



Инцидент-менеджмент: формирование регламентов реагирования при кибератаках и решение внутренних проблем и задач.

Реализаций подхода к противодействию кибератакам, и централизации доступа к сетевой инфраструктуре с применением принципов Нулевого доверия и Минимальных полномочий на базе продукта UnicNet

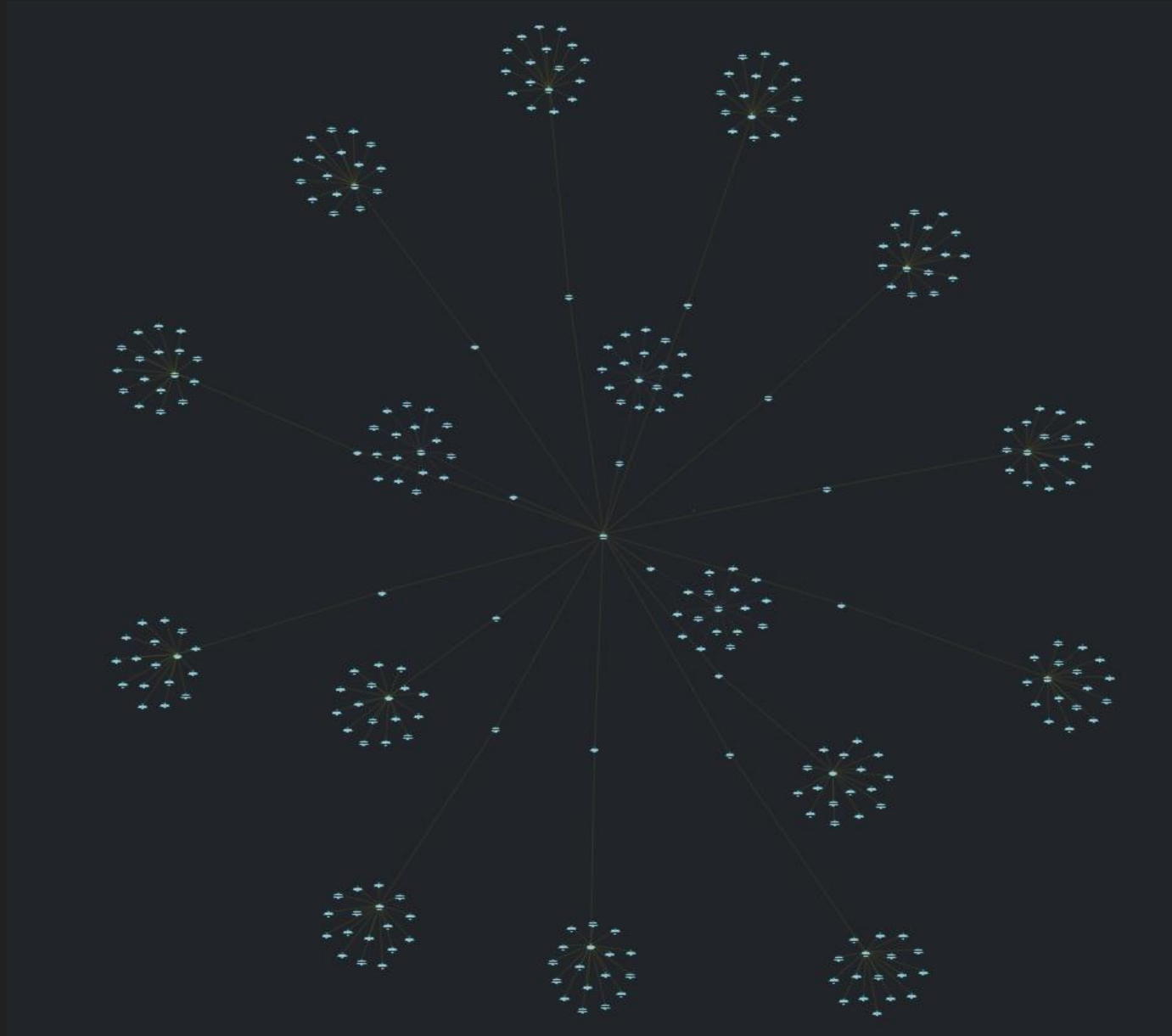


UnicNet



Векторы внутренних проблем

Модель типовой сети объектов КИИ с репликацией



Суть проблемы: шторм, перегрузка uplink, неверный порт



-
- ☒ STP
- ☒ Подписи узлов
- ☒ У выбранного
- ☐ Гравитация
- ☐ Статусы связей

L2 Основная карта



Статус портов 10.0.10.100



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2	3	4	1	2	3	4
1 Gbps	1 Gbps	1 Gbps	1 Gbps	100 Mbps	1 Gbps	1 Gbps	1 Gbps	100 Mbps	1 Gbps	100 Mbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	4 Gbps	4 Gbps	4 Gbps	4 Gbps	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	1	2	3	4	1	2	3	4	
1 Gbps	1 Gbps	1 Gbps	1 Gbps	100 Mbps	1 Gbps	1 Gbps	100 Mbps	1 Gbps	100 Mbps	100 Mbps	100 Mbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	1 Gbps	4 Gbps	4 Gbps	4 Gbps	4 Gbps	

Автообновление портов



Список портов устройства



L2 топология → STP данные поступают с задержкой или не поступают вовсе
STP данные root bridge, изменения, блокировки портов

1.1.1.1, 10.24.0.1, 10.24.0.2

Описание10.25.0.2

1.1.1.1
Cloudflare
Internet

10.24.0.1
GW, VNI-24.1
VIP

10.24.0.2
SI-MES5318
Switch

01.01.20262026-02-04 18:00:24.00000004.02.2026

Все записи

1.1.1.1

10.24.0.1

10.24.0.2

* Все записи1.1.1.110.24.0.110.24.0.2

2026-02-04 18:00:16	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:UnicNet cmd:login, aggregated (1)
2026-02-04 18:00:17	10.24.0.2	%SYS-4-WARN: Watchdog: no heartbeat from main process (timeout=30s)
2026-02-04 18:00:18	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:UnicNet cmd:show unit
2026-02-04 18:00:19	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:UnicNet cmd:show version
2026-02-04 18:00:20	10.24.0.2	%AAA-I-DISCONNECT: User CLI session for user UnicNet over telnet , source 0.0.0.0 destination 0.0.0.0 TEI
2026-02-04 18:00:21	10.24.0.2	%SYSLOG-F-OSFATAL: caught segmentation fault exception
2026-02-04 18:00:22	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:admin cmd:login, aggregated (10)
