

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**

W e e k	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

W ee k	CyberOps Modules in Lectures	Exam from:
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
1 0	Chapter 27 Working with Network Security Data (Security Onion and ELK) Chapter 28 Digital Forensics and Incident Analysis and Response	24-25
1 1	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



Introduction Chapter 11



# 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



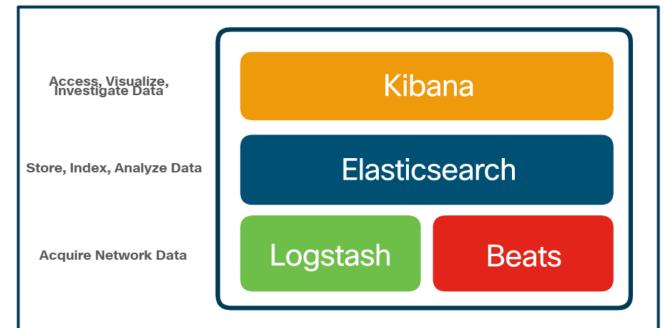
### A Common Data Platform

# 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

		ogstas	sh	CSV File
Log File Twitter	Input	Filter	Output	Elasticsearch Message Queue
<b>P</b>	Vstupné	Filtračné	Výstupné	
STDIN	Beats	grok	ТСР	Email
	súbor	JSON	stdout	
	HTTP	GeoIP	súbor	
	Kafka	xml	email	
	Syslog		Elasticsearch	. Cisco 8



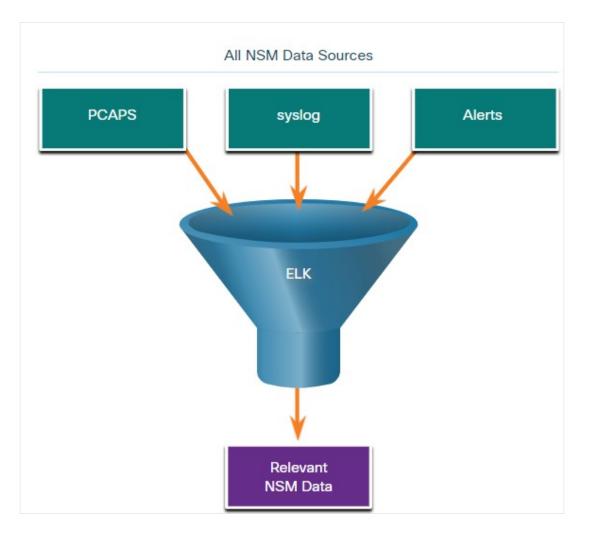
# Logstash – plugin Beats – FileBetas and others...

- 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

# A Common Data Platform 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.



# A Common Data Platform 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.

# A Common Data Platform 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 <u>specified by</u> 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

Search										Search 📀
All (care	eful) Bound	ng Last Packet	Time Range: 1	7247 days 09:09:31						
,000			Q Q < :	Session Packe	ts Databytes		. 1 1			
0 1969/12/3 19:00:00	) 19:00:0		19:00:00	1989/12/31 19:00:00 1 - 50 of 60,958 entries	19:00:00 1	99/12/31 9:00:00		009/12/31 19:00:00	2	
	▲ Start Time	Stop Time	Src IP / Country	⇒ Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	⇒ Moloch Node	Info
udp	1969/12/31 19:00:00	1969/12/31 19:00:00	1.1.1.1	10000	2.2.2.2	2948	1	437 445	demo	
udp	1970/01/01 00:18:25	1970/01/01 00:18:37	1.1.1.1	623	2.2.2.2	623	1,138	74,094 83,198	demo	
udp	1970/01/01 00:21:32	1970/01/01 00:22:24	1.1.1.1	623	2.2.2.2	623	726	46,615 52,423	demo	
udp	1970/01/04 02:44:00	1970/01/04 02:44:06	192.85.1.2	1024	192.0.0.1	3784	31	2,666 2,914	demo	
udp	1970/01/04 03:23:35	1970/01/04 03:23:40	192.85.1.2	1024	192.0.0.1	3784	25	2,250 2,450	demo	
udp	1970/01/06 10:54:23	1970/01/06 10:54:26	192.85.1.2	1024	192.0.0.1	3784	15	1,065 1,185	demo	
udp	1970/07/21 16:01:41	1970/07/21 16:05:14	10.0.2.148	31656	10.0.2.28	48140	8,957	717,193 788,849	demo	
udp	1970/07/21 16:01:44	1970/07/21 16:05:13	10.0.2.148	31657	10.0.2.28	48141	43	4,018 4,362	demo	
udp	1999/03/11 08:45:02	1999/03/11 08:45:02	3ffe:507:0:1:200:86ff fe05:80da	f: 2396	3ffe:501:4819:0:0:0:0 :42	53	2	584 600	demo	coconut.itojun.org itojun.org kiwi.itojun.o

Id: 990311-eBTgyga-eBpP34R1k3OxvIsG

Protocols: udp dns

Start: 1999/03/11 08:45:02 Stop: 1999/03/11 08:45:02 Node: demo IP Protocol: udp

Src: Packets 1 Bytes 90 Databytes 82 Dst: Packets 1 Bytes 510 Databytes 502

Ethernet: Src Mac 00:00:86:05:80:da Dst Mac 00:60:97:07:69:ea

Src IP/Port: [3ff:e:50:7:::1:20::86:ff:f:e05::80da:] : 2396

Dst IP/Port: [3ffe:501:4819::42] : 53

Payload8: src 0006010000010000 ( 00000 ) Dst 0006858000010006 ( 00000 )

ılıılı cisco

### A Common Data Platform 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



## 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 <u>correlates</u> similar alerts <u>into a single line</u> 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 <u>sort</u> the CNT column to display the alerts with the highest frequency.

