UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Prednáška 10
Digital Forensics, Incident Analysis and Response

Riešenie bezpečnostných incidentov
(CyberOps Associate v1.02)

Mgr. Jana Uramová, PhD.
Katedra informačných sietí
Fakulta riadenia a informatiky, UNIZA

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.

Ktorý výsledok pokrýva táto prednáška

Výsledky vzdelávania

Študent po absolvovaní predmetu získa vedomosti a zručnosti potrebné na úspešné zvládnutie úloh, povinností a zodpovedností bezpečnostného analytika v operačnom centre bezpečnosti.
Študent po absolvovaní predmetu bude vedieť:

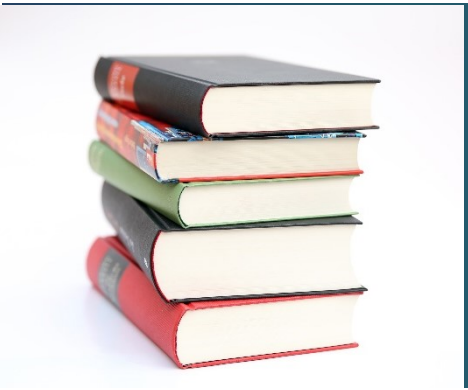
- Vysvetliť rolu analytika v rámci kybernetickej bezpečnosti
- Vysvetliť prostriedky operačného systému Windows a Linux a charakteristiky pre podporu analýzy v rámci kybernetickej bezpečnosti
- Analyzovať operácie v rámci sieťových protokolov a služieb
- Vysvetliť operácie sieťovej infraštruktúry
- Klasifikovať rôzne typy sieťových útokov
- Použiť sieťové monitorovacie nástroje na identifikáciu útokov proti sieťovým protokolom a službám
- Použiť rôzne metódy na prevenciu škodlivého prístupu do počítačových sietí, k používateľom a k dátam
- Vysvetliť vplyvy kryptografie v rámci monitorovania bezpečnostných sietí
- Vysvetliť, ako skúmať a vyhodnocovať zraniteľnosti a útoky koncových zariadení
- Identifikovať hlásenia v rámci sieťovej bezpečnosti
- Analyzovať sieťovú prevádzku na overenie potencionálneho zneužitia siete
- Aplikovať reakčné modely na incident, a získať prostriedky na manažovanie sieťových bezpečnostných incidentov

- Prerekvizity:
  - Princípy IKS, Počítačové siete 1, Úvod do OS

Preliminary version of topics for lectures

Planning

Week	CyberOps Modules in lectures	Exam from:
1	Chapter 1 The Danger Chapter 2 Fighters in the War Against Cybercrime Chapter 3: The Windows Operating System	none
2	Chapter 4: Linux Overview Chapter 5 Network Protocols Chapter 6 Ethernet and Internet Protocol (IP) Chapter 7 Connectivity Verification Chapter 8 Address Resolution Protocol Chapter 10 Network Services Chapter 11 Network Communication Devices	1-2
3	Chapter 9 The Transport Layer (+nmap) Chapter 12 Network Security Infrastructure	3-4
4	Chapter 13 Attackers and Their Tools Chapter 14 Common Threats and Attacks	5-10
5	Chapter 15 Network Monitoring and Tools *(SIEM, SOAR)* Chapter 16 Attacking the Foundation *(L2, L3 protocols vulnerabilities and attacks)* Chapter 17 Attacking What We Do *(L7 vulnerabilities and attacks)*	11-12
6	Chapter 18 Understanding Defense *(security management)* Chapter 19 Access Control *(AAA)* Chapter 20 Threat Intelligence *(commercials, CVE database)*	13-17
7	Chapter 21 Cryptography Chapter 22 Endpoint Protection	18-20
8	Chapter 23 Endpoint Vulnerability Assessment Chapter 24 Technologies and Protocols	none
9	Chapter 25 Network Security Data Chapter 26 Evaualting Alerts (in Security Onion)	21-23
10	Chapter 27 Working with Network Security Data (Security Onion and ELK) Chapter 28 Digital Forensics and Incident Analysis and Response	24-25
11	Expert talk (invited lecture)	26-28



Obsah dnešnej prednášky

Čo prejdeme spolu na prednáške:

- **Chapter 27 Working with Network Security Data (Security Onion and ELK)**
- **Chapter 28 Digital Forensics and Incident Analysis and Response**

Module 27:
Working with Network Security Data
(Security Onion and ELK)

Module Objective: Explain the types of network security data used in security monitoring.

Topic Title	Topic Objective
A Common Data Platform	Explain how data is prepared for use in a Network Security Monitoring (NSM) system.
Investigating Network Data	Use Security Onion tools to investigate network security events.
Enhancing the Work of the CyberSecurity Analyst	Describe network monitoring tools that enhance workflow management.

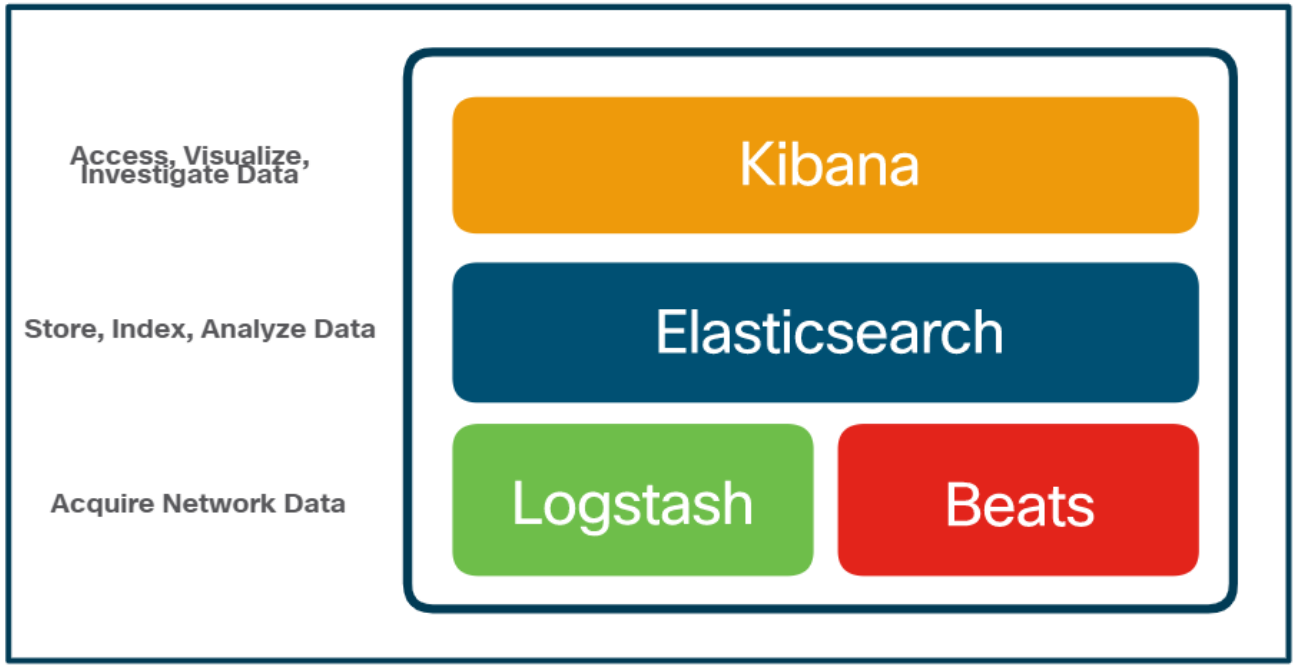
27.1 A Common Data Platform

ELK

Security Onion includes Elastic Stack that consists of Elasticsearch, Logstash, and Kibana (ELK).

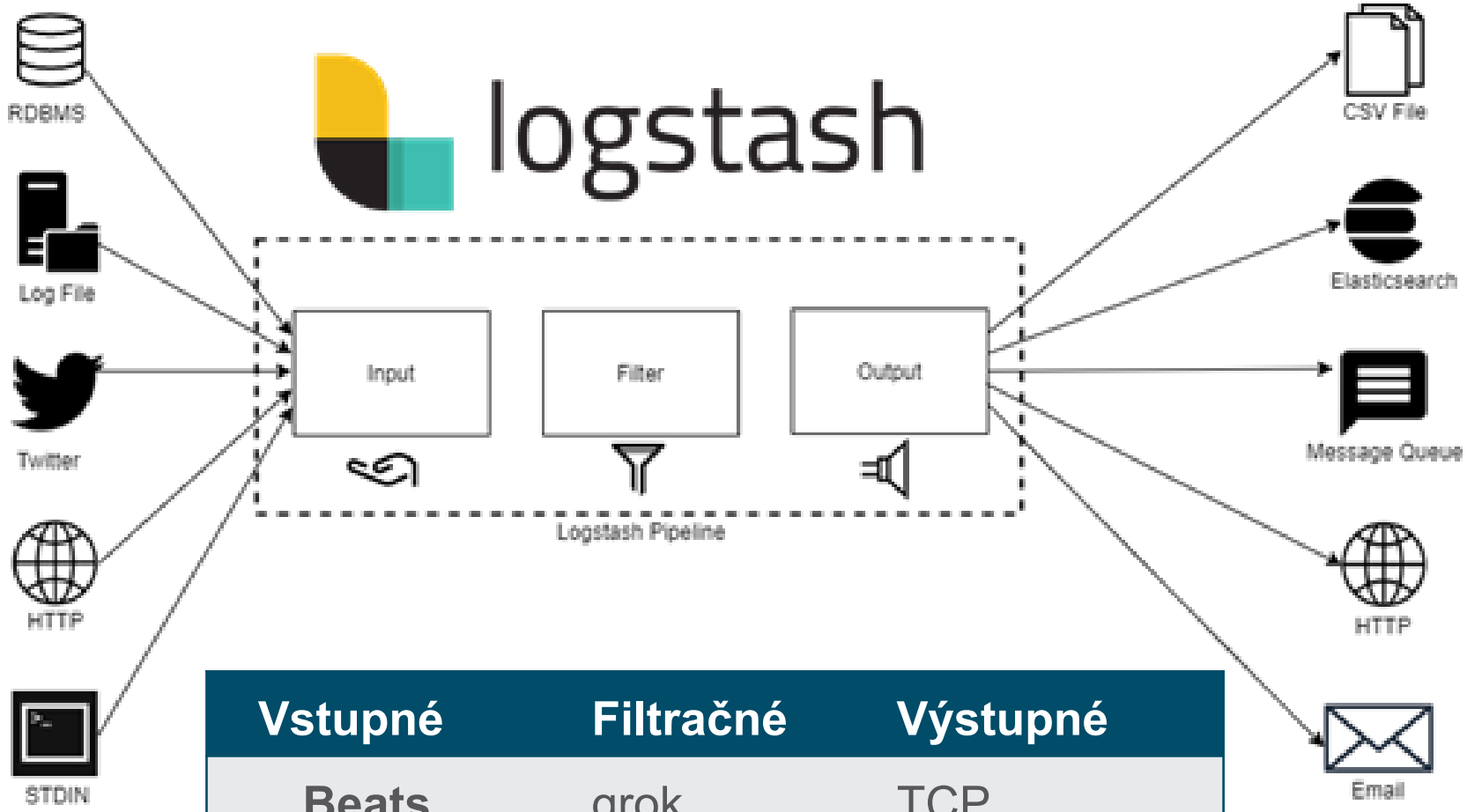
Core Components of ELK:

- **Elasticsearch**: An open-core platform for searching and analyzing an organization's data in near real time.
- **Logstash**: Enables collection and normalization of network data into data indexes that can be efficiently searched by Elasticsearch.
- **Kibana**: Provides a graphical interface to data that is compiled by Elasticsearch.
- **Beats**: Series of software plugins that send different types of data to the Elasticsearch data stores.



Logstash

- Pôvodne podporoval hlavne zber logov
- v súčasnosti vie akýkoľvek typ udalosti rozšíriť alebo transformovať
  - pomocou širokej škály vstupných, filtračných a výstupných doplnkov
- Obsahuje viac ako 200 pluginov
- ponúka aj možnosť vytvoriť si vlastné



Vstupné	Filtračné	Výstupné
Beats	grok	TCP
súbor	JSON	stdout
HTTP	GeoIP	súbor
Kafka	xml	email
Syslog		Elasticsearch

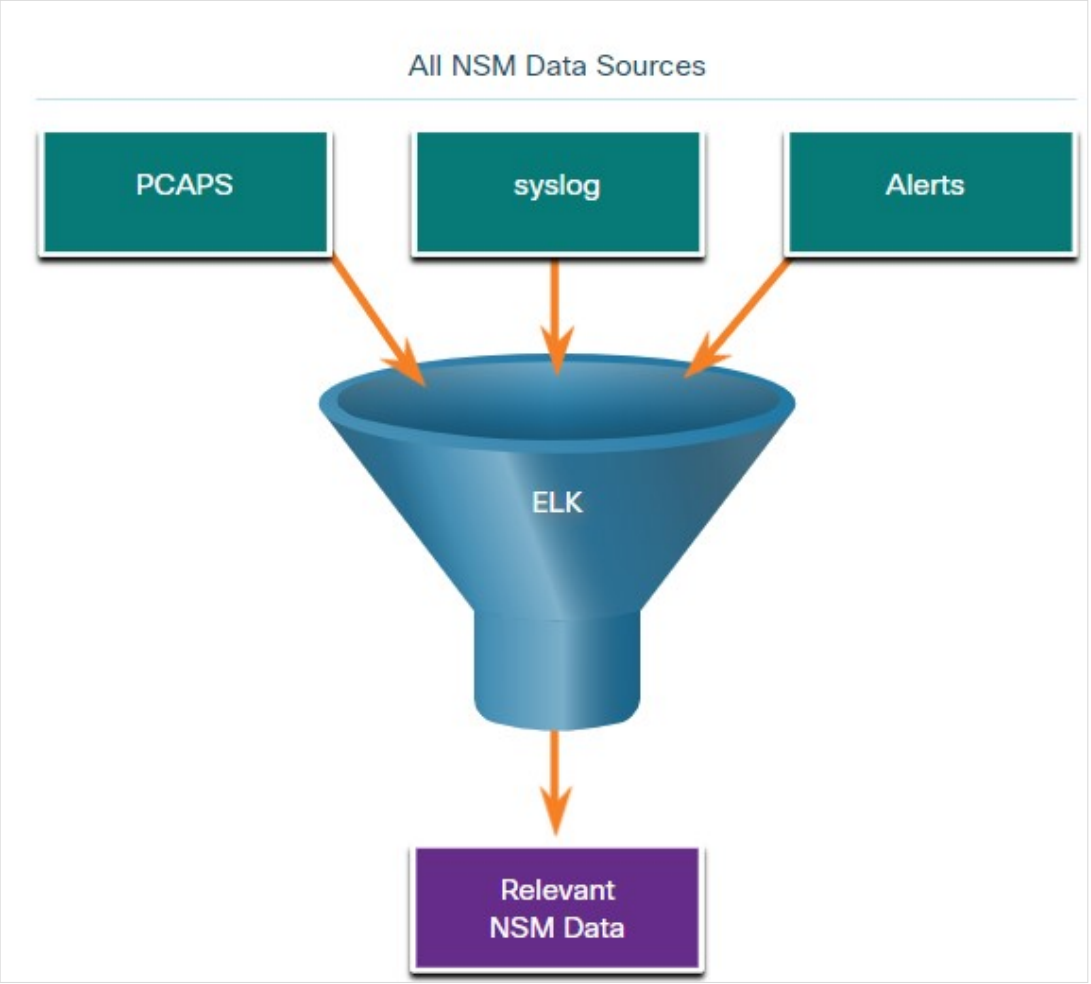
Logstash – plugin Beats – FileBetas and others…

- Beat moduly sa nainštalujú na hostoch a odosielajú rôzne údaje do Elastic Stacku na ďalšiu analýzu
- Každý Beat modul je určený na odosielanie iného typu informácie
  - Winlogbeat napríklad odosiela udalostné logy z OS Windows
  - Metricbeat dodáva metriky hosta
  - Filebeat dodáva súbory s logmi
- Filebeat
  - nainštalovaný na serveri, kde sa generujú logy
  - sleduje logy a preposiela údaje
    - buď do Logstash-u pre pokročilejšie spracovanie
    - alebo priamo do ES databázy na indexovanie
  - môže buď pracovať samostatne a nahradiť Logstash, alebo s ním môže spolupracovať.