2026-02-04 18:00:23	10.24.0.2	%AAA-W-REJECT: New telnet connection, source 0.0.0.0 destination 0.0.0.0, local user table REJECTED.
2026-02-04 18:00:24	10.24.0.2	%SYS-2-CRIT: Watchdog timer expired, rebooting system
2026-02-04 18:00:25	10.24.0.2	%SYS-5-RESTART: System restarted -- Watchdog reset
2026-02-04 18:00:26	10.24.0.2	%SYS-5-BOOT: Booting Eltex RouterOS version 1.12.3
2026-02-04 18:00:27	10.24.0.2	%SYS-5-INIT: System initialization completed
2026-02-04 18:00:28	10.24.0.2	%SNMP-W-SNMPAUTHFAIL: Access attempted by unauthorized NMS: ?, aggregated (1)
2026-02-04 18:00:29	10.24.0.2	%AAA-I-CONNECT: User CLI session for user UnicNet over telnet , source 0.0.0.0 destination 0.0.0.0, loca
2026-02-04 18:00:30	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:UnicNet cmd:login
2026-02-04 18:00:31	10.24.0.2	%AAA-I-DISCONNECT: User CLI session for user UnicNet over telnet , source 0.0.0.0 destination 0.0.0.0 TEI
2026-02-04 18:00:32	10.24.0.2	%SYSLOG-F-OSFATAL: caught segmentation fault exception
2026-02-04 18:00:33	10.24.0.2	%AAA-I-CONNECT: User CLI session for user UnicNet over telnet , source 0.0.0.0 destination 0.0.0.0, loca
2026-02-04 18:00:34	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:UnicNet cmd:login, aggregated (2)
2026-02-04 18:00:35	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:UnicNet cmd:show unit
2026-02-04 18:00:36	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:UnicNet cmd:show version
2026-02-04 18:00:37	10.24.0.2	%SYSLOG-F-OSFATAL: caught segmentation fault exception
2026-02-04 18:00:38	10.24.0.2	%AAA-I-DISCONNECT: User CLI session for user UnicNet over telnet , source 0.0.0.0 destination 0.0.0.0 TEI
2026-02-04 18:00:39	10.24.0.2	%SYS-4-WARN: System response slow (possible hang)
2026-02-04 18:00:40	10.24.0.2	%STP-W-PORTSTATUS: g11/0/1: forwarding
2026-02-04 18:00:41	10.24.0.2	%LINK-W-Down: g11/0/1
2026-02-04 18:00:42	10.24.0.2	%STP-W-PORTSTATUS: g11/0/1: blocking
2026-02-04 18:00:43	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:UnicNet cmd:login, aggregated (1)
2026-02-04 18:00:44	10.24.0.2	%GCLI-I-CMD-EXEC: source:0.0.0.0 destination:0.0.0.0 user:UnicNet cmd:show unit
2026-02-04 18:00:45	10.24.0.2	%LINK-W-Down: g11/0/1