							SGUIL-0.9	0 - Connected	To localhost								-	
ile Qui	ny <u>R</u> epor	ts Sound: Off	ServerN	lame: localhos	t UserNan	ne: analyst Use	riD: 2									2020-	05-29 20	:06:11 G
RealTin	e Events	Escalated Eve	ents	7.1998	Event Qu	ery 1												
ST	7 CNT	Sensor	Alert ID	Date	Time	Src IP	SPor	t Dst IP	DPort	Pr	Event M	essage						
RT	1059	seconion	1.3	2020-04-2	9 15:26:36	0.0.0.0		0.0.00		0	OSSEC	Received	10 packet	ts in desig	gnated tim	e interval	(defined	in os
RT	881	seconion	1.2	2020-04-2	9 15:22:36	0.0.0.0		0.0.00		0	OSSEC	] Listened	ports stat	tus (netst	at) change	ed (new po	ort opene	d or c.
RT	647	seconion	7.1	2020-04-2	9 16:08:59	209.165.201.1	7	209.165.201.2	1	1	GPL ICM	AP_INFO P	PING "NIX	(				
RT	/iew Corre	lated Events	5.1	2020-04-2	9 16:55:12	209.165.201.1	7	209.165.200.2	35	1	GPL ICM	INFO F	PING *NIX	<				
RT	296	seconion	5.792	2020-05-1	0 21:20:28	209.165.201.1	7 5220	6 209.165.200.2	35 80	6	ET WEB	SERVER	Script ta	g in URI I	Possible (	Cross Site	Scriptin	g Atte.
RT	296	seconion	7.1105	2020-05-1	0 21:20:28	209.165.201.1	7 5220	6 209.165.200.2	35 80	6	ET WEB	SERVER	Script ta	g in URI I	Possible (	Cross Site	Scriptin	g Atte
RT	252	seconion	3.1	2020-04-2	9 16:44:19	192.168.0.11		192.168.0.1		1	GPL ICM	INFO P	PING *NIX	(				
RT	123	seconion	5.466	2020-05-1	0 21:20:26	209.165.201.1	7 5217	4 209.165.200.2	35 80	6	ET WEB	SERVER	Possible	CVE-20	14-6271 A	ttempt		
RT	123	seconion	5.467	2020-05-1	0 21:20:26	209.165.201.1	7 5217	4 209.165.200.2	35 80	6	ET WEB	SERVER	Possible	CVE-20	14-6271 A	ttempt in I	Headers	
RT	123	seconion	7.779	2020-05-1	0 21:20:26	209.165.201.1	7 5217	4 209.165.200.2	35 80	6	ET WEB	SERVER	Possible	CVE-20	14-6271 A	ttempt		
RT	123	seconion	7.780	2020-05-1	0 21:20:26	209.165.201.1	7 5217	4 209.165.200.2	35 80	6	ET WEB	SERVER	Possible	CVE-20	14-6271 A	ttempt in	Headers	
RT	76	seconion	7.691	2020-05-1	0 21:20:25	209.165.201.1	7 5215	8 209.165.200.2	35 80	6	ET INFO	Executab	le Downio	ad from a	dotted-qua	d Host		
RT	76	seconion	5.378	2020-05-1	0 21:20:25	209.165.201.1	7 5215	8 209.165.200.2	35 80	6	ET INFO	Executab	le Downlo	ad from a	dotted-qua	d Host		
87	66	seconion-	7 1672	2020-05-1	0 21-20-52	209 165 201 1	7 5220	4 209 165 200 2	175 80	6	FT WER	SERVER	Evolait 9	Susnerter	I DHD Inia	ection Atta	ack /cm/	1=1
	`		~	\ \			Show F	Packet Data 🗟 Sh	ow Rule									
IP Re	solution	Agent Status	Snort St	atistics Sys	em Msgs	User Msgs	alert icmp	SEXTERNAL_NET	any -> \$HOM	E_NET	any (msg	"GPL ICM	P_INFO P	PING *ND	X"; itype:8	; content:	" 10 11 1	2 13 1
Reve	rse DNS	Enable Exter	nal DNS				15 16 17 1	8 19 1A 1B 1C 1D	1E 1FF; depth	:32; cla	asstype:mi	sc-activity	sid:2100	366; rev:	8; metada	ta:created	_at 2010	0_09_2
rc IP:							1D	Source IP	Dest	IP	Ver	HL TOS	len	ID	Flags	Offset	TTL	ChkS
rc Nan	ie:							209.165.201.17	209.165.20	1.21	4 5	0	84	13326	2	0	64	53544
st IP:							ICMP	т	ype		Code		ChkSum		ID		Seq	#
st Nan	ie:							8			0	2368		111		1		
hois Q	uery: 🔹 I	None C Src IP	O Dst I	P				03 A5 A9 5E 0 10 11 12 13 1							^	.SN		
								20 21 22 23 2	4 25 26 27						!"#\$%8	'()*+,-	./	
							DATA	30 31 32 33 3	4 35 36 37						0123456	57		
								s	earch Packet	Pavloa	1 C He	e 🖲 Text	□ NoCa	se				

#### Sguil Alerts Sorted on CNT

# Investigating Network Data 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 <u>names</u> and some issues with field <u>values</u> to effectively build queries in Sguil.
- For example, Sguil stores
   IP addresses in an integer representation.