- Filebeat
  - v jazyku Go
  - založený na protokole Lumberjack
    - malá pamäťová náročnosť, schopnosť spracovávať veľké objemy dát a podporou šifrovania
  - Zaznamenáva aj posledný úspešne spracovaný log
    - v prípade problémov so sieťou si dokáže zapamätať, kde skončil, a po opätovnom nadviazaní spojenia tam bude pokračovať
  - obsahuje vyše 60 rôznych modulov:
    - Apache
    - AWS
    - Cisco
    - Fortinet
    - MySQL
    - Suricata

Data Reduction

- To reduce data, it is essential to identify the network data that should be gathered and stored to reduce the burden on systems.
- By limiting the volume of data, tools like Elasticsearch will be far more useful.



Data Normalization

- Data normalization is the process of combining data from a number of sources into a **common format**.
  - A common schema will specify the **names** and **formats** for the required data fields.
  - For example, IPv6 addresses, MAC addresses, and date and time can be represented in varying formats:

IPv6 Address Formats	Mac Formats	Date Formats
2001:db8:acad:1111:2222::33	A7:03:DB:7C:91:AA	Monday, July 24, 2017 7:39:35pm
2001:DB8:ACAD:1111:2222::33	A7-03-DB-7C-91-AA	Mon, 24 Jul 2017 19:39:35 +0000
2001:DB8:ACAD:1111:2222:0:0:33	A70.3DB.7C9.1AA	2017-07-24T19:39:35+00:00

- Data normalization is also required to simplify searching for **correlated events**.

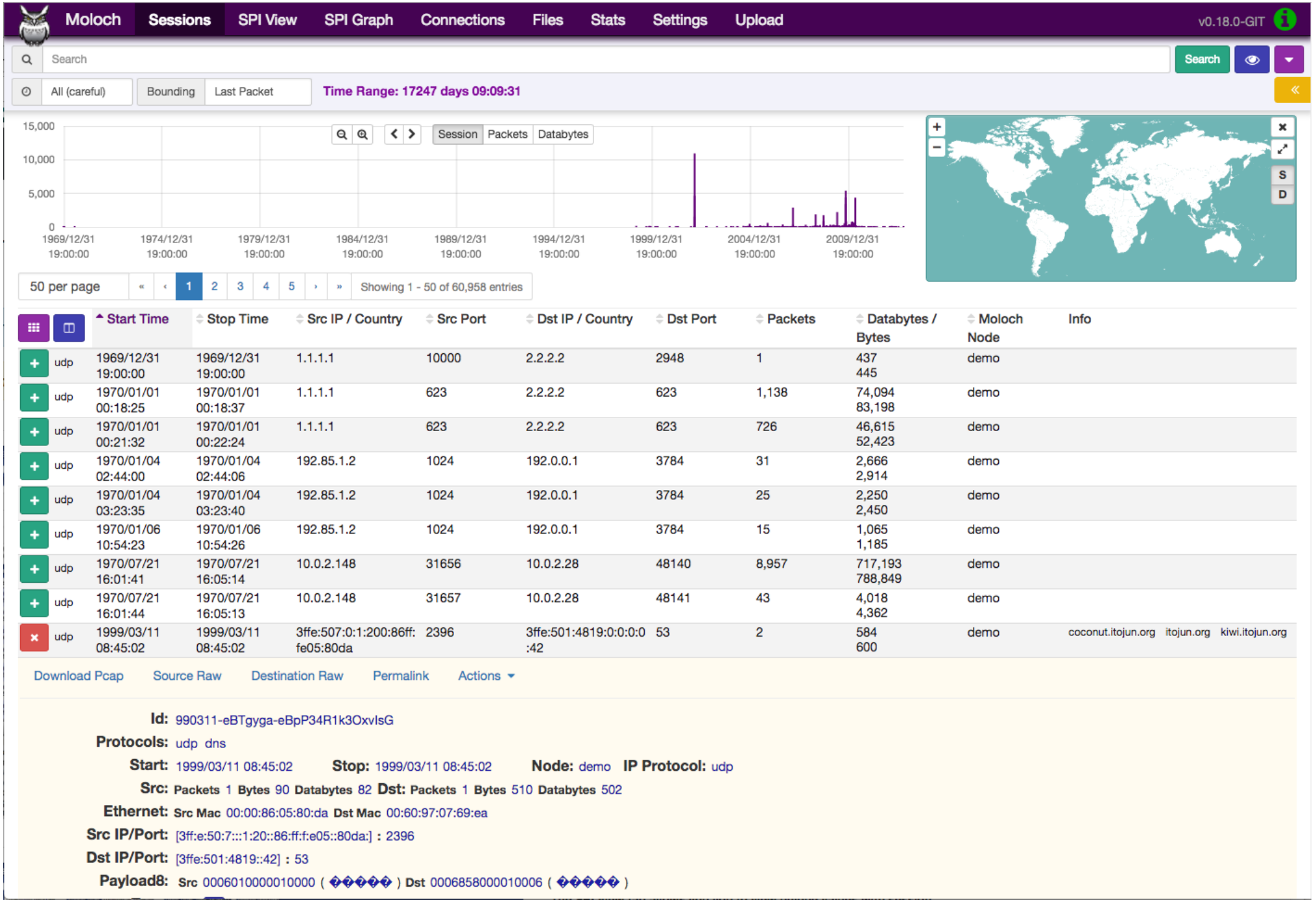
Data Archiving

- Retaining Network Security Monitoring (NSM) data **indefinitely** is not feasible due to storage and access issues.
- The retention period for certain types of network security information may be specified by **compliance frameworks**.
- Sguil alert data is retained for 30 days by default. This value is set in the **securityonion.conf** file.
- Security Onion data can always be archived to **external storage** by a data archive system, depending on the needs and capabilities of the organization.

***Note**: The storage locations for the different types of Security Onion data will vary based on the Security Onion implementation.*

Archivation tools

- Arkime



Lab - Convert Data into a Universal Format

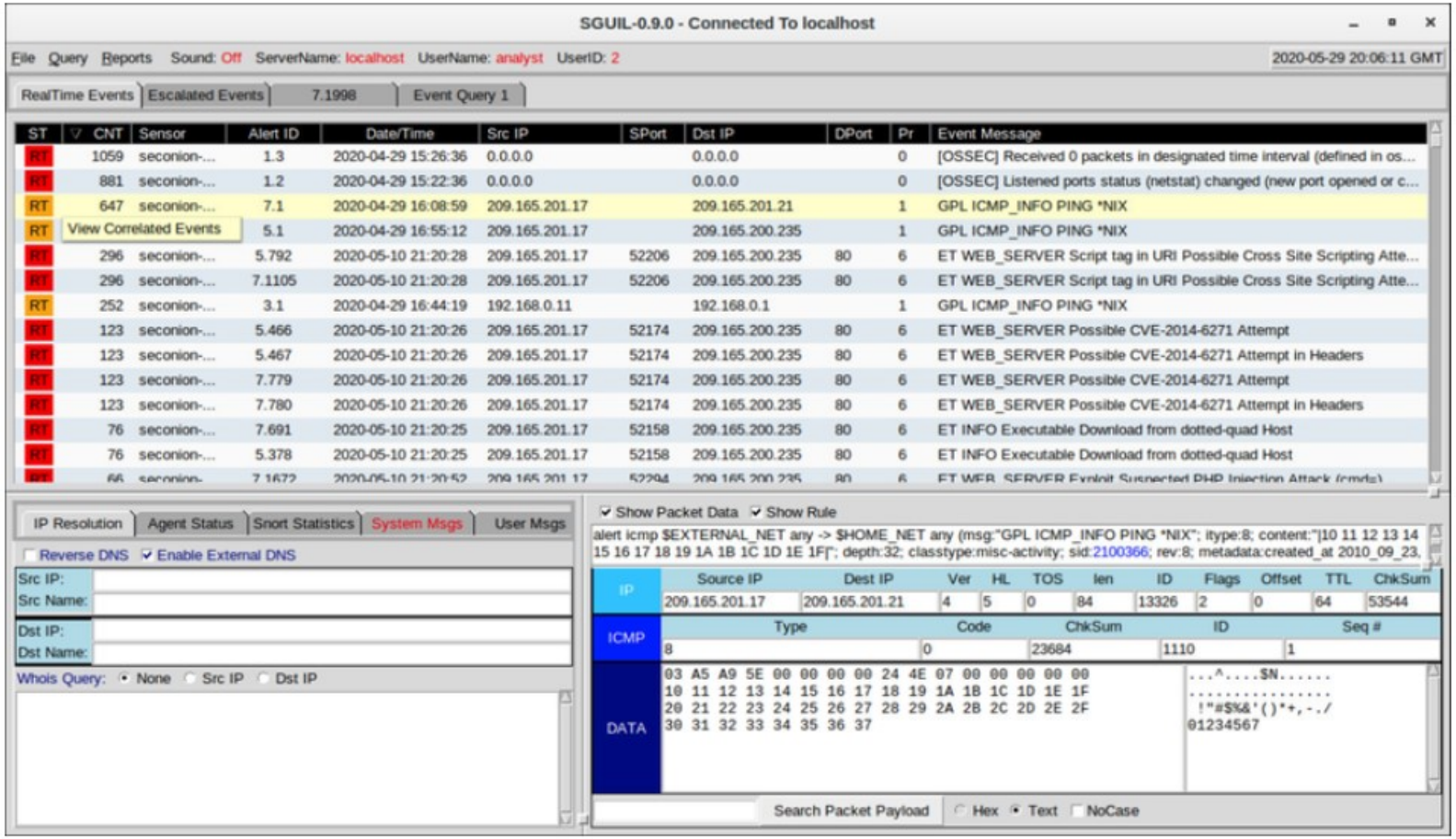
In this lab, you will complete the following objectives:

- **Part 1**: Use command line tools to manually normalize log entries.
- **Part 2**: The timestamp field must be normalized.
- **Part 3**: The IPv6 field requires normalization.

27.2 Investigating Network Data

Working in Sguil

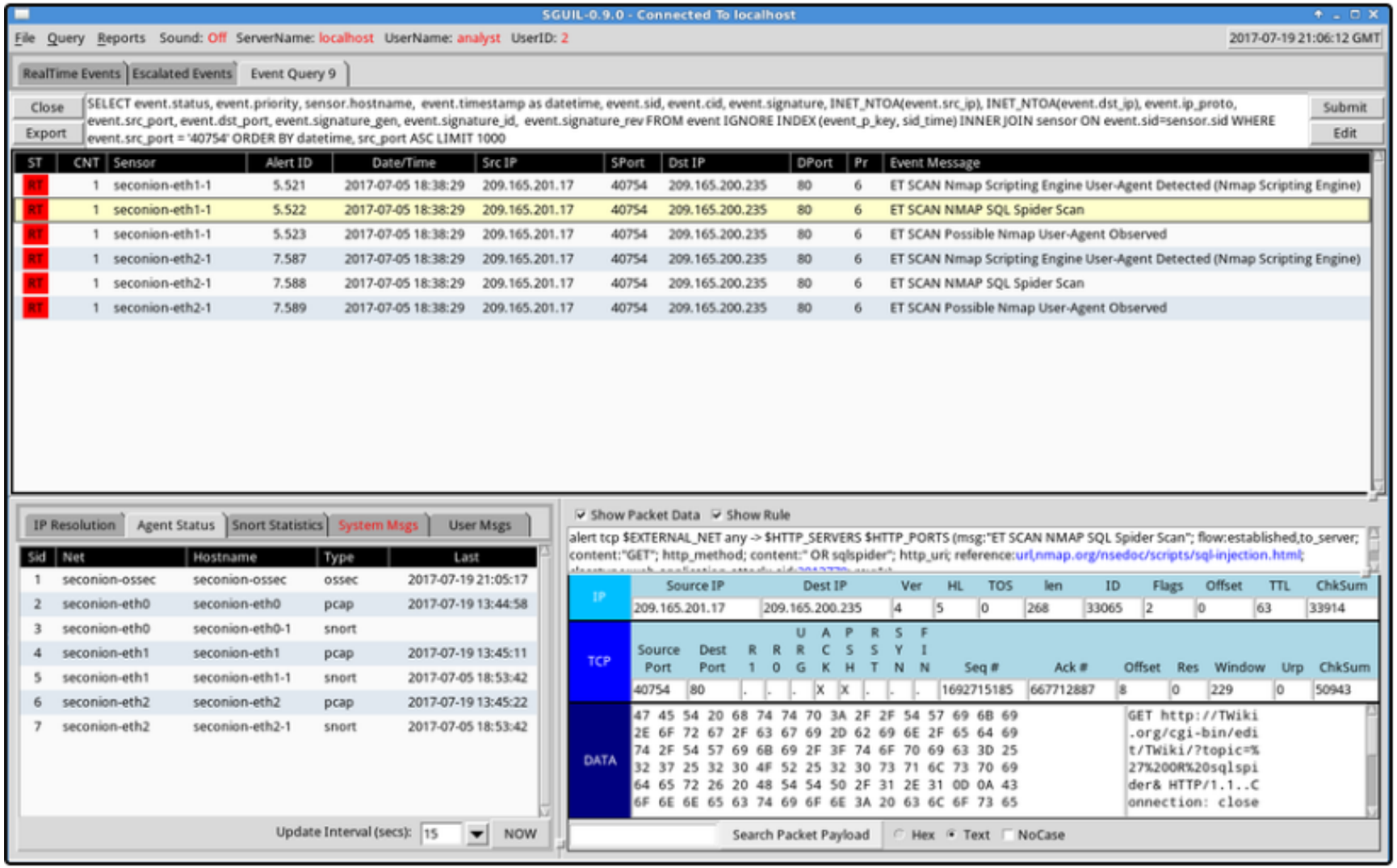
- In Security Onion, the **first place** that a cybersecurity analyst will go to verify alerts is **Sguil**.
- Sguil **automatically correlates** similar alerts into a single line and provides a way to view correlated events represented by that line.
- To understand what is happening in the network, it may be useful to **sort** the **CNT** column to display the alerts with the highest frequency.



