimization	

Function	Category	How to	Information
Detect	Anomalies and Events	- Define Baseline to Monitor Ex. Utilization, threshold (CPU, Memory, Disk) - The monitoring point must be appropriate in order to be able to detect abnormal events such as attacks - Can tell the effect to determine the severity of the problem	- Define Baseline to Monitoring - Review the monitoring point because when there is a problem, it is often difficult to find out or take a long time.
	Security Continuous Monitoring	- Security-related monitoring , such as virus infections, abnormal behavior monitoring. - Vulnerability check and penetration testing for risk.	- Vulnerability Check and Penetration test .
	Detection Processes	- Define a process when detecting an abnormal situation. - Rehearse when something goes wrong, such as checking Threshold settings, checking Escalate.	- Event Management - Escalation Process

Function	Category	How to	Information
Response	Response Planning	- Define duties and responsibility (both Internal & External) in case incident occurs. - Develop Incident Respond plan for handle incident case.	
	Communications	- Define concerned in charge person involved and communicate as required that aligned with secret level (Communication plan) - Make Template of Incident report.	
	Analysis	- When an incident occurs, there must be information that can be analyzed for the problem. (Must install the sensors point or monitor method appropriately) - Investigate and find Root cause to prevent problem re-occurs	
	Mitigation	- Having a backup plan or design that will reduce the fragmentation of the problem	
	Improvements	- Check for points that can be improved, can be rehearsal before the event occurs and find a point to improve .	

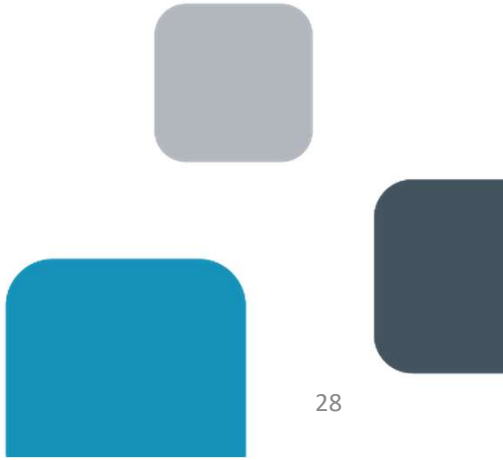
Function	Category	How to	Information
Recover	Recovery Planning	- Restoration plan Ex. Manual/Operation Step - During Recovery data , must not destroy information that will be evidence. (find a solution to prevent data lost first)	- Backup / Restore - Manual/ Operation step when start and shutdown system
	Improvements	- Figure out the points to improve for a quick and complete system recovery.	
	Communications	- Both communication Internal and External when system recovery	- Must not destroy information that will be evidence.

Trend Analysis

- Detecting indicators over a time series
- Prediction of future events
- Visualization
- Frequency-based
  - Number of events per period
- Volume-based
  - Increasing or decreasing size
- Statistical deviation
  - Identify anomalous data points

Network, OS, and Security Log Files

- System and security logs
  - Application
  - Security/audit
  - System
  - Setup
  - Forwarded events
- Network logs
  - Traffic and access data from network appliances
- Authentication logs
  - Security log or RADIUS/TACACS+ application logs
- Vulnerability scan output



Application Log Files

- DNS event logs
  - Types of queries made by clients
  - Hosts using suspicious IP address ranges or domains
  - Statistical anomalies
- Web/HTTP access logs
  - HTTP status codes
  - HTTP headers
- VoIP and call managers and Session Initiation Protocol (SIP) traffic
  - Log endpoint connections
  - Type of connection
  - Via headers
- Dump files
  - Data from system memory

Network Data Sources

- Protocol analyzer output
  - Pivot from alert event to per-packet or frame analysis
  - Extract binary data
- Netflow/IPFIX
  - Records traffic statistics
  - Flows defined by endpoints and ports (keys)
  - Netflow exporters and collectors
- Bandwidth monitor

ควบคุมกักกันดูแล ขั้นตอน การควบคุม (control) ตัวอาจ Lead ไปยังตอนเกิดปัญหา ตอนขึ้น prod.