	Barrate Co	and off from the	In calls and a	in a shi na sa			Connected To localh	051						2007	07 10 34	
e g	uery <u>R</u> eports So	und: Off ServerNam	e localhost u	JserName: an	alyst UserID:	2								2017-	07-19 21	:06:12 (
RealT	ime Events Escalat	ed Events Event Qu	ery 9													
Clos Expo	event.src_port		.signature_ge	n, event.signa	ture_id, event		.sid, event.cid, event.si v FROM event IGNORE								RE	Subr Edi
ST	CNT Sensor	Alert I	D Da	te/Time	Src IP	SPO	t Dst IP	DPort	Pr	Event Message						
RT	1 seconion-	eth1-1 5.521	2017-07	-05 18:38:29	209.165.201.	17 4075	4 209.165.200.235	80	6	ET SCAN Nmap Scrip	ting Engine U	Jser-Agen	t Detecte	ed (Nmap S	Scripting	Engin
RT	1 seconion-	eth1-1 5.522	2017-07	405 18:38:29	209.165.201.	17 4075	4 209.165.200.235	80	6	ET SCAN NMAP SQL	Spider Scan					
RT	1 seconion-	eth1-1 5.523	2017-07	-05 18:38:29	209.165.201.	17 4075	4 209.165.200.235	80	6	ET SCAN Possible Nr	nap User-Age	int Obser	ved			
RT	1 seconion-	eth2-1 7.587	2017-07	-05 18:38:29	209.165.201.	17 4075	4 209.165.200.235	80	6	ET SCAN Nmap Scrip	ting Engine U	Jser-Agen	t Detecte	ed (Nmap S	Scripting	Engin
RT	1 seconion-	eth2-1 7.588	2017-07	-05 18:38:29	209.165.201.	17 4075	4 209.165.200.235	80	6	ET SCAN NMAP SQL	Spider Scan					
RT	1 seconion-	eth2-1 7.589	2017-07	-05 18:38:29	209.165.201.	17 4075	4 209.165.200.235	80	6	ET SCAN Possible Nn	hap User-Age	nt Obser	ved			
									_							
			ics) System I	-	r Msgs	alert tcp \$E	acket Data 🖙 Show Re XTERNAL_NET any → St	HTTP_SERVE								serve
	Net	Hostname	Туре	Las	4	alert tcp \$E content:"G	XTERNAL_NET any -> \$1 ET"; http_method; con	HTTP_SERVI	lspide	er"; http_uri; reference:	url,nmap.org	g/nsedoc	/scripts/s	sql-injection	n.html;	_
	Net seconion-ossec	Hostname seconion-ossec	Type ossec	Las 2017-07-19	21:05:17	alert tcp \$E content:"G	XTERNAL_NET any -> \$I ET"; http_method; con Source IP	HTTP_SERVI tent:" OR so Dest II	įlspide P	er"; http_uri; reference: Ver HL TOS	url,nmap.org len	g/nsedoc. ID	/scripts/s Flags	offset	n.html; TTL	ChkS
Sid 1 2	Net seconion-ossec seconion-eth0	Hostname seconion-ossec seconion-eth0	Type ossec pcap	Las	21:05:17	alert tcp \$E content:"G	XTERNAL_NET any -> \$I ET"; http_method; con Source IP	HTTP_SERV tent:" OR so Dest II 09.165.200.	alspide P 235	Ver HL TOS	url,nmap.org len	g/nsedoc ID	/scripts/s Flags	sql-injection	n.html; TTL	ChkS
	Net seconion-ossec seconion-eth0 seconion-eth0	Hostname seconion-ossec seconion-eth0 seconion-eth0-1	Type ossec pcap snort	Las 2017-07-19 2017-07-19	21:05:17 13:44:58	alert tcp \$E content:"G	XTERNAL_NET any -> Si TT"; http_method; con Source IP 209.165.201.17 20	HTTP_SERV tent:" OR so Dest II 09.165.200.	p 235 P R	Ver HL TOS	url,nmap.org len	g/nsedoc. ID	/scripts/s Flags	offset	n.html; TTL	ChkS
Sid 1 2 3	Net seconion-ossec seconion-eth0 seconion-eth1	Hostname seconion-ossec seconion-eth0 seconion-eth0-1 seconion-eth1	Type ossec pcap snort pcap	2017-07-19 2017-07-19 2017-07-19	21:05:17 13:44:58 13:45:11	alert tcp \$E content:"G IP TCP	KTERNAL_NET any -> Si TT': http_method; cont Source IP 209.165.201.17 20 Source Dest R Port Port 1	HTTP_SERV tent:" OR so Dest II 29.165.200.	e 235 P R S S	Ver HL TOS 4 5 0 5 F Y I N N Seq#	len 268 3 Ack #	g/nsedoc ID 33065 Offs	/scripts/s Flags 2 set Res	Offset 0 6 Window	n.html; TTL i3 3 v Urp	ChkS 33914 ChkS
5id 1 2 3 4	Net seconion-ossec seconion-eth0 seconion-eth0	Hostname seconion-ossec seconion-eth0 seconion-eth0-1	Type ossec pcap snort	Las 2017-07-19 2017-07-19	21:05:17 13:44:58 13:45:11 18:53:42	alert tcp \$E content:"G IP TCP	KTERNAL_NET any -> Si ET*; http_method; cont Source IP 109.165.201.17 [20] Source Dest R	U A R R C	e 235 P R S S	Ver HL TOS 4 5 0 5 F Y I N N Seq#	len 268 3	g/nsedoc ID 33065 Offs	/scripts/s Flags 2	Offset 0 6	n.html; TTL i3 3 v Urp	ChkS 33914 ChkS
5 id 1 2 3 4 5	Net seconion-ossec seconion-eth0 seconion-eth1 seconion-eth1	Hostname seconion-ossec seconion-eth0 seconion-eth0-1 seconion-eth1 seconion-eth1-1	Type ossec pcap snort pcap snort	2017-07-19 2017-07-19 2017-07-19 2017-07-05	4 221:05:17 13:44:58 13:45:11 18:53:42 13:45:22	alert tcp SE content: "G IP TCP	KTERNAL_NET any -> \$4           Source IP           009.165.201.17         20           Source Dest R         Port Port 1           10754         80         .           17         45         54         20         68         74	HTTP_SERV tent:" OR so Dest II 29.165.200. U A R C 0 G K . X 74 70 3/	P 235 P R S S H T X	Ver         HL         TOS           4         5         0           5         F         7           Y         I         N           N         Seq #         .           .         1692715185         2F           2F         54         57         69         68	len 268 3 Ack # 667712887	g/nsedoc ID 33065 0 0ffs 7 8 GE	/scripts/s Flags 2   set Res 0 T http:	Offset 0 6 Window 229 ://TWiki	n.html; TTL i3 3 v Urp	ChkS 33914 ChkS
5id 1 2 3 4 5	Net seconion-ossec seconion-eth0 seconion-eth1 seconion-eth1 seconion-eth2	Hostname seconion-ossec seconion-eth0 seconion-eth1-1 seconion-eth1-1 seconion-eth2	Type ossec pcap snort pcap snort pcap	Las 2017-07-19 2017-07-19 2017-07-19 2017-07-05 2017-07-19	4 221:05:17 13:44:58 13:45:11 18:53:42 13:45:22	alert tcp SE content:"G TCP DATA	KTERNAL_NET any -> \$i           Source IP           009.165.201.17           Source Dest R           Port Port 1           00754           80	HTTP_SERVit tent:" OR si Dest II 99.165.200. U A R R C 0 G K - X 74 70 3J 67 69 21 69 25 3I 52 25 3I 54 54 50	235 P R S S H T X . 262 0 5 74 0 2 30 0 2F	Ver         HL         TOS           4         5         0           5         F         Y           N         N         Seq #           .         1692715185         2F           2F         54         57         69         68         69           6F         70         69         63         3D         25           73         71         6C         73         70         63           31         2E         31         0D         0A         43	len 268 3 Ack # 667712887	2/nsedoco ID 33065 7 8 GE 6 C 1/ 27 de	/scripts/s Flags 2 0 T http: rg/cgi- TWiki/7 %200R%2 r& HTTF	Offset 0 6 Window 229	n.html; TTL i3 3 v Urp	Chk54 33914