Sguil Alerts Sorted on CNT

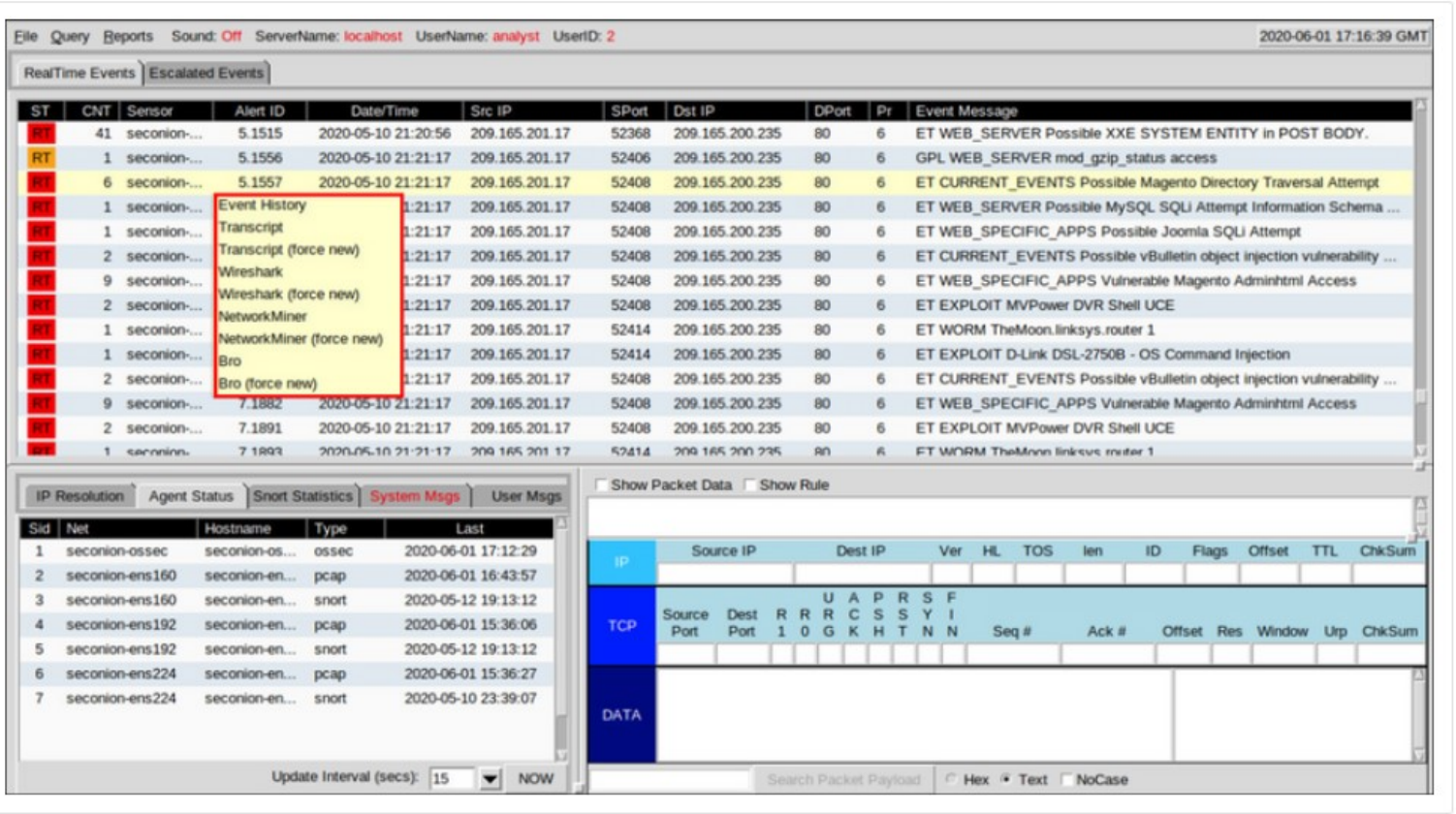
Sguil Queries

- Queries can be constructed in Sguil using the **Query Builder**. It simplifies constructing queries to a certain degree.
- Cybersecurity analyst must know the **field** names and some issues with field values to effectively build queries in Sguil.
- For example, Sguil stores **IP addresses** in an integer representation.



Pivoting from Sguil

- Sguil provides the ability for the cybersecurity analyst to pivot to other information sources and tools.
- Log files are available in Elasticsearch.
- Relevant packet captures can be displayed in Wireshark.
- Sguil can provide pivots into PRADS, SANCP
  - Passive Real-time Asset Detection System (PRADS, PADS in Squil interface)
  - Security Analyst Network Connection Profiler (SANCP) information



PRADS and SANCP – also in Squil

Passive Real-time Asset Detection System (PRADS)

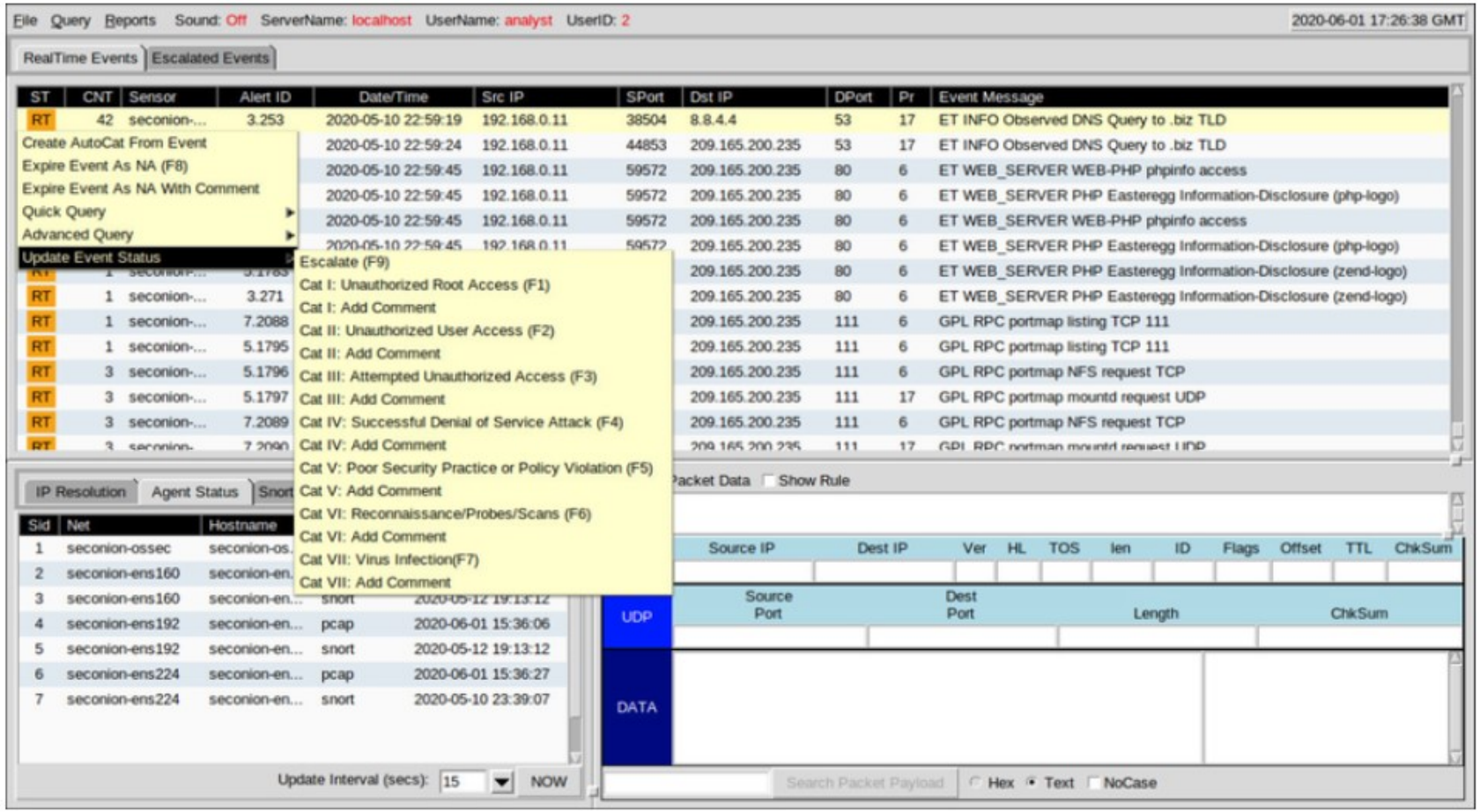
- passively listens to network traffic
- gathers information about hosts and services sending traffic
- potential use of this data is
  - to map out your network without performing an active scan (no packets are ever sent)
  - allowing you to enumerate active hosts and services
    - And monitor for changes in real time
  - can be used together with your favorite IDS/IPS setup for "event to application" correlation
- https://github.com/gamelinux/prads

Security Analyst Network Connection Profiler (SANCP)

- network security tool designed to
  - create connection logs and record network traffic
  - for the purpose of
    - Auditing
    - historical analysis
    - network activity discovery
- https://sancp.sourceforge.net/

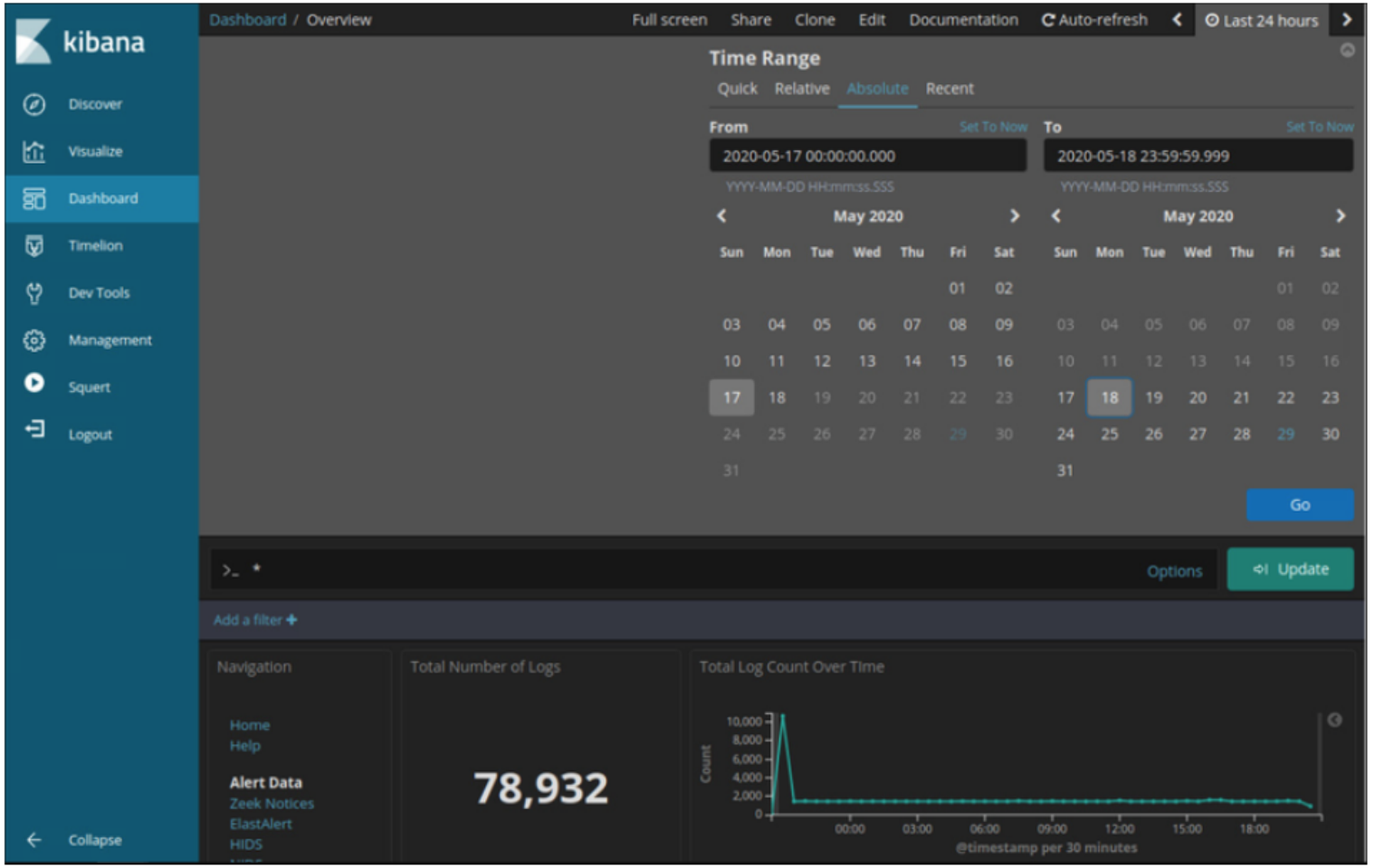
Event Handling in Sguil

- Sguil enables to **investigate**, **verify**, and **classify** security alerts.
- Three tasks can be completed in Squil to manage alerts:
  - Alerts that have been found to be false positives can be **expired**.
  - An event can be **escalated** by pressing the F9 key.
  - An event can be **categorized**.
    - Sguil includes 7 pre-built categories
      - that can be assigned by using a **menu** or by pressing the **function key**.



Working in ELK

- **Logstash** and **Beats** are used for data ingestion *(prijatie)* in the Elastic Stack.
- **Kibana**, which is the visual interface into the logs, is configured to show **the last 24 hours** by default.
- Logs are ingested into Elasticsearch into separate **indices *(indexy)*** or databases based on a configured range of time.
- The best way to monitor the data in Elasticsearch is **to build** customized visual **dashboards**.



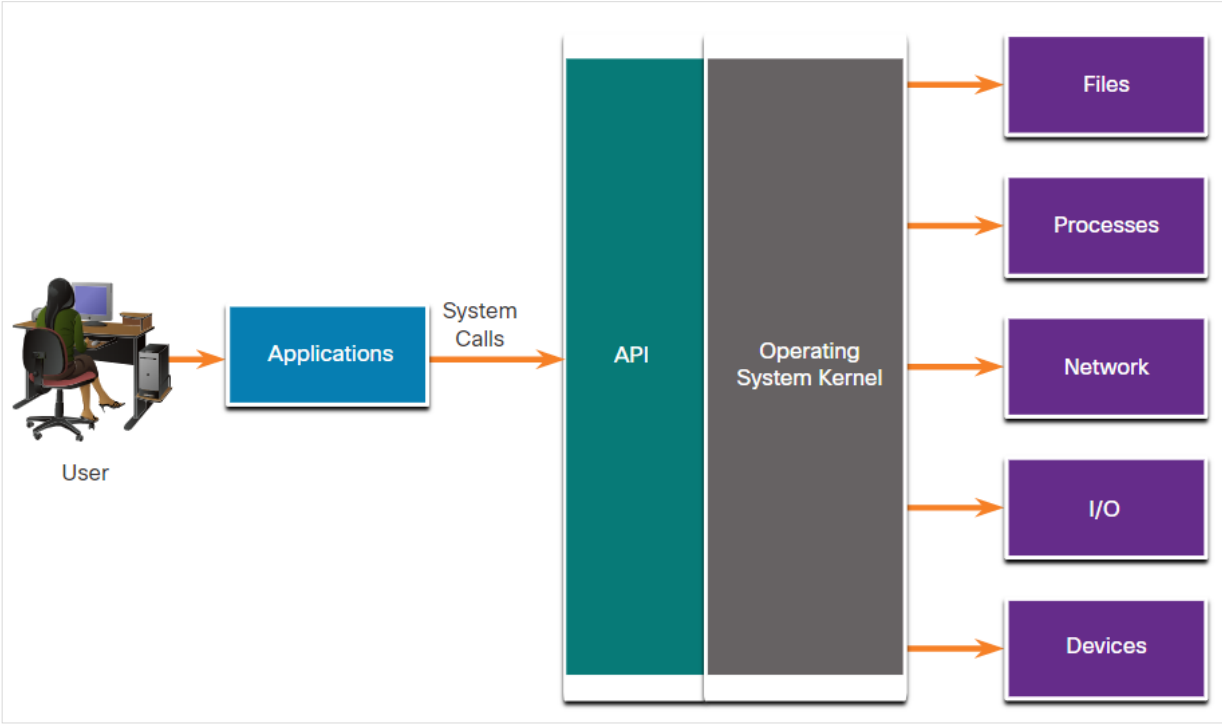
Queries in ELK

- Elasticsearch is built on **Apache Lucene**, an open-source search engine software library featuring full text indexing and searching **capabilities**.
- Using Lucene software libraries, Elasticsearch has its **own query language** based on JSON called **Query Domain Specific Language (DSL).**
- Along with JSON, Elasticsearch **queries** make use of elements such as Boolean operators, Fields, Ranges, Wildcards, Regex, Fuzzy Search, and Text Search.
- Elasticsearch was designed to interface with users using **web-based clients** that follow the **HTTP REST framework**.
- Methods used for executing the queries are URI, cURL, JSON and Dev Tools.