. **SYSLOG**: смена топологии/ высокая нагрузка/ STP события

- 1. Превентивная защита: включить BPDU Guard на edge-портах
Смысл: если кто-то воткнул “левый” свитч/петлю — порт сам уйдет в защиту, включить BPDU Guard / PortFast (если поддерживается)
- 2. Превентивная защита: storm-control (антишторм по broadcast/multicast)
Смысл: если начинается broadcast storm — сеть не умирает полностью.
- 3. Быстро “потушить пожар”: выключить подозрительный порт
Смысл: NOC/SOC увидели порт, где шторм → мгновенно вырубили.
- 4. Защита ядра: Root Guard на аплинках (чтобы никто не стал root)
Смысл: “подключили свитч и он внезапно стал STP root” — классика аварий.
- 5. Задача - каждые N часов обновлять всю инфу - собирать STP/порты/таблицы” → раннее выявление изменений для реагирования и выработки подхода к решению.

Редактирование задачи

Case 1.4

Приоритет: Низкий Тип: Скрипт

Группы

Устройства

Скрипт группы Новая группа

Новая группа

configure terminal
interface ethernet 1/0/48
spanning-tree guard root
exit
write memory

Закреть

Редактирование задачи

Case 1.2

Приоритет: Низкий Тип: Скрипт

Группы

Устройства

Скрипт группы Новая группа

Новая группа

configure terminal
interface range ethernet 1/0/1-1/0/24
storm-control broadcast level 5
storm-control multicast level 5
storm-control unicast level 10
exit
write memory