# Investigating Network Data 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

-		ports Soun		ame: localhos	t UserNa	me: analyst Use	rID: 2		_		_		_		_			2020-0	6-01 17	16:3
т		Sensor	Alert ID	Date/T	me	Src IP	SPort	Dst IP	DP	ort P	r i F	vent Me	55309							
a l		seconion	5.1515	2020-05-10		209.165.201.17	52368	209.165.200.235	80	6				ER Poss	ible XX	E SYST	TEM ENTI	TY in POS	T BOD	YY.
RT	1	seconion	5.1556	2020-05-10	21:21:17	209.165.201.17	52406	209.165.200.235	80	6	G	PL WEE	B_SER	ER mo	d_gzip_	status a	access			
	6	seconion	5.1557	2020-05-10	21:21:17	209.165.201.17	52408	209.165.200.235	80	6	E	TCURR	ENT_E	VENTS	Possib	le Mage	nto Direct	ory Traver	sal Atte	mp
	1	seconion	Event History		1:21:17	209.165.201.17	52408	209.165.200.235	80	6	E	T WEB	SERVE	ER Poss	ible My	SQL SO	QLI Attemp	pt Informat	ion Sch	em
	1	seconion	Transcript		1:21:17	209.165.201.17	52408	209.165.200.235	80	6	E	TWEB	SPECI	FIC_AP	PS Pos	sible Jo	omia SQL	J Attempt		
	2	seconion	Transcript (for	ce new)	1:21:17	209.165.201.17	52408	209.165.200.235	80	6	E	TCURR	ENT_E	VENTS	Possib	le vBull	etin object	injection i	vulnerat	bility
1	9	seconion	Wireshark (force new)	100000	1:21:17	209.165.201.17	52408	209.165.200.235	80	6	E	T WEB	SPECI	FIC_AP	PS Vul	nerable	Magento /	Adminhtml	Access	5
	2	seconion	Wireshark (for NetworkMiner	ce new)	1:21:17	209.165.201.17	52408	209.165.200.235	80	6	E	TEXPL	OIT MV	Power I	OVR Sh	ell UCE				
1	1	seconion	NetworkMiner	force pour	1:21:17	209.165.201.17	52414	209.165.200.235	80	6	E	TWOR	M TheM	loon.link	sys.rou	ter 1				
1	1	seconion	Bro	(ioice new)	1:21:17	209.165.201.17	52414	209.165.200.235	80	6	E	TEXPL	OIT D-I	ink DSL	-27508	- OS C	ommand I	njection		
1	2	seconion	Bro (force new	0	1:21:17	209.165.201.17	52408	209.165.200.235	80	6	E	T CURR	ENT_E	VENTS	Possib	le vBull	etin object	injection	vulnerat	bility
	9	seconion	7.1882	2020-05-10	21:21:17	209.165.201.17	52408	209.165.200.235	80	6	E	T WEB	SPECI	FIC_AP	PS Vul	nerable	Magento /	Adminhtml	Access	5
	2	seconion	7.1891	2020-05-10	21:21:17	209.165.201.17	52408	209.165.200.235	80	6	E	TEXPL	OIT MV	Power I	OVR Sh	ell UCE				
	1	seconion.	7 1893	2020-05-10	21-21-17	209 165 201 17	52414	209 165 200 235	RN	6	F	TWOR	M TheM	Innn link		tor 1				
lid	esolution			tistics Sys	L	User Msgs	Show P	Source IP		Dest IP	2	Ver	HL	TOS	len	ID	Flags	Offset	TTL	Ch
			seconion-en	pcap		01 16:43:57	IP I	Source IP	-	Dest IP		Ver	-	105	Heri I	10	riags	Chister		-
			seconion-en	snort		12 19:13:12			U	A P	R	SF								-
-			seconion-en	pcap		01 15:36:06	тср	Source Dest R	RR	C S		YI		2						
5	seconior		seconion-en	snort	2020-05-1	12 19:13:12	1000	Port Port 1	0 G	КН		NN	Seq		Ack #	0	ITSEC Ret	s Window	Urp	G
6	seconior	ens224	seconion-en	pcap	2020-06-0	01 15:36:27						_		_			_			-
7	seconior		seconion-en	snort	2020-05-3	10 23:39:07	DATA													
			Updat	e Interval (se	cs): 15	V NOW		Ser	ich Pa	cket Pá	virunt	CH	w (# 7	ext 🗆	NoCase					_