***Note**: Advanced Elasticsearch queries are beyond the scope of this course. In the labs, you will be provided with the complex query statements, if necessary.*

Investigating Process or API Calls

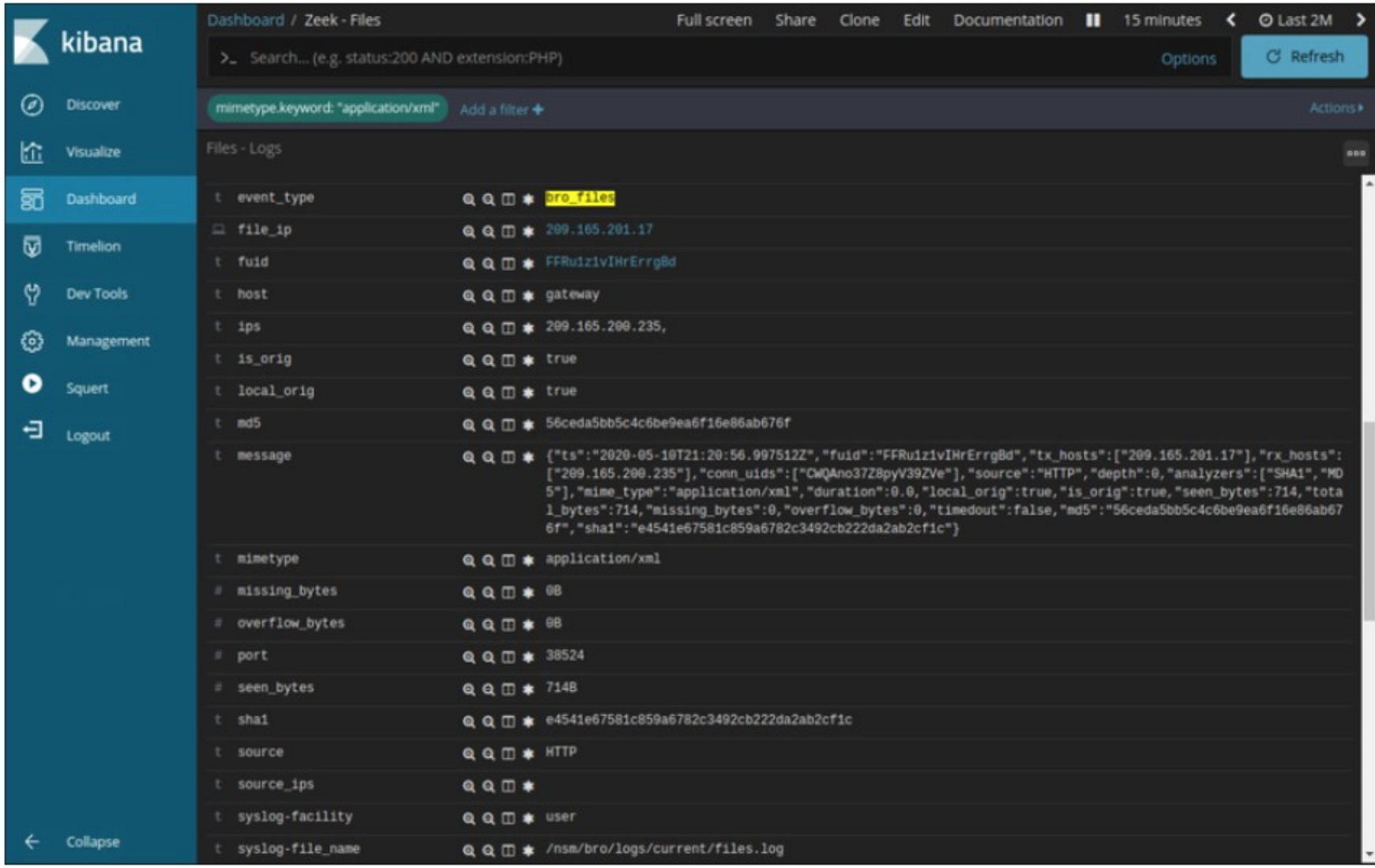
- Applications interact with an Operating System (OS) through **system calls** to the OS Application Programming Interface (API).
- If malware can fool *(obalamutit')* an OS kernel into allowing it to make system calls, many exploits are possible.
- **OSSEC** rules
  - detect changes in host-based parameters.
  - will trigger an alert in Sguil.
- Pivoting to Kibana on the host IP address
  - allows to choose the type of alert based on the program that created it.



- Filtering for OSSEC indices results in a view of the OSSEC events that occurred on the host, including indicators that malware may have interacted with the OS kernel

Investigating File Details

- In Sguil, if the cybersecurity analyst is **suspicious** *(má podozrenie)* of a file, the **hash value** can be submitted to an **online site** to determine if the file is a known **malware**.
- In Kibana, **Zeek** Hunting can be used to display information regarding the files that have entered the network.
- Note that in Kibana, the event type is shown as **bro_files**, even though the new name for Bro is Zeek.



Lab - Interpret HTTP and DNS Data to Isolate Threat Actor

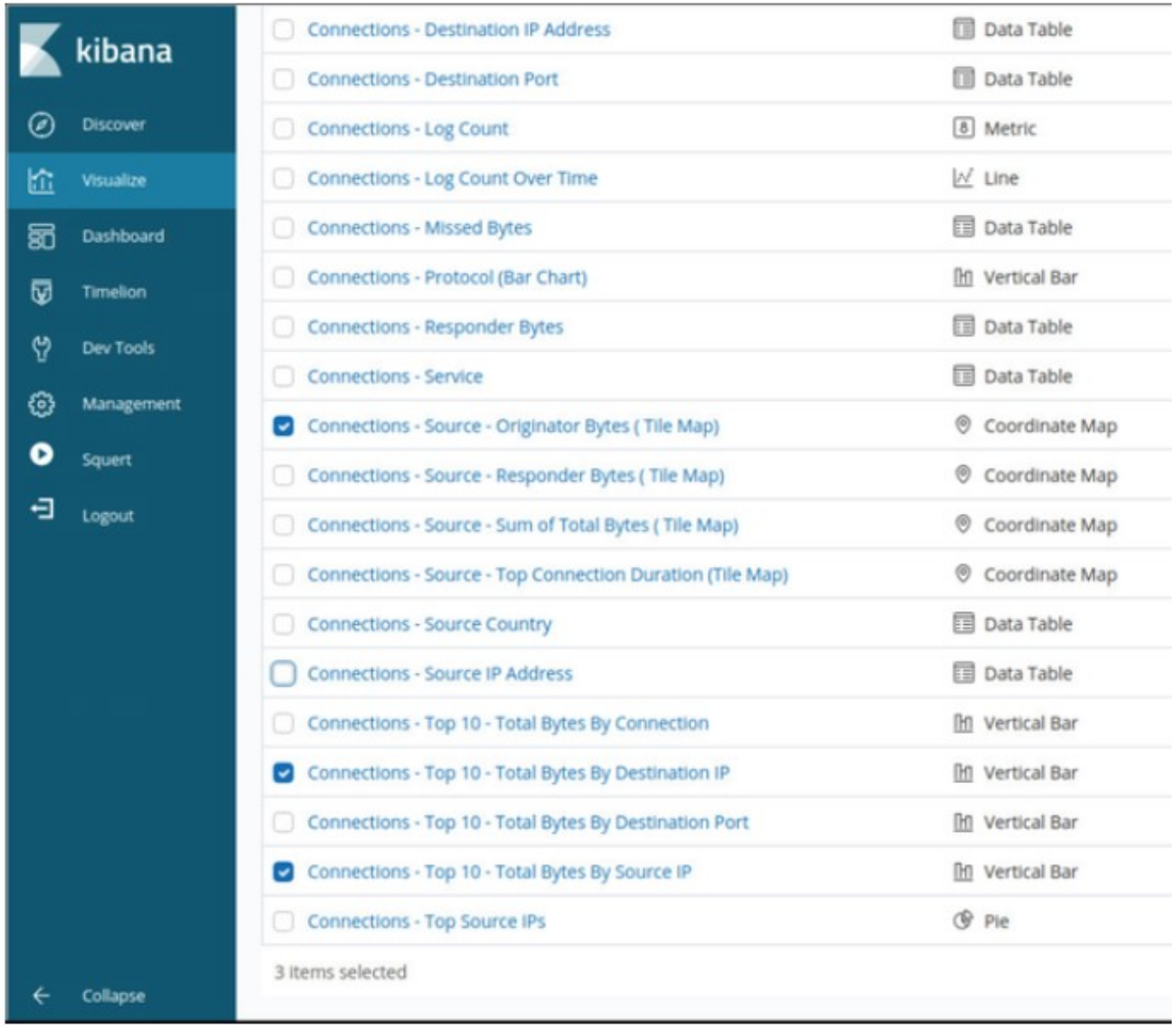
In this lab, you will complete the following objective:

- Investigate SQL injection and DNS exfiltration exploits using Security Onion tools.

27.3 Enhancing the Work of the Cybersecurity Analyst

Dashboards and Visualizations

- Dashboards provide a combination of **data** and **visualizations** which allows cybersecurity analysts to focus on specific details and information.
- Dashboards are usually **interactive**.
- Kibana includes the capability of designing **custom** dashboards.
- In addition, tools such as **Squert** in Security Onion provide a visual interface to NSM data.



Workflow Management

- Workflows are the sequence of processes and procedures through which work tasks are completed.
- Managing the SOC workflows:
  - **Enhances** the efficiency of the cyberoperations team
  - **Increases** the accountability *(zodpovednosť)* of the staff
  - **Ensures** that all potential alerts are treated properly
- How:
  - **Sguil** provides a basic workflow management but not a good choice for large operations.
  - There are **third party** systems available that can be customized.
- Automated queries add efficiency to the cyberoperations workflow.
  - These queries automatically search for complex security incidents that may evade other tools.

27.4 Working with Network Security Data Summary

What Did I Learn in this Module?

- A network security monitoring platform such as ELK or Elastic Stack must unite the data for analysis.
- ELK consists of Elasticsearch, Logstash, and Kibana with components, Beats, ElastAlert, and Curator.
- Network data must be reduced so that only relevant data is processed by the NSM system.
- Network data must also be normalized to convert the same types of data to consistent formats.
- Sguil provides a console that enables a cybersecurity analyst to investigate, verify, and classify security alerts.
- Kibana visualizations provide insights into NSM data by representing large amounts of data formats that are easier to interpret.
- Workflow management adds efficiency to the work of the SOC team.

Chapter 28:
Digital Forensics and Incident Analysis and Response

Module Objective: Explain the process of evaluating alerts

Topic Title	Topic Objective
Evidence Handling and Attack Attribution	Explain the role of digital forensics processes
The Cyber Kill Chain	Identify the steps in the Cyber Kill Chain
The Diamond Model of Intrusion Analysis	Classify an intrusion event using the Diamond Model
Incident Response	Apply the NIST 800-61r2 incident handling procedures to a given incident scenario

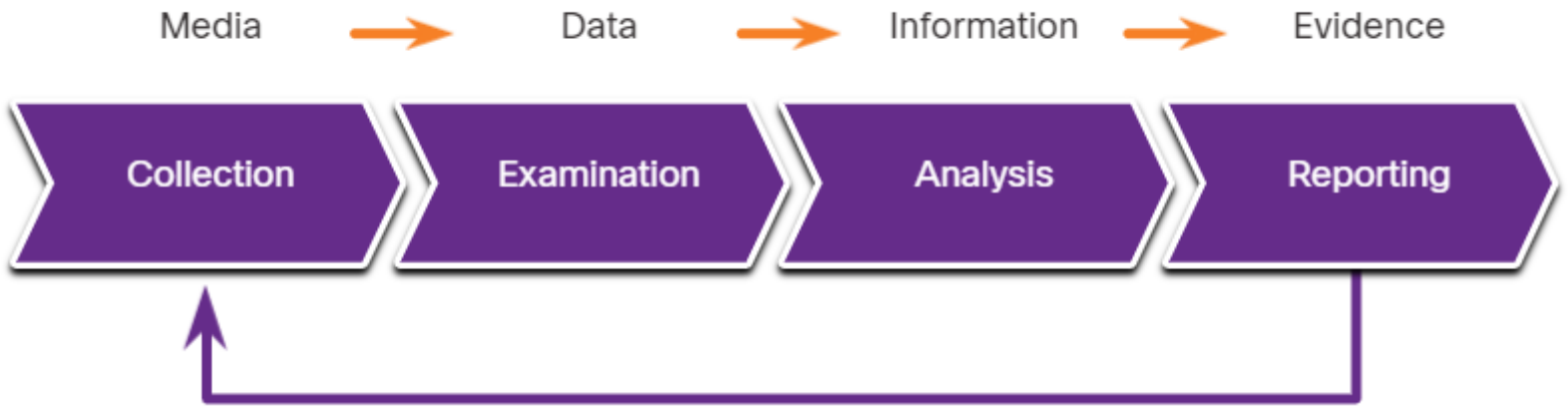
28.1 Evidence Handling and Attack Attribution

Digital Forensics

- It is the recovery and investigation of information found on digital devices as it relates to criminal activity.
- **Indicators of compromise** are the evidence that a cybersecurity incident has occurred.
- For **example**, under the US **HIPAA** regulations, if data breach has occurred involving patient information, then notification of the breach (porušenie) must be made to the affected individuals.
  - Digital forensic investigation must be used to determine the affected individuals and also to certify the number of affected individuals so that appropriate notification can be made in compliance with HIPAA regulations.
  - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- At times *(občas)*, Cybersecurity analysts may find themselves in direct contact with digital forensic evidence *(dôkazy)* that details the conduct *(správanie)* of members of the organization.
- Analysts **must know** the requirements regarding the preservation and handling of such evidence.

The Digital Forensics Process

- NIST describes the 4 phases of the digital evidence forensic process:
  - **Collection -** Identification of potential sources of forensic data and acquisition, handling (manipulácia), and storage of that data
  - **Examination *(skúmanie)*** – Assessing *(hodnotenie)* and extracting relevant information from the collected data
  - **Analysis -** Drawing conclusions from the data and correlation of data from multiple sources
  - **Reporting -** Preparing and presenting information that resulted from the analysis phase.