Закреть

Редактирование задачи

Case 1.1

Приоритет: Низкий Тип: Скрипт

Расписание выполнения задачи

Weekly by at 00:00

Группы

Устройства

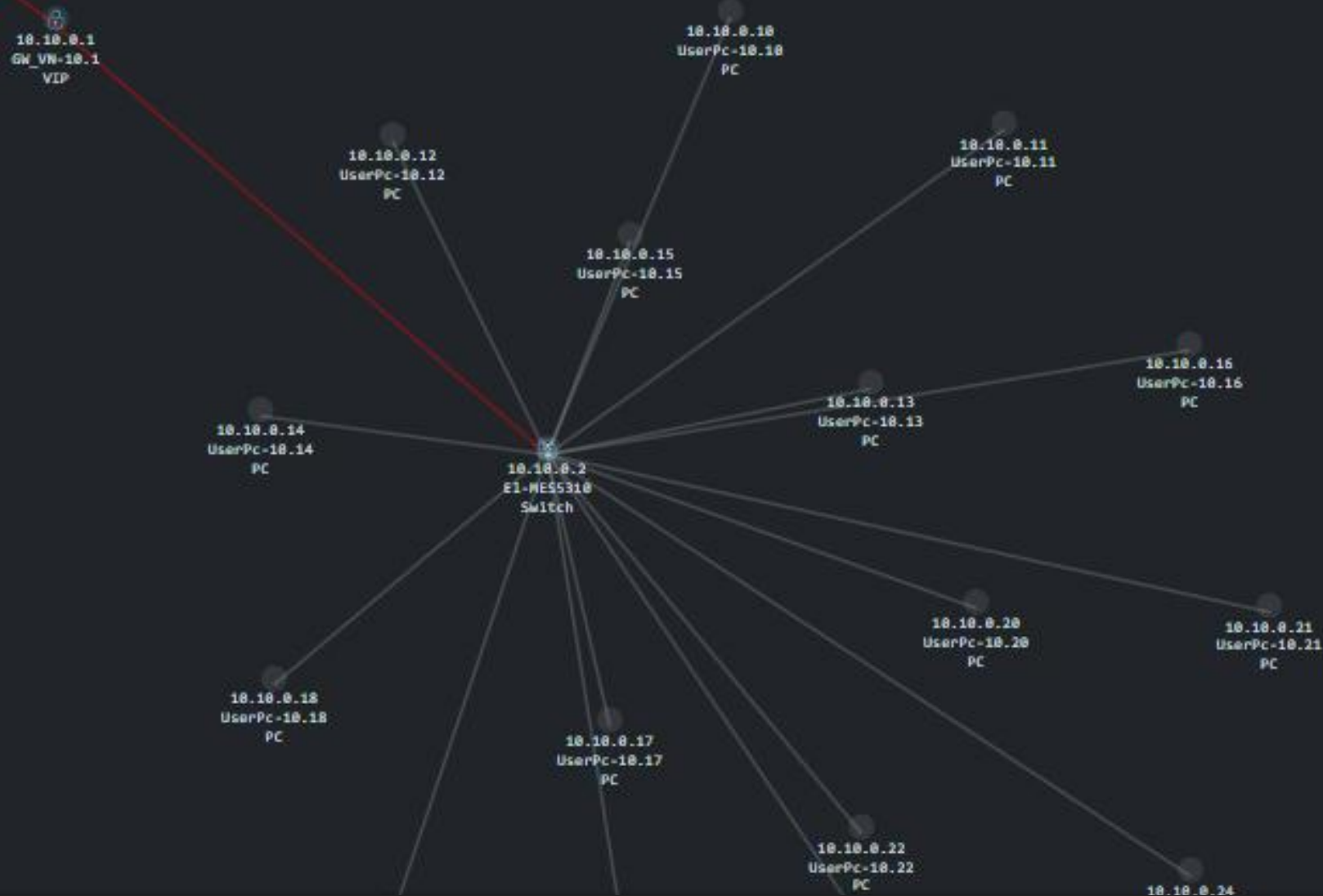
Скрипт группы Новая группа

Новая группа

10.0.100.4

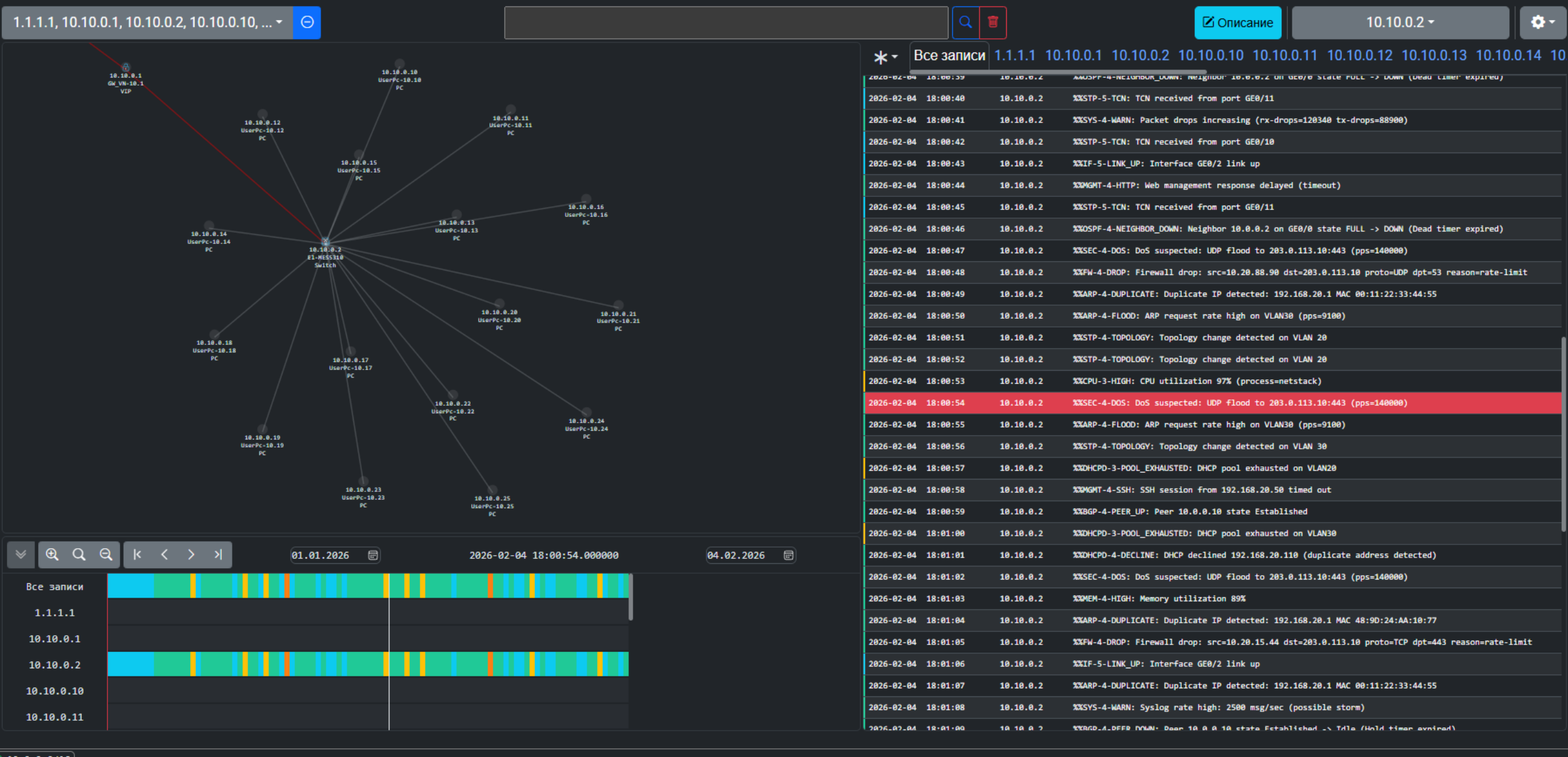
configure terminal
interface range ethernet 1/0/1-1/0/24
spanning-tree portfast
spanning-tree bpduguard enable
exit
write memory

Сохранить изменения Закреть



Кейс 2 — Рост трафика, DDoS: лаги, DoS/перегрузка

Суть: временный всплеск нагрузки + хаос в маршрутизации/связности.



SYSLOG: “шторм” на контрольном коммутаторе L3

- 1. Включение rate-limit / storm-control (защита от флуда и “шумных клиентов”)
- 2. Отключение неиспользуемых портов (“Закрыть всё лишнее”: отключение неиспользуемых портов)
- 3. Включение нужных ACL/ограничений (фильтрация трафика для мероприятия):

3 показательных ACL-сценария:

Запрет управления сетью (SSH/Telnet/SNMP) из пользовательского VLAN

Разрешить только нужные сервисы наружу (например DNS/NTP/HTTP/HTTPS)

Антискан: запрет межклиентского общения внутри VLAN (частично)

Принцип:

“Один сценарий → применили к устройствам → однообразие конфигурации → готовность к повышению нагрузки, распределение нагрузки”.

Редактирование задачи

Case 2.1-2

Группы

Устройства

Скрипт группы

Новая группа

Новая группа

```

configure terminal
interface range ethernet 1/0/1-1/0/24
rate-limit input 10m
rate-limit output 50m
exit
write memory

configure terminal
interface range ethernet 1/0/1-1/0/24
broadcast suppression 2
exit
write memory