# **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
- <u>https://sancp.sourceforge.net/</u>

## Investigating Network Data 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.

uluilu cisco

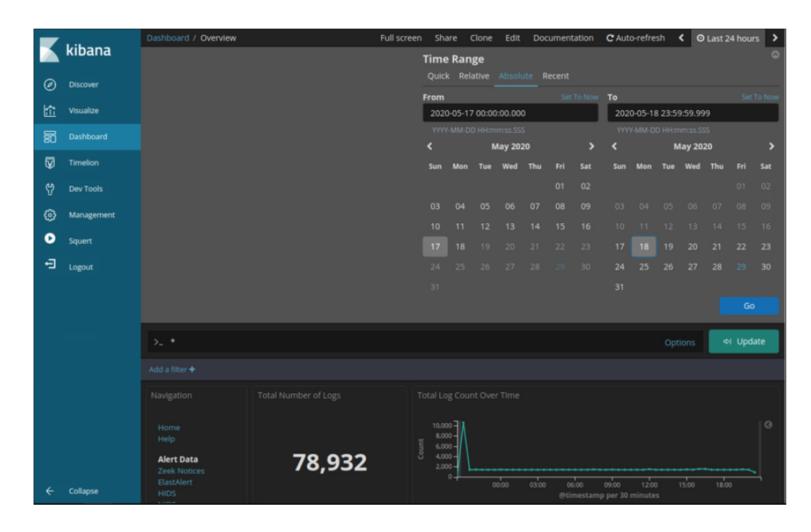
ST CNT Sens	r Alert I	D Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Mes	sage					
RT 42 secon	ion 3.253	3 2020-05-10 22:59:	19 192.168.0.11	38504	8.8.4.4	53	17	ET INFO O	bserved DN	S Query to	.biz TLD			
create AutoCat From	Event	2020-05-10 22:59:	24 192.168.0.11	44853	209.165.200.235	53	17	ET INFO O	bserved DN	S Query to	.biz TLD			
xpire Event As NA (		2020-05-10 22:59:4	45 192.168.0.11	59572	209.165.200.235	80	6	ET WEB_S	ERVER WE	B-PHP php	info access			
Expire Event As NA V	With Comment	2020-05-10 22:59:4	45 192.168.0.11	59572	209.165.200.235	80	6	ET WEB_S	ERVER PH	P Eastereg	g Information-	Disclosure	(php-log	0)
Quick Query		2020-05-10 22:59:4	45 192.168.0.11	59572	209.165.200.235	80	6	ET WEB_S	ERVER WE	B-PHP php	info access			
Idvanced Query Ipdate Event Status		2020-05-10 22:59	45 192.168.0.11	59572	209.165.200.235	80	6	ET WEB_S	ERVER PH	P Eastereg	g Information-	Disclosure	(php-log	0)
	017 0.176	Escalate (F9)			209.165.200.235	80	6	ET WEB_S	ERVER PH	P Eastereg	g Information-	Disclosure	(zend-lo	go)
RT 1 secon	ion 3.271	Cat I: Unauthorized Ro Cat I: Add Comment	oot Access (F1)		209.165.200.235	80	6	ET WEB_S	ERVER PH	P Eastereg	g Information-	Disclosure	(zend-lo	go)
RT 1 secon	ion 7.208		ker Access (E2)		209.165.200.235	111	6	GPL RPC	ortmap listin	g TCP 111				
RT 1 secon	ion 5.179		sei Access (F2)		209.165.200.235	111	6	GPL RPC	ortmap listin	g TCP 111				
RT 3 secor	ion 5.179		uthorized Access (F3)		209.165.200.235	111	6	GPL RPC	ortmap NFS	request To	CP			
RT 3 secon	ion 5.179	7 Cat III: Add Comment			209.165.200.235	111	17	GPL RPC	ortmap mou	ntd request	UDP			
RT 3 secon	ion 7.208	9 Cat IV: Successful De	nial of Service Attack	(F4)	209.165.200.235	111	6	GPL RPC	ortmap NFS	request T(	CP			
RT 3 secon	inn- 7 209	Cat IV: Add Comment			209 165 200 235	111	17	GPI RPC	ontman mos	ntri remiest	IINP			
	- Person	Cat V: Poor Security P on Cat V: Add Comment Cat VI: Reconnaissan			acket Data 🦳 Show	Rule								
Sid Net	Hostname	Cat VI: Add Comment			0			Mar. 1		1	10 00-00	0.000		-
1 seconion-osse		Cat VII: Virus Infection	n(F7)		Source IP	Des	st IP	Ver H	IL TOS	len	ID Flags	Offset	TTL	ChkS
2 seconion-ens1		Cat VII: Add Commen			Source			Dest						
3 seconion-ens1			-05-12 19:13:12	UDP	Port			Port		Lengt	th		ChkSum	
4 seconion-ens1		F-4	-06-01 15:36:06											
5 seconion-ens1			-05-12 19:13:12											
6 seconion-ens2		F-4	-06-01 15:36:27											
7 seconion-ens2	4 seconion-e	n snort 2020	-05-10 23:39:07	DATA										

- Sguil includes 7 pre-built categories
  - that can be assigned by using a menu or by pressing the function key.....

### Investigating Network Data 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** <u>customized visual</u> dashboards.

CISCO



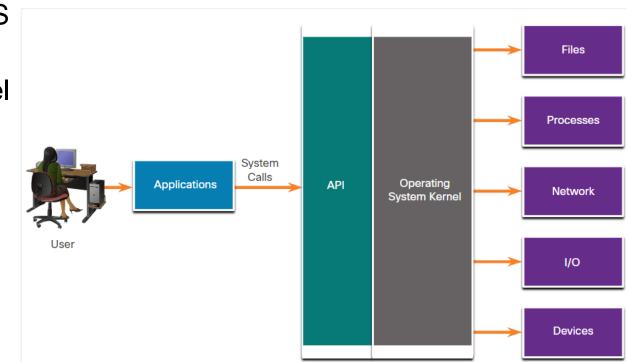
### Investigating Network Data Queries in ELK

- Elasticsearch is built on Apache Lucene, an open-source search engine software library featuring <u>full text indexing</u> and <u>searching</u> 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 <u>make use of elements</u> such as <u>Boolean operators</u>, Fields, Ranges, Wildcards, Regex, Fuzzy Search, and Text Search.
- Elasticsearch was designed to interface with users <u>using</u> web-based clients <u>that follow</u> 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 Network Data Investigating Process or API Calls

- <u>Applications</u> interact with an Operating System (<u>OS</u>) through **system calls** to the OS Application Programming Interface (<u>API</u>).
- 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.
- <u>Filtering for OSSEC indices</u> 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 Network Data 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 <u>Hunting</u> 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.

7	kibana	Dashboard / Zeek - Files	Full screen Share Clone Edit Documentation 🔢 15 minutes < 🧿 Last 2M 🗦
	kibana	>_ Search (e.g. status:200 AND	extension:PHP) Options C Refresh
Ø	Discover	mimetype.keyword: "application/xml"	
ĥ	Visualize		
30	Dashboard	t event_type	QQⅢ \$ Dro_files
V	Timelion	😐 file_ip	Q Q II # 209.165.201.17
Ŵ	THINKING I	t fuid	Q Q II + FFRuizivIHrErrgBd
Q	Dev Tools	t host	Q Q ∏ ★ gateway
٢	Management	t ips	Q Q Ⅲ ★ 209.165.200.235,
		t is_orig	Q Q ∏ ≱ true
0	Squert	t local_orig	Q Q Ⅲ ★ true
÷	Logout	t md5	<b>Q Q II *</b> 56ceda5bb5c4c6be9ea6f16e86ab676f
		t message	<pre>Q Q II * {"ts":"2020-05-10T21:20:56.997512Z", "fuid":"FFRuizivIHrErrgBd", "tx_hosts":["209.165.201.17"], "rx_hosts":</pre>
		t mimetype	Q Q □ # application/xml
		# missing_bytes	Q, Q, [] ≢ <sup>68</sup>
		# overflow_bytes	Q, Q, [] ★ 68
		# port	Q Q II 🛊 38524
		# seen_bytes	Q Q II * 7148
		t shai	Q Q ∏ ★ e4541e67581c859a6782c3492cb222da2ab2cf1c
		t source	Q Q II * HTTP
		t source_ips	e e □ *
		t syslog-facility	Q,Q, □ ★ user
÷	Collapse	t syslog-file_name	Q Q T * /nsm/bro/logs/current/files.log