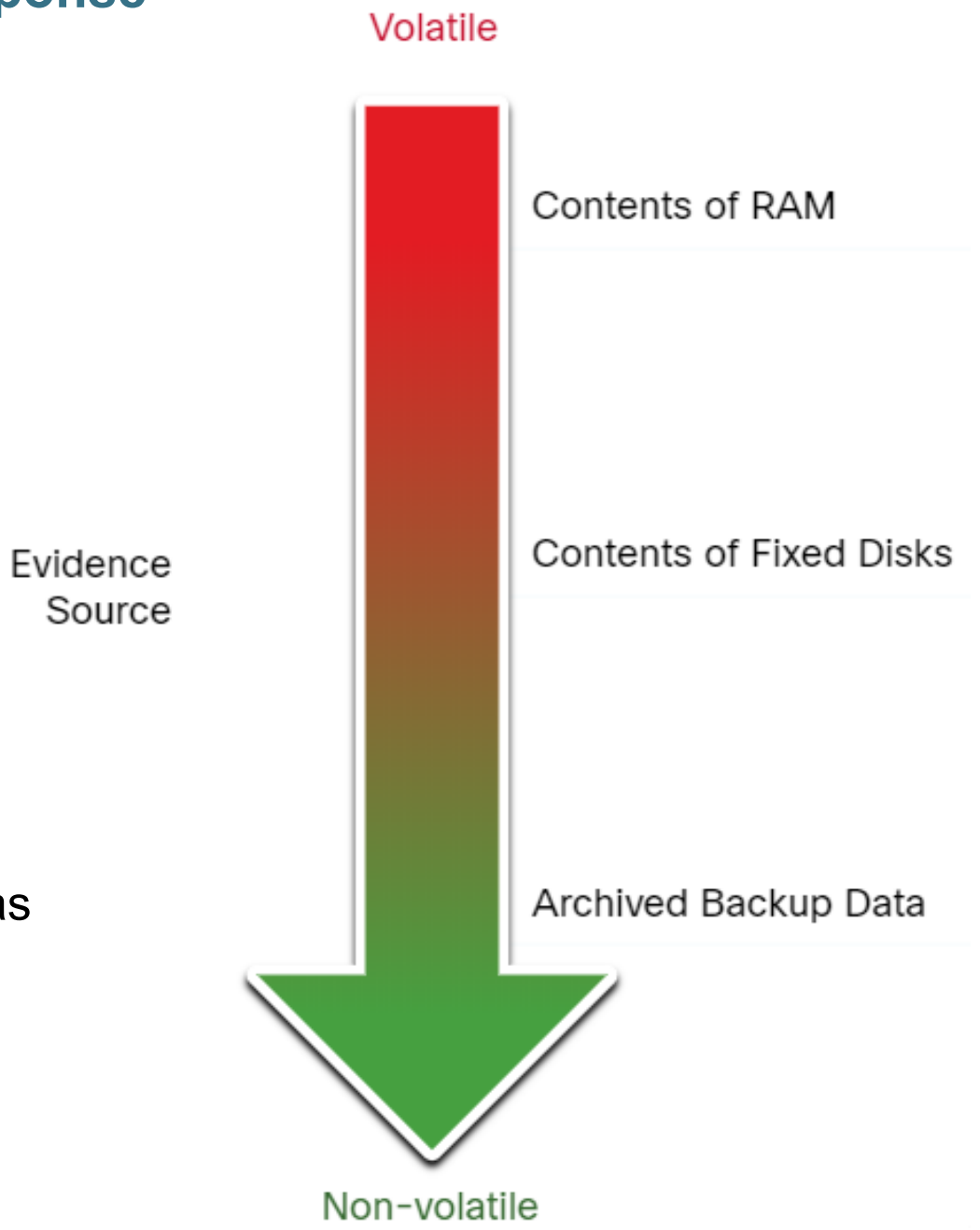
Types of Evidence

In legal proceedings *(súdnom konaní)*, evidence *(dôkaz)* is broadly *(vo všeobecnosti)* classified as following:

- **Direct Evidence** - The evidence that was indisputably in the possession of the accused, or is eyewitness evidence from someone who directly observed criminal behavior.
  - *„ Dôkazy, ktoré mal obvinený nepochybne k dispozícii, alebo sú očitým dôkazom od niekoho, kto priamo pozoroval kriminálne správanie.“*
- **Indirect evidence** - This evidence establishes a hypothesis in combination with other facts. It is also known as circumstantial evidence.
  - *„nepriamy dôkaz“*
- **Best evidence** – This evidence could be storage devices used by an accused, or archives of files that can be proven to be unaltered.
  - *„Týmito dôkazmi môžu byť úložné zariadenia používané obvineným alebo archívy spisov, pri ktorých sa dá dokázať, že sú nezmenené“*
- **Corroborating evidence** - This evidence supports an assertion that is developed from best evidence.
  - „ Tento dôkaz podporuje tvrdenie, ktoré vychádza z najlepších dôkazov.“

Evidence Collection Order

- IETF RFC 3227 describes an **order** for the collection of digital evidence based on the **volatility** of the data.
  - RFC - Guidelines for Evidence Collection and Archiving, 2002, cat: Best current practise
- Data stored in **RAM** is the most volatile and it will be lost when the device is turned off.
- The collection of digital evidence should **begin** with the most volatile evidence and **proceed** *(postupovať)* to the least volatile:
  - Details of the systems from which the evidence was collected
    - including who has access to those systems
    - and at what level of permissions should be recorded.



Chain of Custody *(Reťazec spracovania dôkazov)*

- involves the
  - Collection
  - Handling
  - secure storage of evidence.
- Detailed records should be kept of the following:
  - **Who** discovered and collected the evidence?
  - **All details** regarding the **handling of evidence** including times, places, and personnel involved.
  - **Who** has primary responsibility for the evidence, when responsibility was assigned, and **when** custody *(spracovanie dôkazov)* changed?
  - **Who** has physical access to the evidence while it was stored? Access should be **restricted** to only the most essential personnel.

Data Integrity and Preservation *(Integrita a ochrana údajov)*

Following these processes will **ensure** that any evidence of malpractice *(všetky dôkazy o nesprávnom/nepovolenom postupe)* will be preserved, and any indicators of compromise can be identified:

- **Time stamping** of files
  - should be preserved *(zachované)!*
    - => the original evidence should be copied
    - => and analysis should only be conducted on copies of the original.
  - may be part of the evidence
    - => opening files from the original media should be avoided.
- Archive and protect the **original disk**
  - to keep it in its original, untampered with, condition
- **Special tools** should be used to preserve forensic evidence (zachovanie dôkazov)
  - before the device is shut down and evidence is lost.
- **Users should not** disconnect, unplug, or turn off **infected machines**
  - unless explicitly told to do so by security personnel.

Attack Attribution („Komu sa incident pripíše na účet“)

- refers to the act of determining the **individual**, **organization**, or **nation** responsible for a successful intrusion or attack incident
  - = Identifying responsible threat actors
  - should occur through the principled and systematic investigation of the evidence.
- In an evidence-based investigation, the incident response team correlates **Tactics, Techniques, and Procedures (TTP)** that were used in the incident with other known exploits.
- Some aspects of a threat that can aid in attribution *(komu to pripíšeme na účet)* are
  - the location of originating hosts or domains
  - features of the code used in malware and the tools
  - other techniques.
- For **internal threats**, asset management plays a major role.
  - Uncovering the devices from which an attack was launched can lead directly to the threat actor.
- **IP addresses, MAC addresses, and DHCP logs** can help track the addresses used in the attack back to a specific device.

The MITRE ATT&CK Framework

- The MITRE **Adversarial *(protivník)*** Tactics, Techniques & Common Knowledge (ATT&CK) Framework
  - enables the ability to detect attacker's Tactics, Techniques, and Procedures (TTP)
  - as a part of **threat defense** and **attack attribution**.
- **Tactics** consist of the technical goals that an attacker must accomplish to execute an attack.
- **Techniques** are the means by which the tactics are accomplished.
- Procedures are the specific actions taken by threat actors in the techniques that have been identified.
- The MITRE ATT&CK Framework is a global knowledge base of threat actor behavior.
- The framework is designed to enable automated information sharing by defining data structures for exchanging information between its community of users and MITRE.

  ***Note**: Do an internet search on MITRE ATT&CK to learn more about the tool.*

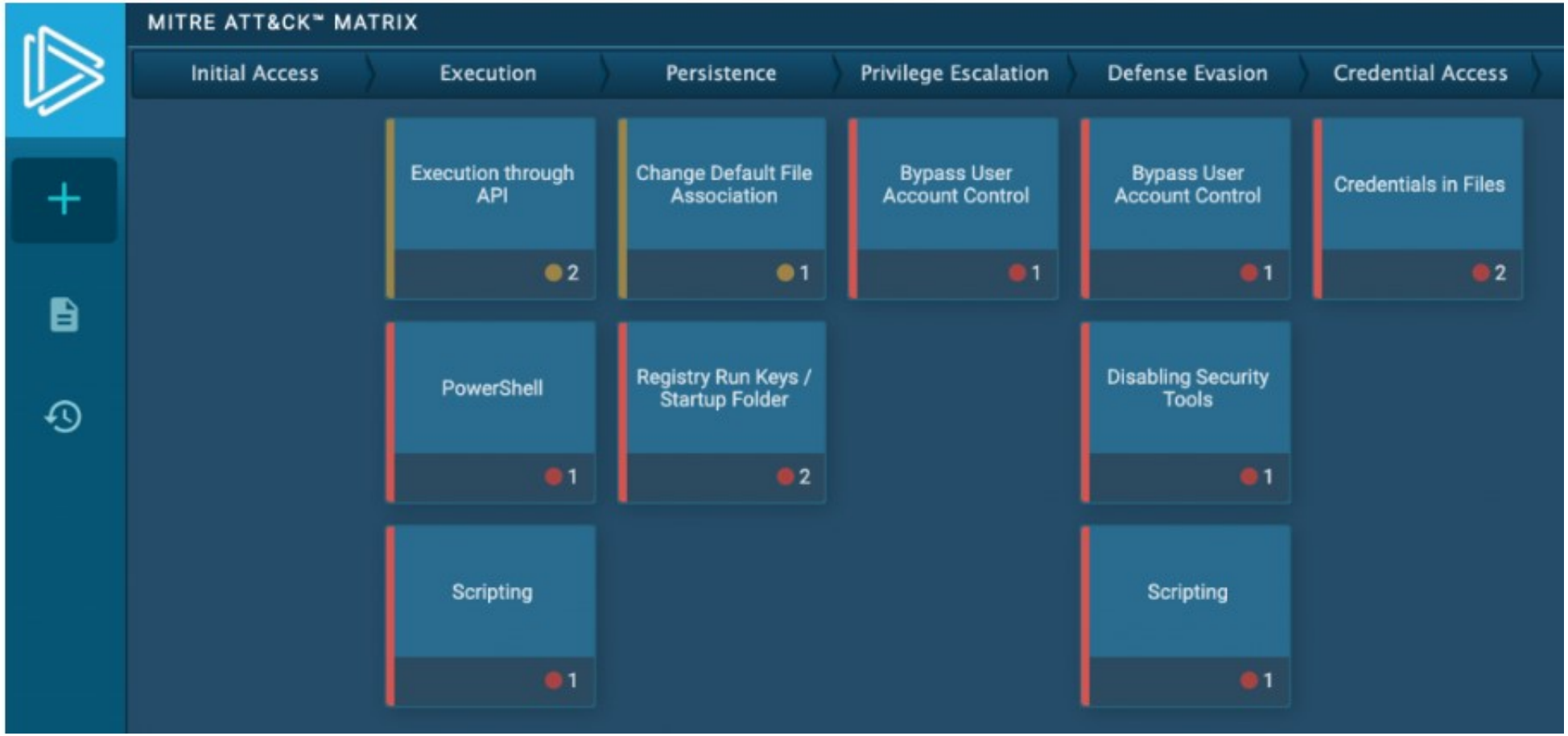
  https://attack.mitre.org/

The MITRE ATT&CK Framework (Contd.)

- The figure shows an analysis of a ransomware exploit from the ANY.RUN online sandbox. The columns show the enterprise attack matrix tactics, with the techniques that are used by the malware.

- Persistance
  = *vytrvalosť*
- Evasion
  = *únik*

MITRE ATT&CK Matrix for a Ransomware Exploit



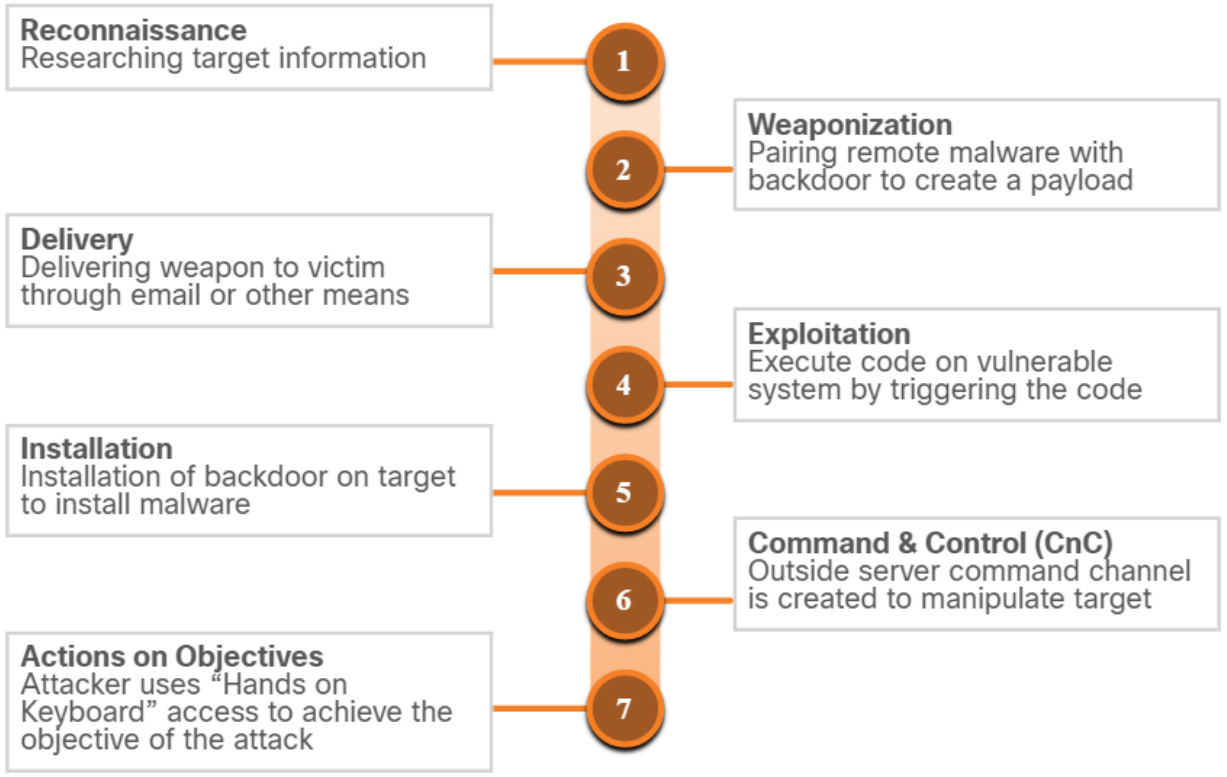
https://any.run/cybersecurity-blog/mitre-attack/

28.2 The Cyber Kill Chain

Steps of the Cyber Kill Chain

- The Cyber Kill Chain was developed by **Lockheed Martin** to identify and prevent cyber intrusions.
- When responding to a security incident, the objective is to detect and stop the attack at the earliest in the kill chain progression to avoid further damage.
- If the attacker is stopped at any stage, the kill chain is broken and the defender successfully thwarted the threat actor's intrusion.

Lockheed Martin Corporation is an American aerospace, arms, defense, information security, and technology corporation with worldwide interests. I



Steps of Cyber Kill Chain

***Note**:* Threat actor refers to the party instigating the attack. However, Lockheed Martin uses the term "adversary" in Cyber Kill Chain. Therefore, the terms adversary and threat actor are used interchangeably in this topic.

Reconnaissance

- Reconnaissance is when the threat actor performs research, gathers intelligence, and selects targets.
- The threat actor will choose targets that have been **neglected** *(zanedbané)* or **unprotected** because they will have a higher likelihood of becoming **penetrated** and **compromised**.
- The table summarizes the tactics and defenses used during the reconnaissance step.

Adversary Tactics	SOC Defences
Plan and conduct research: • Harvest *(zozbieraj)* email addresses • Identify employees on social media • Collect all public relations information (press releases, awards, conference attendees and so on) • Discover internet-facing servers • Conduct scans of the network to identify IP addresses and open ports	Discover adversary's intent: • Web log alerts and historical searching data • Data mine browser analytics • Build playbooks for detecting behavior that indicate recon activity • Prioritize defense around technologies and people that reconnaissance activity is targeting

The Cyber Kill Chain

Weaponization

- Weaponization uses the information from reconnaissance **to develop** a **weapon** against specific **targeted systems or individuals** in the organization.
- It is often more effective to use a **zero-day attack** to avoid detection methods.
  - A zero-day attack uses a weapon that is unknown to defenders and network security systems.
- The table summarizes the tactics and defenses used during the weaponization step.

Adversary Tactics	SOC Defence
Prepare and stage the operation: • Obtain an automated tool to deliver the malware payload (weaponizer) • Select or create a document to present to the victim. • Select or create a backdoor and command and control infrastructure.	**Detect and collect weaponization artifacts:** • Ensure that IDS rules and signatures are up to date. • Conduct full malware analysis. • Build detections for the behavior of known weaponizers. • Is malware old, “off the shelf” or new malware that might indicate a tailored attack *(na mieru šitý)*? • Collect files and metadata for future analysis. • Determine which weaponizer artifacts are common to which campaigns.

Delivery

- During this step, the weapon is transmitted to the target using a **delivery vector**
  - If the weapon is not delivered, the attack will be unsuccessful.
- The threat actor will use different methods to increase the odds
  (aby zväčšil pravdepodobnosť)
  of delivering the payload such as:
  - encrypting communications
  - making the code look legitimate
  - obfuscating *(zahmlievanie)* the code
- Security sensors are so advanced that they can detect the code as malicious unless it is **altered** to avoid detection.
- The table summarizes the tactics and defenses used during the delivery step.