Containment Phase (Apply Mitigation Controls)

- Response must satisfy different or competing objectives
  - What is the loss or potential for loss?
  - What countermeasures are available?
  - What evidence can be collected?
- Isolation-based containment
  - Remove the affected system
  - Disconnect hosts from power
  - Prevent hosts communicating on network
  - Disable user accounts or applications
- Segmentation-based containment ← ลดผลกระทบไม่ให้ทั่ว เกิดเป็นวงกว้าง
  - Use sinkhole or sandbox to analyze attack

Incident Eradication and Recovery

- Eradication of attack tools and access methods
- Recovery of systems to restore the operation of business workflows
- Reconstitution of affected systems
- Re-audit security controls – what could have prevented the intrusion?
- Notification and third-party impacts

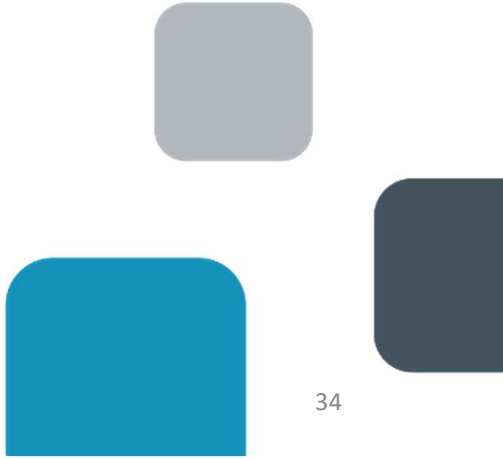
Firewall Configuration Changes

- Analyze attack to determine vector
- Reduce attack surface through configuration changes
  - New security control
  - Update existing control configuration
- Egress filtering for firewall rules
- Detection of other covert channels

Exam

Content Filter Configuration Changes

- Secure web gateway for egress filtering
  - Update URL/content filtering using threat data
- Data loss prevention (DLP)
  - Identify whether DLP mechanisms were circumvented
- Mobile device management (MDM)
  - Identify whether MDM mechanisms were circumvented
- Update or revoke certificates
  - Remove compromised root certificates from trust stores
  - Revoke certificates on compromised hosts
    - Re-key certificate



Endpoint Configuration Changes

- Re-assess attack surface and attack vectors
  - Social engineering
  - Vulnerabilities
  - Lack of security controls
  - Configuration drift
  - Weak configuration
- Application allow lists/block lists
  - Change to least privilege
  - Identify failure of controls to prevent execution
- Quarantine
  - Isolate suspect systems for analysis in sandbox

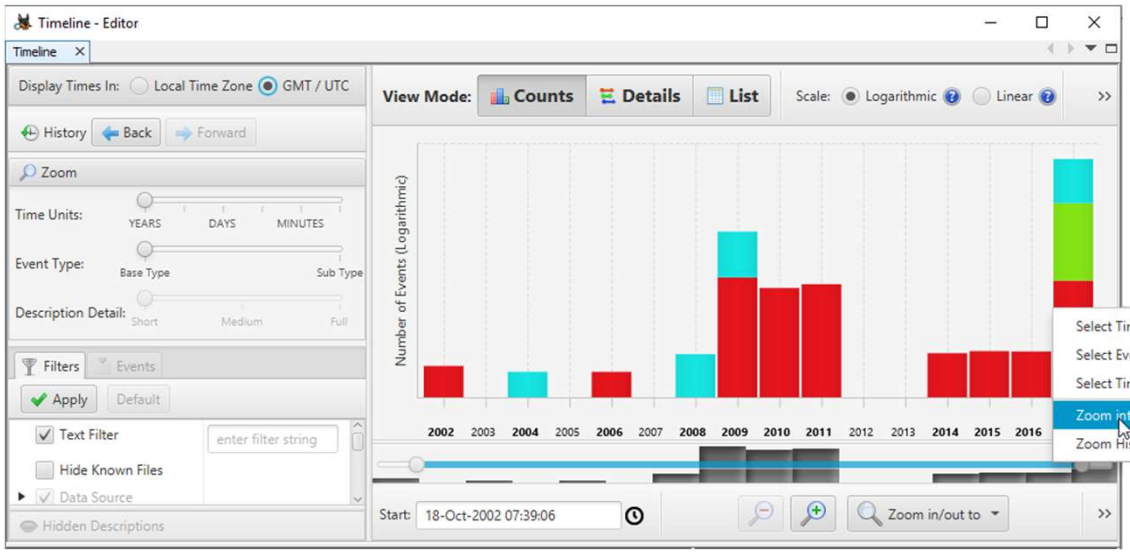
Digital Forensics Reports

- 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

Video and Witness Interviews

- Video
  - Record all actions
  - Log/video steps taken
- Witness interviews
  - Informal statements
  - Avoid leading questions
  - Formal questioning

Timelines



Screenshot: Autopsy - the Sleuth Kit (sleuthkit.org/autopsy.)

- Sequence of events
- Time stamps
  - OS/file system methods for recording time
  - Correct synchronization of local time source
- Time offset
  - Coordinated Universal Time (UTC)
  - Local time
- Date/time settings tampering