### Investigating Network Data 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



# 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 <u>visual interface</u> to NSM data.

kibana	Connections - Destination IP Address	🗍 Data Table
Riballa	Connections - Destination Port	🔲 Data Table
Discover	Connections - Log Count	8 Metric
Visualize	Connections - Log Count Over Time	📈 Line
Dashboard	Connections - Missed Bytes	🔲 Data Table
Timelion	Connections - Protocol (Bar Chart)	🕅 Vertical Bar
Dev Tools	Connections - Responder Bytes	🔲 Data Table
	Connections - Service	🔲 Data Table
Management	Connections - Source - Originator Bytes (Tile Map)	Coordinate Map
Squert	Connections - Source - Responder Bytes ( Tile Map)	Coordinate Map
Logout	Connections - Source - Sum of Total Bytes (Tile Map)	Coordinate Map
	Connections - Source - Top Connection Duration (Tile Map)	Coordinate Map
	Connections - Source Country	🔲 Data Table
	Connections - Source IP Address	🔲 Data Table
	Connections - Top 10 - Total Bytes By Connection	🛅 Vertical Bar
	Connections - Top 10 - Total Bytes By Destination IP	🔝 Vertical Bar
	Connections - Top 10 - Total Bytes By Destination Port	🕅 Vertical Bar
	Connections - Top 10 - Total Bytes By Source IP	🕅 Vertical Bar
	Connections - Top Source IPs	() Pie
Collapse	3 items selected	
comapse		

34

# Enhancing the Work of the Cybersecurity Analyst 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 part**y 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

### Working with Network Security Data 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.



Introduction Chapter 11



# Chapter 28: Digital Forensics and Incident Analysis and Response

#### Module Objective: Explain the process of evaluating alerts

Topic Title	Topic Objective
<b>Evidence Handling and Attack Attribution</b>	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

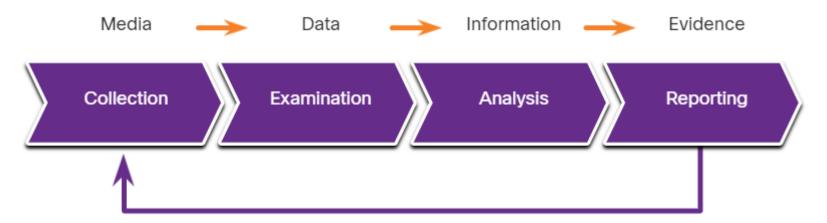


# Digital Forensics and Incident Analysis and Response **Digital Forensics**

- 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 <u>requirements</u> regarding the <u>preservation and handling of</u> <u>such evidence</u>.

### Digital Forensics and Incident Analysis and Response The Digital Forensics Process

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



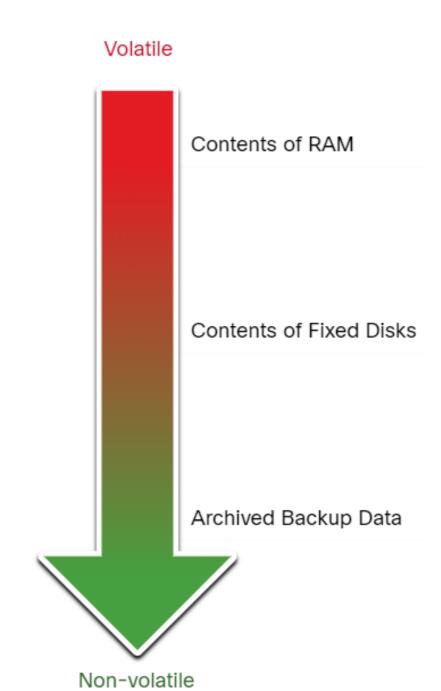
### Digital Forensics and Incident Analysis and Response **Types of Evidence**

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."

### Digital Forensics and Incident Analysis and Response Evidence Collection Order

- IETF RFC 3227 describes an order for the <u>collection of digital evidence</u> 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.



Evidence

#### Digital Forensics and Incident Analysis and Response Chain of Custody (Reťazec spracovania dôkazov)

- involves the
  - Collection
  - Handling
  - secure storage of evidence.
- Detailed records should be kept of the following:
  - Who <u>discovered</u> 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 <u>physical access to the evidence</u> while it was stored? Access should be restricted to <u>only the most essential personnel</u>.

#### Digital Forensics and Incident Analysis and Response **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.

#### Digital Forensics and Incident Analysis and Response 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 <u>systematic investigation</u> of the evidence.
- In an evidence-based investigation, the incident response team <u>correlates</u> 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 <u>can help track the addresses</u> used in the attack back to a specific device.

#### Digital Forensics and Incident Analysis and Response 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/

#### Digital Forensics and Incident Analysis and Response 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.
   MITRE ATT&CK Matrix for a Ransomware Exploit
- Persistance
   = vytrvalosť
- Evasion
   = únik

cisco



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

# 28.2 The Cyber Kill Chain



### The Cyber Kill Chain Steps of the Cyber Kill Chain

- The Cyber Kill Chain was developed by Lockheed Martin to <u>identify</u> and <u>prevent</u> 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.

cisco

# The Cyber Kill Chain **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**

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

**SOC Defences** 

- 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

uluilu cisco

- Weaponization <u>uses the information</u> <u>from reconnaissance</u> to develop a <u>weapon</u> <u>against specific</u> targeted systems or individuals in the organization.
- It is often <u>more effective to use</u> 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 Detect and collect Prepare and stage** the operation: weaponization artifacts: Ensure that IDS rules and Obtain an signatures are up to date. automated tool to Conduct <u>full malware analysis</u>. deliver the malware Build detections for the payload (weaponizer) behavior of known Select or create a weaponizers. document to Is malware old, "off the shelf" present to the or new malware that might indicate a tailored attack victim. Select or create a (na mieru šitý)? backdoor and Collect files and metadata for command and future analysis. • Determine which weaponizer control artifacts are common to which infrastructure. campaigns.

# The Cyber Kill Chain **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

CISCO

- making the code look legitimate
- obfuscating (zahmlievanie) the code
- Security sensors are so advanced that they <u>can</u> <u>detect</u> the code as malicious <u>unless it is **altered**</u> to avoid detection.
- The table summarizes the tactics and defenses used during the delivery step.

Adversary Tactics	SOC Defence
<ul> <li>Launch malware at target:</li> <li>Direct against webservers</li> <li>Indirect delivery through:</li> <li>Malicious email</li> <li>Malware on USB stick</li> <li>Social media interactions</li> <li>Compromised websites</li> </ul>	<ul> <li>Block delivery of malware:</li> <li>Analyze the infrastructure path used for delivery.</li> <li>Understand targeted servers, people, and data available to attack.</li> <li>Infer intent of the adversary based on targeting.</li> <li>Collect email and web logs for forensic reconstruction.</li> </ul>
© 2016 Cisco	and/or its affiliates. All rights reserved. Cisco

# The Cyber Kill Chain **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
<ul> <li>Exploit a vulnerability to gain</li> <li>access: <ul> <li>Use software, hardware, or human vulnerability</li> <li>Acquire or develop the exploit</li> <li>Use an adversary-triggered exploit for server vulnerabilities</li> <li>Use a victim-triggered exploit such as opening an email attachment or malicious web link</li> </ul> </li> </ul>	<ul> <li>Train employees, secure code, and harden devices:</li> <li>Employee security awareness training and periodic email testing</li> <li>Web developer training for securing code</li> <li>Regular vulnerability scanning and penetration testing</li> <li>Endpoint hardening measures</li> <li>Endpoint auditing to forensically determine origin of exploit</li> </ul>

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

# The Cyber Kill Chain 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**

## 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

#### **SOC Defence**

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.