Adversary Tactics	SOC Defence

Launch malware at target:
• Direct against web servers
• Indirect delivery through:
  • Malicious email
  • Malware on USB stick
  • Social media interactions
  • Compromised websites
	Block delivery of malware:
	• Analyze the infrastructure path used for delivery.
	• Understand targeted servers, people, and data available to attack.
	• Infer intent of the adversary based on targeting.
	• Collect email and web logs for forensic reconstruction.

Exploitation

- After the weapon has been delivered, the threat actor uses it to break the vulnerability and gain control of the target.
- The most common exploit targets are applications, operating system vulnerabilities, and users.
- The table summarizes the tactics and defenses used during the exploitation step.

Adversary Tactics	SOC Defence
Exploit a vulnerability to gain access: • Use software, hardware, or human vulnerability • Acquire or develop the exploit • Use an adversary-triggered exploit for server vulnerabilities • Use a victim-triggered exploit such as opening an email attachment or malicious web link	Train employees, secure code, and harden devices: • Employee security awareness training and periodic email testing • Web developer training for securing code • Regular vulnerability scanning and penetration testing • Endpoint hardening measures • Endpoint auditing to forensically determine origin of exploit

Installation

- In the Installation step, the threat actor establishes a back door into the system to allow for continued access to the target.
- To preserve this backdoor, the remote access should not alert cyber security analysts or users. The access method must survive through antimalware scans and rebooting of the computer to be effective.
- The table summarizes the tactics and defenses used during the installation step.

Adversary Tactics	SOC Defence
Install persistent backdoor: • Install webshell on web server for persistent access. • Create point of persistence by adding services, AutoRun keys, etc. • Some adversaries modify the timestamp of the malware to make it appear as part of the operating system.	Detect, log, and analyze installation activity: • HIPS to alert or block on common installation paths. • Determine if malware requires elevated privileges or user privileges • Endpoint auditing to discover abnormal file creations. • Determine if malware is known threat or new variant.

Command and Control

- The goal is to establish Command and Control (CnC or C2) with the target system.
- Compromised hosts usually beacon out of the network to a controller on the internet.
- Threat actors use CnC channels to issue commands to the software that they installed on the target.
- The cyber security analyst must be able to detect CnC communications to discover the compromised host.

Adversary Tactics	SOC Defence
Open channel for target manipulation: • Open two-way communications channel to CNC infrastructure • Most common CNC channels over web, DNS, and email protocols • CnC infrastructure may be adversary owned or another victim network itself	Last chance to block operation: • Research possible new CnC infrastructures • Discover CnC infrastructure though malware analysis • Isolate DNS traffic to suspect DNS servers, especially Dynamic DNS • Prevent impact by blocking or disabling CnC channel • Consolidate the number of internet points of presence • Customize rules blocking of CnC protocols on web proxies

- The table summarizes the tactics and defenses used during command and control step.

The Cyber Kill Chain

Actions on Objectives

- Actions on Objectives is the final step of the Cyber Kill Chain that describes the threat actor achieving their original objective.
- At this point, the threat actor is deeply rooted in the systems of the organization, hiding their moves and covering their tracks.
- It is extremely difficult to remove the threat actor from the network.
- The table summarizes the tactics and defenses used during the actions on objectives step.

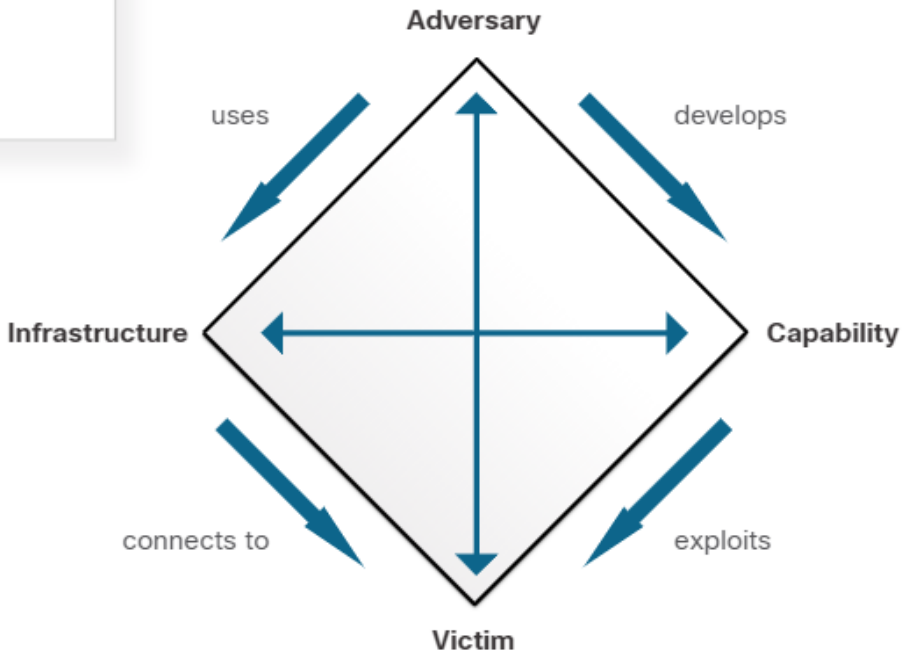
Adversary Tactics	SOC Defence
Reap the rewards *(získať odmenu za)* of successful attack: • Collect user credentials • Privilege escalation • Internal reconnaissance • Lateral movement through environment • Collect and exfiltrate data • Destroy systems • Overwrite, modify, or corrupt data	Detect by using forensic evidence: • Establish incident response playbook • Detect data exfiltration, lateral movement, and unauthorized credential usage • Immediate analyst response for all alerts • Forensic analysis of endpoints for rapid triage • Network packet captures to recreate activity • Conduct damage assessment

28.3 The Diamond Model of Intrusion Analysis

Diamond Model Overview

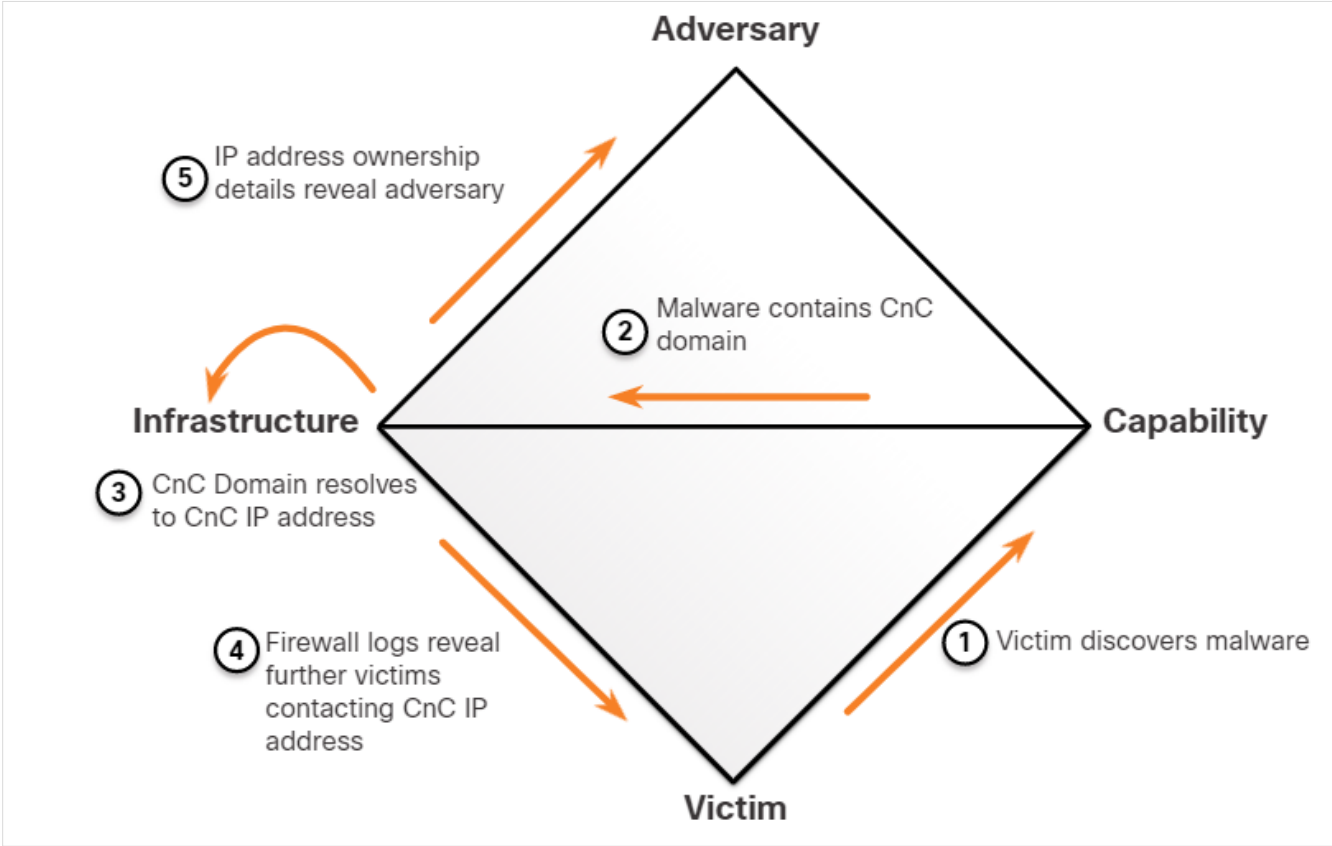
- The Diamond Model of Intrusion Analysis represents a security incident or event.
- The four core features of an intrusion event are:
  - **Adversary** - Parties responsible for the intrusion.
  - **Capability** - Tool or technique used by the adversary to attack the victim.
  - **Infrastructure** – Network path(s) used by the adversary to establish and maintain command and control over their capabilities.
  - **Victim** – Target of the attack.
- Meta-features expand the model slightly to include the important elements: **Timestamp**, **Phase**, **Result**, **Direction**, **Methodology**, and **Resources**

Meta-Features
- Timestamp
- Phase
- Result
- Direction
- Methodology
- Resources



Pivoting Across the Diamond Model

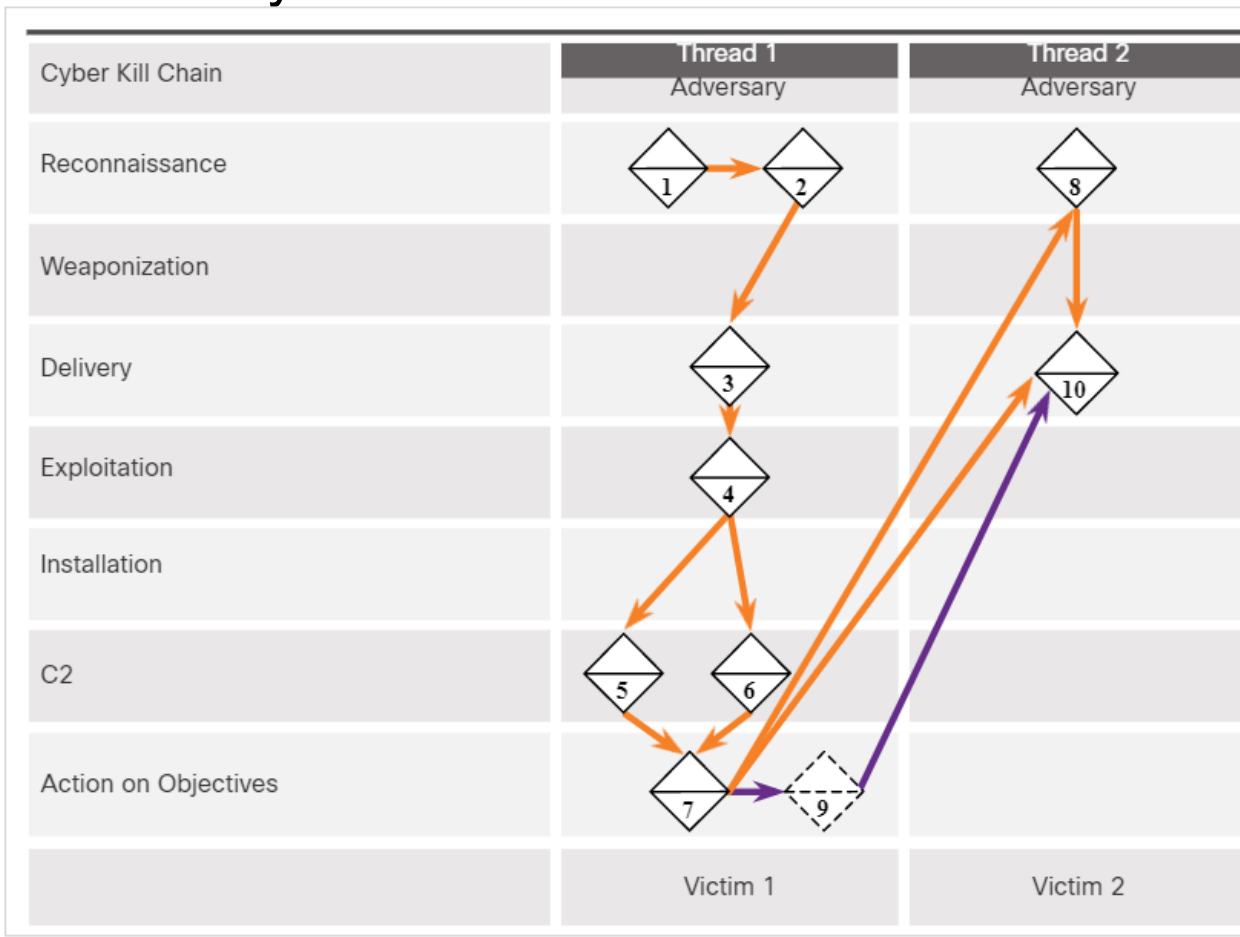
- The Diamond Model is ideal for illustrating how the adversary *(protivník)* pivots from one event to the next. For example:
  - An employee reports that his computer is acting abnormally. A host scan by the security technician indicates that the computer is infected with malware.
  - An analysis of the malware reveals that the malware contains a list of CnC domain names that resolve to a list of IP addresses.
  - These IP addresses are used to identify the adversary and investigate logs to determine if other victims in the organization are using the CnC channel.