Reap the rewards (získať odmenu za) of successful attack:

**Adversary** 

**Tactics** 

- Collect user credentials
- Privilege escalation
- Internal reconnaissance
- Lateral movement through environment
- Collect and exfiltrate data
- Destroy systems
- Overwrite, modify, or corrupt data

## **SOC Defence**

Detect by using forensic evidence:

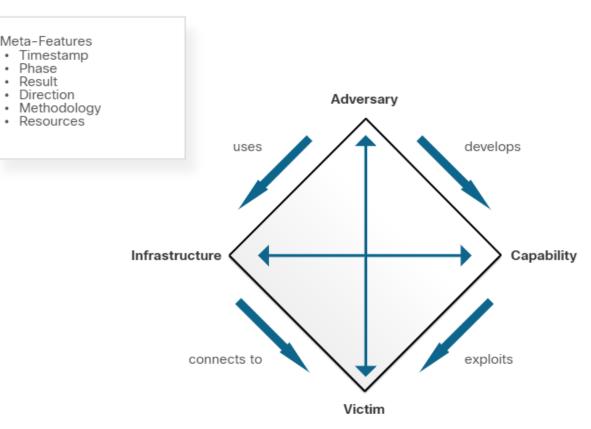
- Establish incident response playbook
- Detect data exfiltration, lateral movement, and unauthorized credential usage
- Immediate analyst response for all alerts
- Forensic analysis of endpoints for rapid triage
- Network packet captures to recreate activity
- Conduct damage assessment

# 28.3 The Diamond Model of Intrusion Analysis



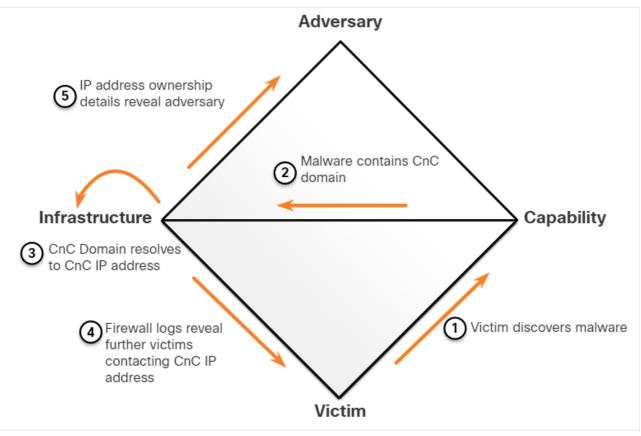
# The Diamond Model of Intrusion Analysis Diamond Model Overview

- 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



# The Diamond Model of Intrusion Analysis 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.

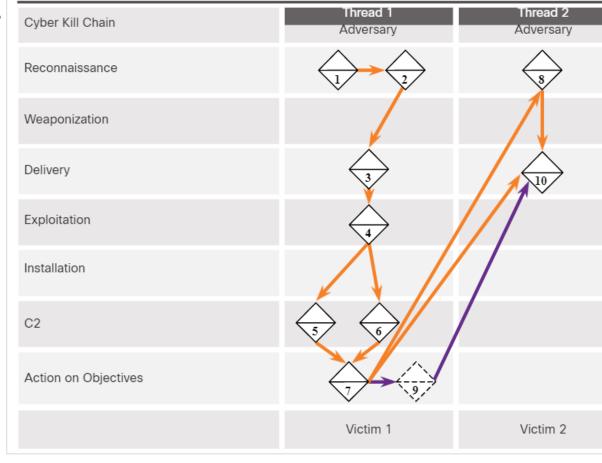


#### Diamond Model Characterization of an Exploit

#### The Diamond Model of Intrusion Analysis

## 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.



© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

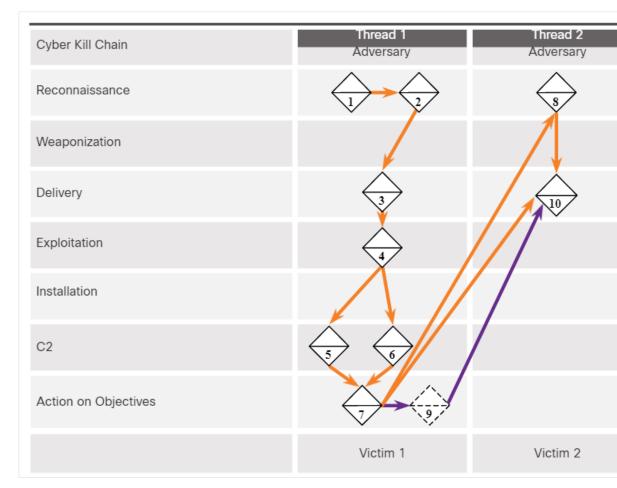
#### The Diamond Model of Intrusion Analysis The Diamond Model and the Cyber Kill Chain (Contd.)

- 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.

Cyber Kill Chain	Thread 1 Adversary	Thread 2 Adversary
Reconnaissance		8
Weaponization		
Delivery	3	10
Exploitation	4	
Installation		
C2	5 6	
Action on Objectives	2	
	Victim 1	Victim 2

# The Diamond Model of Intrusion Analysis 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.



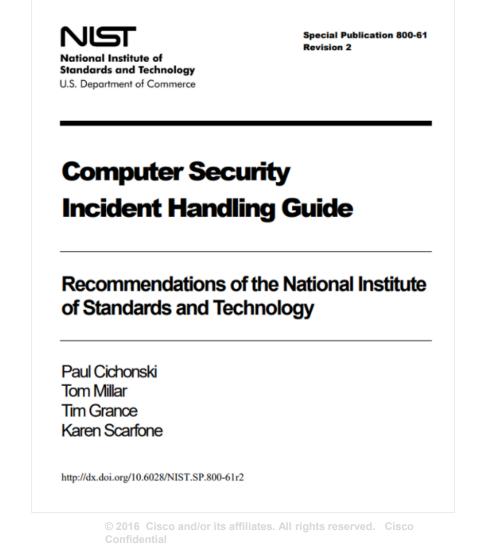
## 28.4 Incident Response



#### 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.



#### Incident Response

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

#### Incident Response Incident Response Stakeholders

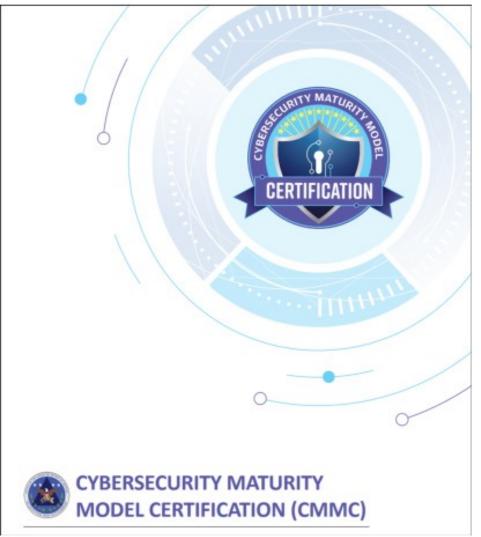
- The stakeholders involved in handing a security incident are as follows:
  - Management
  - Information Assurance
  - IT Support
  - Legal Department
  - Public Affairs and Media Relations
  - Human Resources
  - Business Continuity Planners
  - Physical Security and Facilities Management

#### **Incident Response**

## Incident Response Stakeholders (Contd.)

## The Cybersecurity Maturity Model Certification (CMMC)

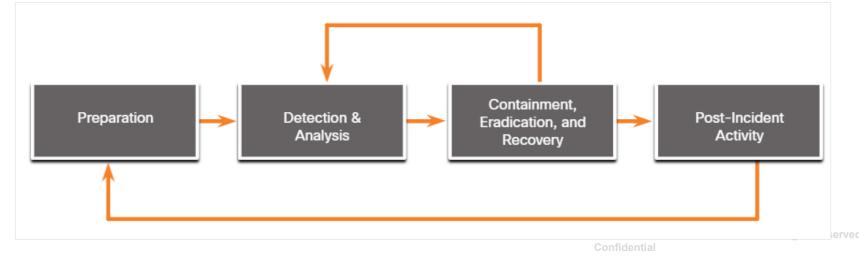
- The CMMC certifies organizations by level. For most domains, there are five levels, however for incident response, there are only four:
  - Level 2 Establish an incident response plan that follows the NIST process.
  - Level 3 Document and report incidents to stakeholders identified in the incident 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.



2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

#### Incident Response NIST Incident Response Life Cycle

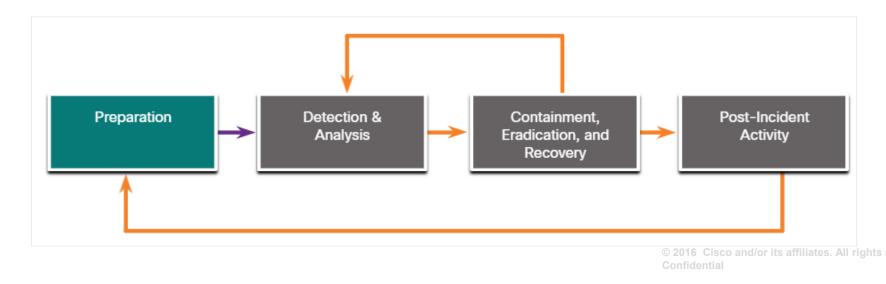
- NIST defines four steps in the incident response process life cycle:
  - Preparation The members of the CSIRT are trained in how to respond to an incident.
  - **Detection and Analysis** CSIRT quickly identifies, analyzes, and validates an incident.
  - Containment, Eradication, and Recovery CSIRT 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.



#### Incident Response Preparation

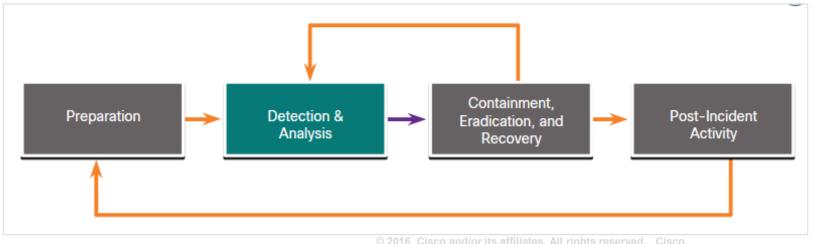
cisco

- 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.



## Incident Response Detection and Analysis

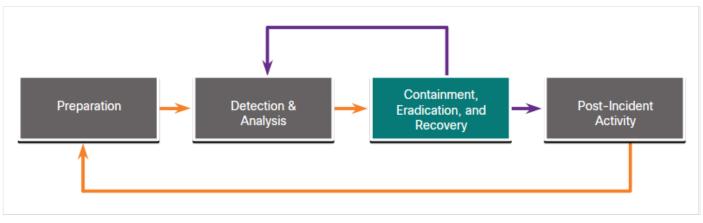
- Different types of incidents will require different responses.
  - Attack Vectors: Web, Email, Loss or Theft, Impersonation, Attrition and Media.
  - Detection: Automated detection Antivirus software, IDS, manual detection user reports.
  - Analysis: Use Network and System Profiling to determine the 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,



#### Incident Response 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.

uluilu cisco

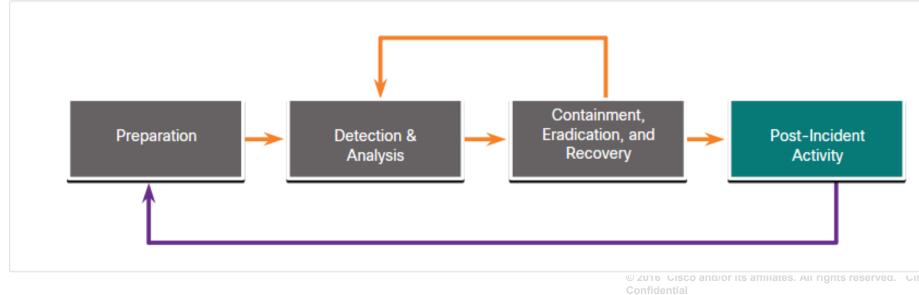


#### Incident Response **Post-Incident Activities**

• 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. ۲



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

## Incident Response

## 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



#### 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.

#### Digital Forensics and Incident Analysis and Response Summary 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.