Diamond Model Characterization of an Exploit

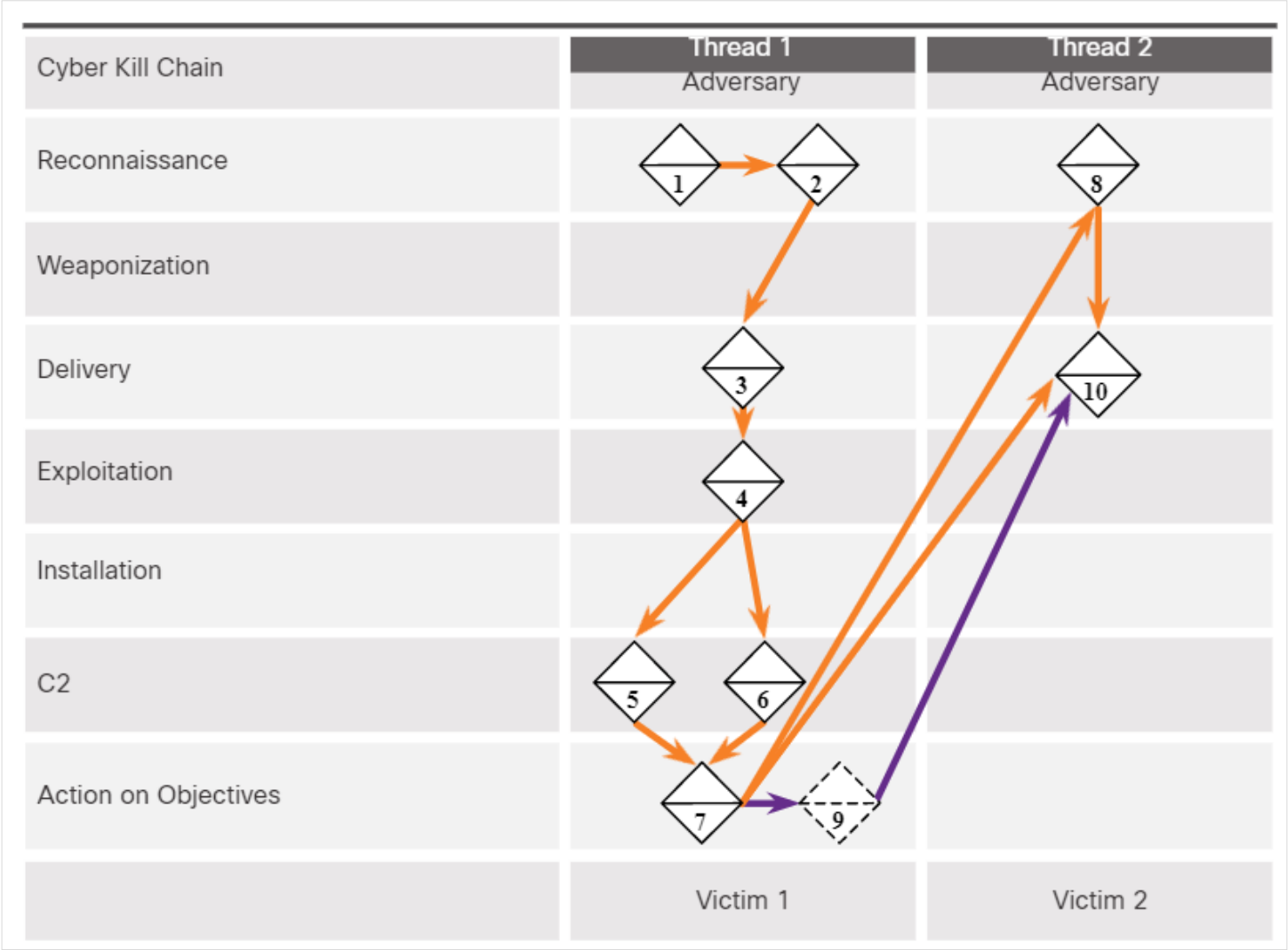
The Diamond Model and the Cyber Kill Chain (Contd.)

- Events are threaded together in a chain in which each event must be completed before the next event. This thread of events can be mapped to the Cyber Kill Chain.
- The example illustrates the end-to-end process of an adversary as they traverse the Cyber Kill Chain:
  - Adversary conducts a web search for victim company Gadgets, Inc. receiving as part of the results the domain name gadgets.com.
  - Adversary search “network administrator gadget.com” and discovers forum postings from users claiming to be network administrators of gadget.com and the profiles reveal their email addresses.
  - Adversary sends phishing emails with a Trojan horse attached to the network administrators.



The Diamond Model and the Cyber Kill Chain (Contd.)

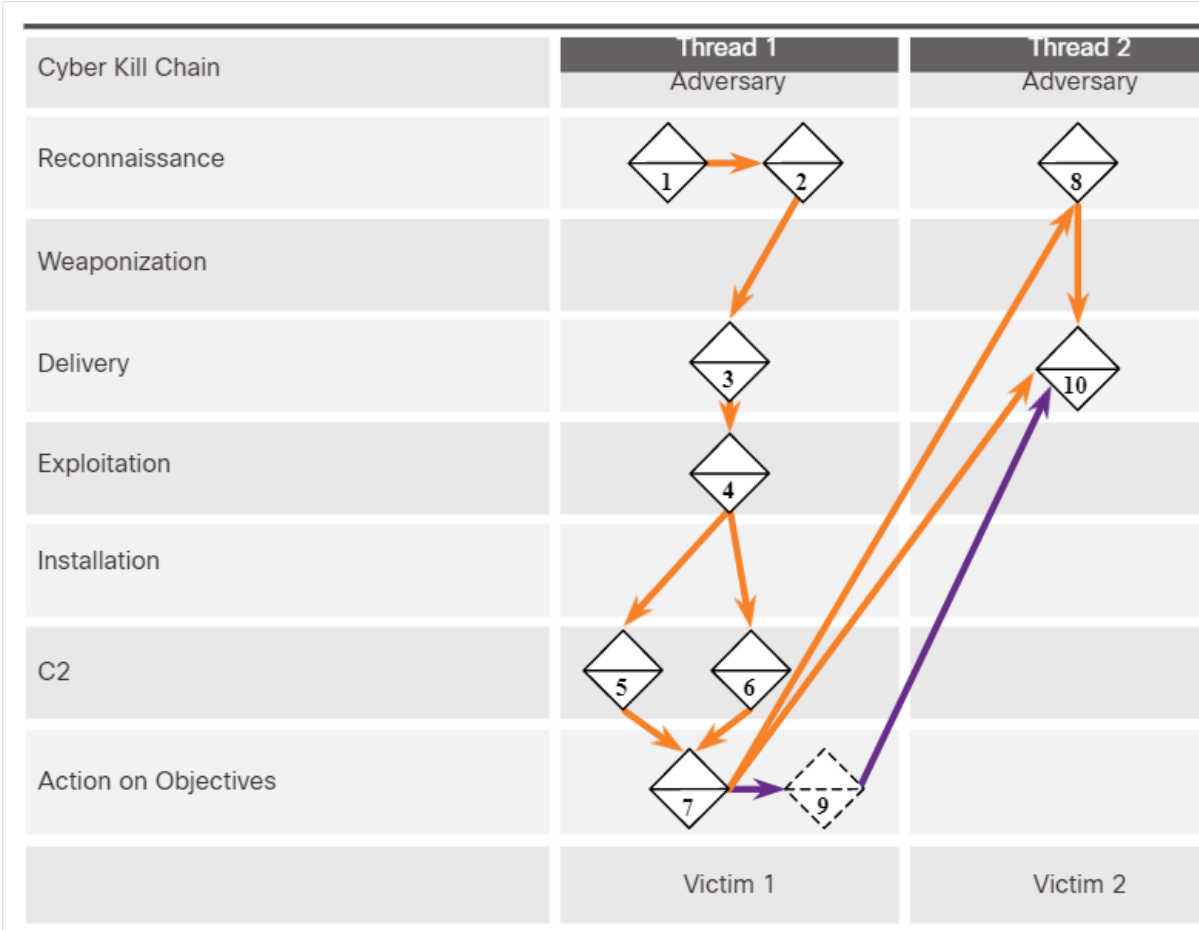
- One network administrator (NA1) opens the malicious attachment which executes the enclosed exploit.
- NA1's host registers with a CnC controller by sending an HTTP Post message and receiving an HTTP Response in return.
- It is revealed from reverse engineering that the malware has additional backup IP addresses.
- Through a CnC HTTP response message sent to NA1's host, the malware begins to act as a proxy for new TCP connections.



The Diamond Model and the Cyber Kill Chain (Contd.)

- Through information from the proxy that is running on NA1's host, Adversary searches the web for "most important research ever" and finds Victim 2, Interesting Research Inc.
- Adversary checks NA1's email contact list for any contacts from Interesting Research Inc. and discovers the contact for the Interesting Research Inc. Chief Research Officer.
- Chief Research Officer of Interesting Research Inc. receives a spear-phish email from Gadget Inc.'s NA1's email address sent from NA1's host with the same payload as observed in Event 3.

- The adversary now has two compromised victims from which additional attacks can be launched.

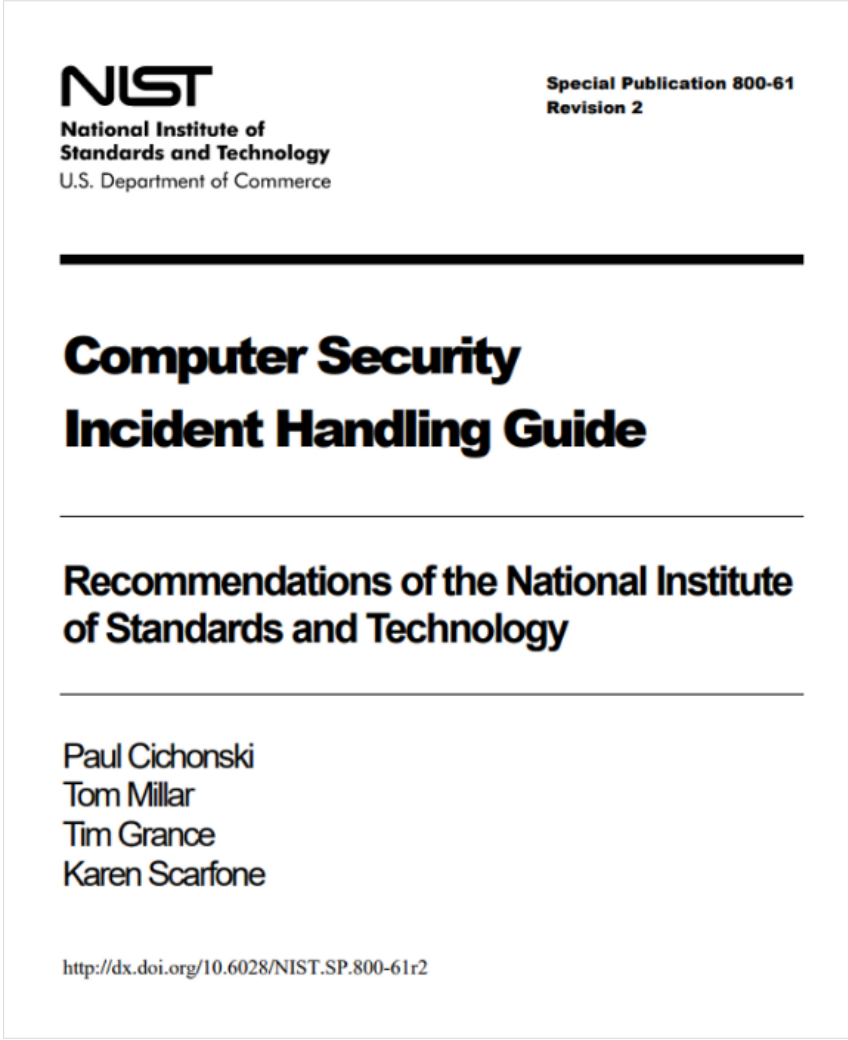


28.4 Incident Response

Establishing an Incident Response Capability

- Incident response aims to limit the impact of the attack, assess the damage caused, and implement recovery procedures.
- Incident Response involves the methods, policies, and procedures that are used by an organization to respond to a cyber attack.

***Note**: Although this chapter summarizes the content in the NIST 800-61r2 standard, you should be familiar with the entire publication as it covers four major exam topics for the Understanding Cisco Cybersecurity Operations Fundamentals exam.*


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

Establishing an Incident Response Capability (Contd.)

- The below table summarizes the policy, plan and procedure elements in an incident response:

Policy Elements	Plan Elements	Procedure Elements
• Statement of management commitment • Purpose and objectives of the policy • Scope of the policy • Definition of computer security incidents and related terms • Organizational structure and definition of roles, responsibilities, and levels of authority • Prioritization of severity ratings of incidents • Performance measures • Reporting and contact forms	• Mission • Strategies and goals • Senior management approval • Organizational approach to incident response • How the incident response team will communicate with the rest of the organization and with other organizations • Metrics for measuring the incident response capacity • How the program fits into overall organization	• Technical processes • Using techniques • Filling out forms • Following checklists

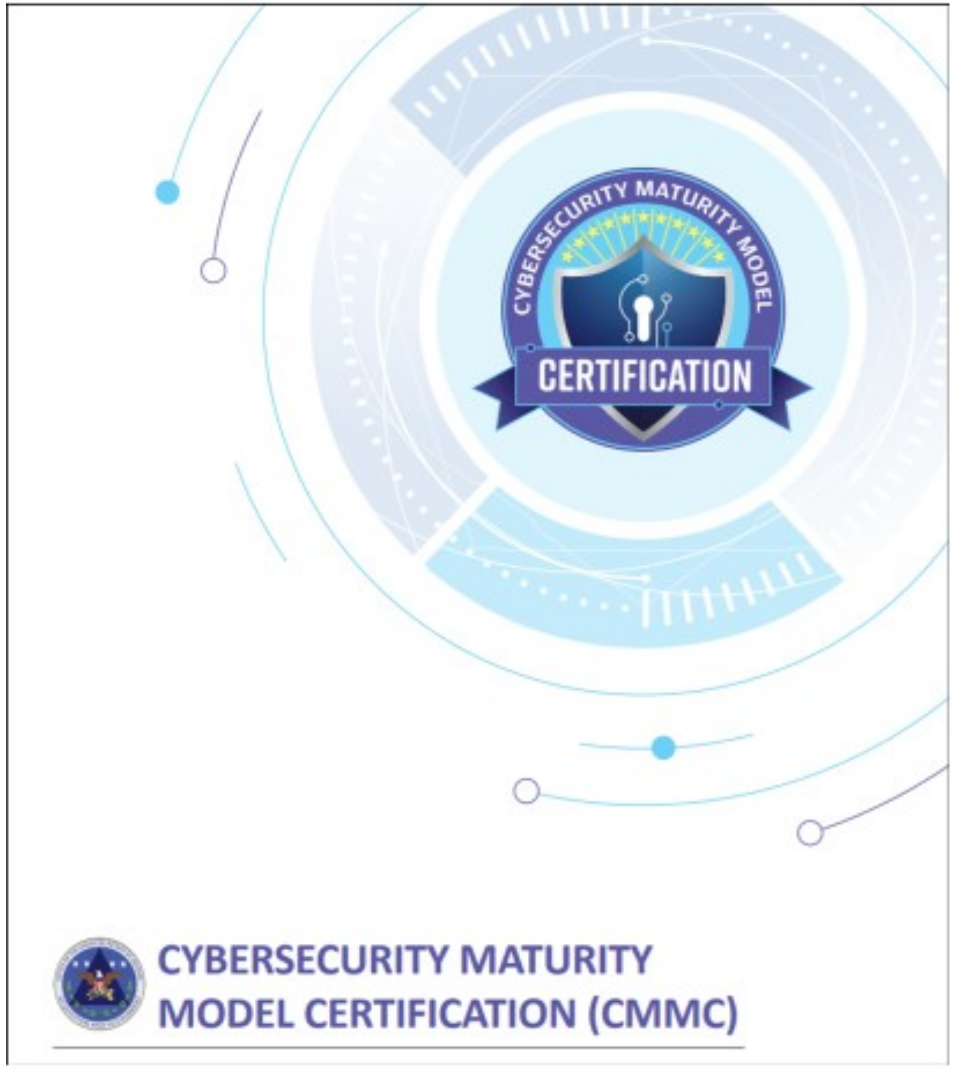
Incident Response Stakeholders

- The stakeholders involved in handing a security incident are as follows:
  - Management
  - Information Assurance
  - IT Support
  - Legal Department
  - Public Affairs and Media Relations
  - Human Resources
  - Business Continuity Planners
  - Physical Security and Facilities Management

Incident Response Stakeholders (Contd.)

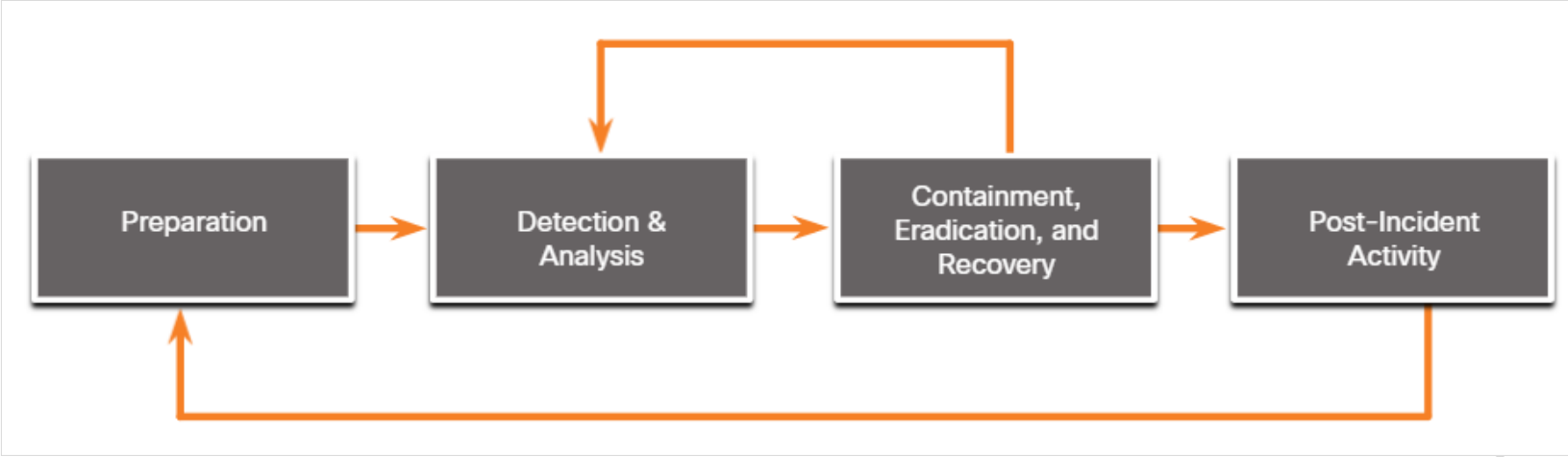
The Cybersecurity Maturity Model Certification (CMMC)

- The CMMC certifies organizations by level. For most domains, there are five levels, however for incident response, there are only four:
  - **Level 2 -** Establish an incident response plan that follows the NIST process.
  - **Level 3** - Document and report incidents to stakeholders identified in the incident response plan.
  - **Level 4 -** Use knowledge of attacker TTP to refine incident response planning and execution.
  - **Level 5 -** Utilize accepted and systematic computer forensic data gathering techniques.



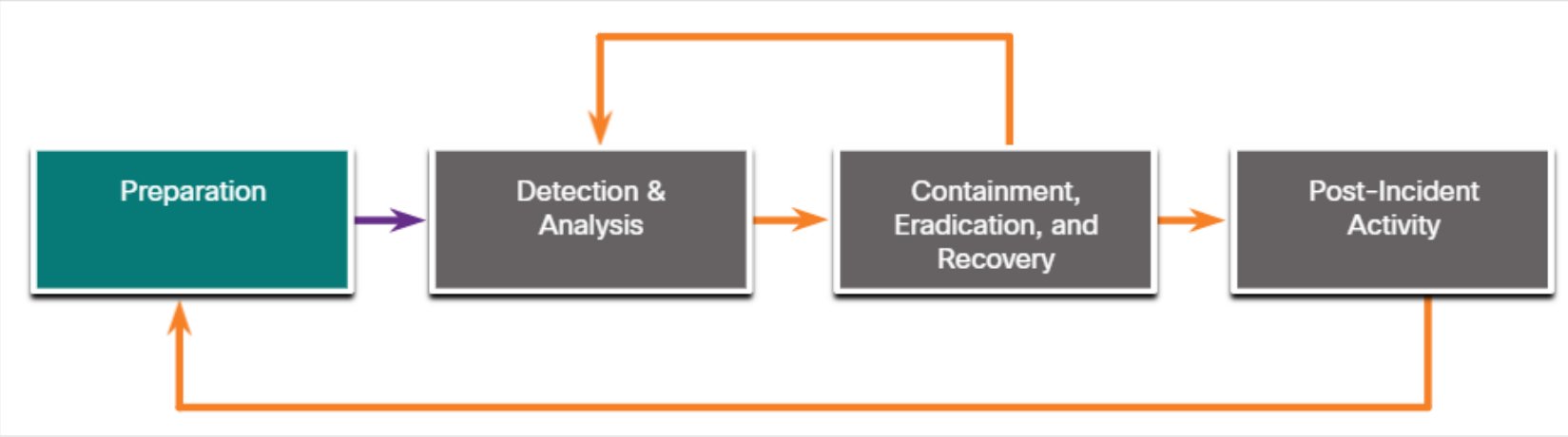
NIST Incident Response Life Cycle

- NIST defines four steps in the incident response process life cycle:
  - **Preparation -** The members of the CSIRT are trained in how to respond to an incident.
  - **Detection and Analysis** – CSIRT quickly identifies, analyzes, and validates an incident.
  - **Containment, Eradication, and Recovery** – CSIRT implements procedures to contain the threat, eradicate the impact on organizational assets, and use backups to restore data and software.
  - **Post-Incident Activities** – CSIRT documents how the incident was handled, recommends changes for future response, and specifies how to avoid a reoccurrence.



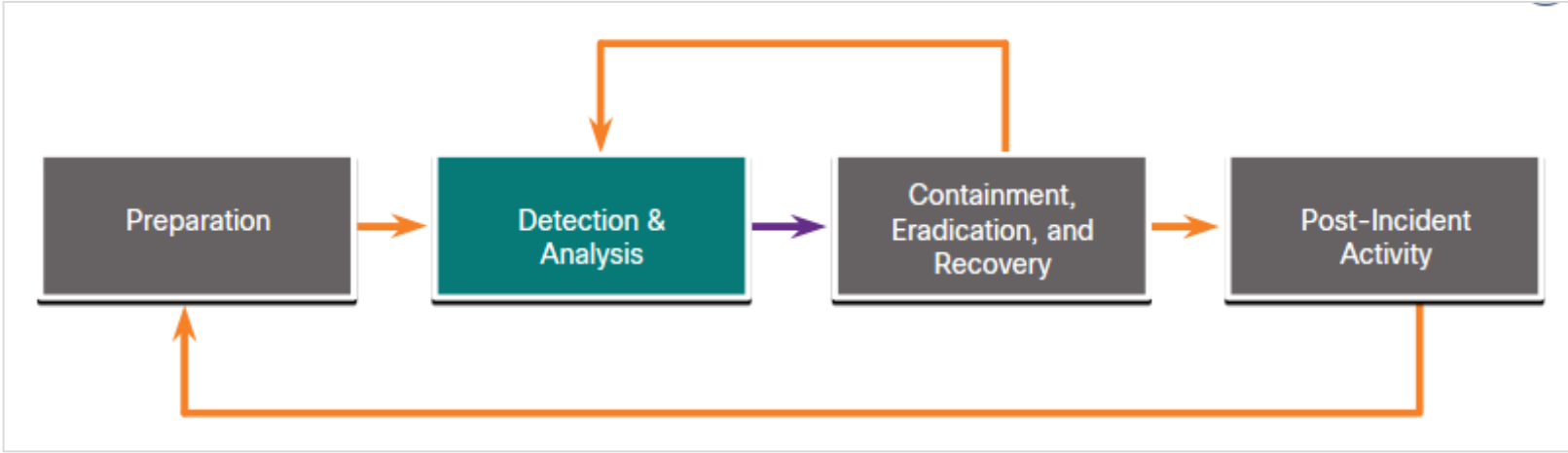
Preparation

- The preparation phase is when the CSIRT is created and trained. The tools and assets that will be needed by the team to investigate incidents are acquired and deployed.
- The examples of actions in the preparation phase are as follows:
  - Facilities to host the response team and the SOC are created.
  - Risk assessments are used to implement controls that will limit the number of incidents.
  - User security awareness training materials are developed.
  - Necessary hardware and software for incident analysis and mitigation is acquired.



Detection and Analysis

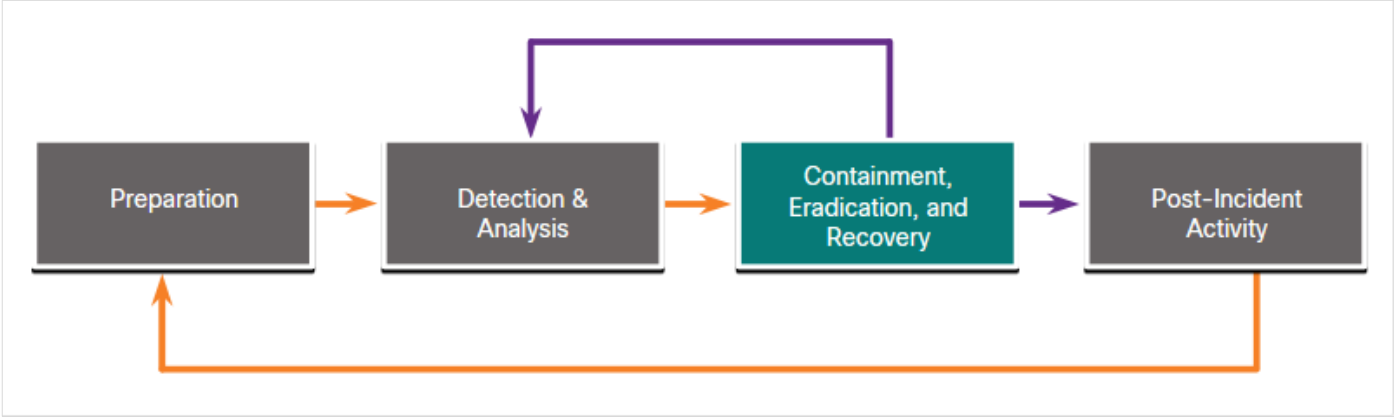
- Different types of incidents will require different responses.
  - **Attack Vectors**: Web, Email, Loss or Theft, Impersonation, Attrition and Media.
  - **Detection:** Automated detection - Antivirus software, IDS, manual detection - user reports.
  - **Analysis**: Use Network and System Profiling to determine the validity of security incidents.
  - **Scoping**: Provide information on the containment of the incident and deeper analysis of the effects of the incident.
  - **Incident Notification**: Notify appropriate stakeholders and outside parties, once the incident is analyzed and prioritized,



Containment, Eradication, and Recovery

- After determining the validity of the incident through detection and analysis, it must be contained.
  - **Containment Strategy**: For every type of incident, a containment strategy should be created and enforced depending on some conditions.
  - **Evidence**: During an incident, evidence must be gathered to resolve it. It is required for subsequent investigation by authorities.
  - **Attacker Identification**: Identifying attackers will minimize the impact on critical business assets and services.

- **Eradication, recovery, and remediation**: to eradicate, identify all hosts that need remediation; to recover hosts, use clean and recent backups, or rebuild them with installation media.

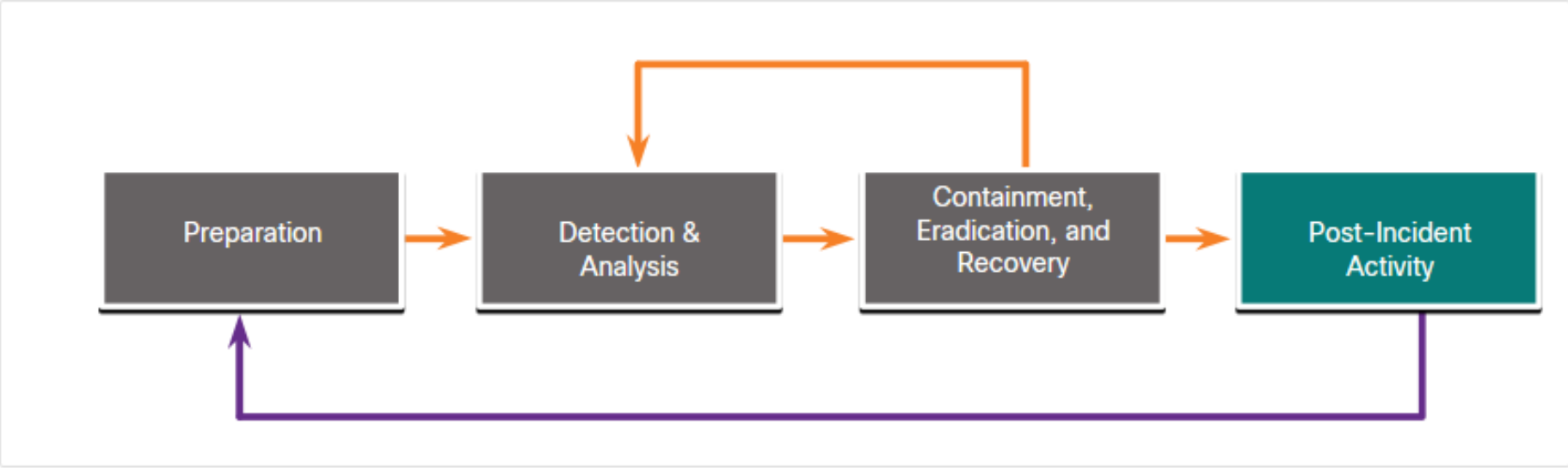


Post-Incident Activities

- It is important to periodically meet with all the parties involved to discuss the events that took place and the actions of all of the individuals while handling the incident.

  Lessons-based hardening:

  - The organization should hold a “lessons learned” meeting to:
    - Review the effectiveness of the incident handling process.
    - Identify necessary hardening needed for existing security controls and practices.



Incident Data Collection and Retention

- The below table summarizes the incident data collection and retention:

Incident Data Collection	Retention

• The collected data after the lessons-learned meeting can be used to:
  • Determine the incident cost for budgeting
  • Determine the effectiveness of the CSIRT
  • Identify possible security weaknesses throughout the system
• The time of each incident provides an insight into the total amount of labor used and the total time of each phase of the incident response process.
• Only collect data that can be used to define and refine the incident handling process.
• Perform an objective assessment of each Incident.
	Some of the determining factors for evidence retention:
	• **Prosecution** - When an attacker will be prosecuted because of a security incident, the evidence should be retained until after all legal actions have been completed.
	• **Data Type** - An organization may specify that specific types of data should be kept for a specific period of time.
	• **Cost** - If there is a lot of hardware and storage media that needs to be stored for a long time, it can become costly.

Reporting Requirements and Information Sharing

- Governmental regulations should be consulted by the legal team to determine the organization's responsibility for reporting the incident.
- Management needs to determine what additional communication is necessary with other stakeholders, such as customers, vendors, partners and so on.
- NIST recommends that an organization coordinate with organizations to share details for the incident. The critical recommendations from NIST for sharing information are as follows:
  - Plan incident coordination with external parties before incidents occur.
  - Consult with the legal department before initiating any coordination efforts.
  - Perform incident information sharing throughout the incident response life cycle.
  - Attempt to automate as much of the information sharing process as possible.
  - Balance the benefits of information sharing with the drawbacks of sharing sensitive information.

28.5 Digital Forensics and Incident Analysis and Response Summary

What Did I Learn in this Module?

- Digital forensics is the recovery and investigation of information found on digital devices as it relates to criminal activity.
- Indicators of compromise are the evidence that a cyber security incident has occurred.
- The forensic process includes four steps: collection, examination, analysis, and reporting.
- In legal proceedings, evidence is broadly classified as direct, indirect, best evidence and corroborating evidence.
- Threat attribution refers to the act of determining the individual, organization, or nation responsible for a successful intrusion or attack incident.
- In an evidence-based investigation, the incident response team correlates Tactics, Techniques, and Procedures (TTP) that were used in the incident with other known exploits.

What Did I Learn in this Module?

- The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Framework enables the ability to detect attacker tactics, techniques, and procedures (TTP) as part of threat defense and attack attribution.
- The Cyber Kill Chain was developed to identify and prevent cyber intrusions.
- The steps in the Cyber Kill Chain are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.
- The Diamond Model of Intrusion Analysis represents a security incident or event.
- The four core features of an intrusion event are adversary, capability, infrastructure and victim.
- Incident Response involves the methods, policies, and procedures that are used by an organization to respond to a cyber attack.

UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Ďakujem za pozornosť

Obsahom boli moduly:

Chapter 27 Working with Network Security Data (Security Onion and ELK)
Chapter 28 Digital Forensics and Incident Analysis and Response

Vyjadrite spätnú väzbu na prednášku a/alebo cvičenie v anonymnej ankete cez google form: link

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.