```

Приоритет: Низкий

Тип: Скрипт

Сохранить изменения

Заккрыть

Редактирование задачи

Case 2.2-1

Группы

Устройства

Скрипт группы

Новая группа

Новая группа

```

configure terminal
interface range ethernet 1/0/13-1/0/46
shutdown
description UNUSED_EVENT_LOCKDOWN
exit
write memory

configure terminal
interface range ethernet 1/0/13-1/0/46
no shutdown
no description
exit
write memory

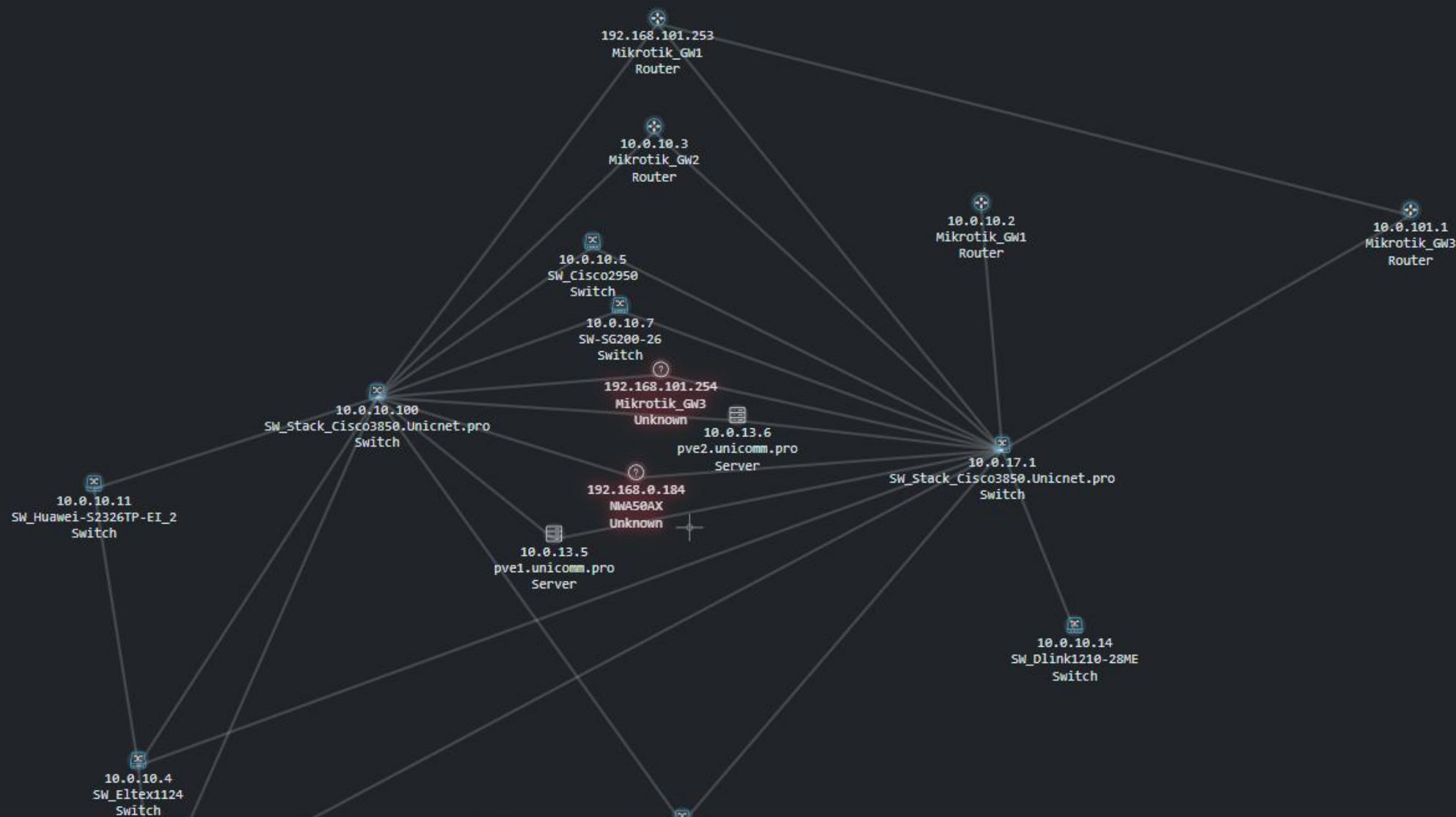
```

Приоритет: Низкий

Тип: Скрипт

Сохранить изменения

Заккрыть



Кейс 3 — Импортозамещение / горячая замена оборудования

Суть: меняем железо → неизвестно, что сломается: VLAN, маршруты, STP, соседство.

- Подготовка “миграционного чек-листа”:
 - какие порты должны быть trunk/access
 - какие VLAN должны быть разрешены
 - какие маршруты должны присутствовать
- Массовая команда: “привести конфигурацию к стандарту”
- Плановый сбор таблиц маршрутизации → контроль “не уехали ли next-hop”

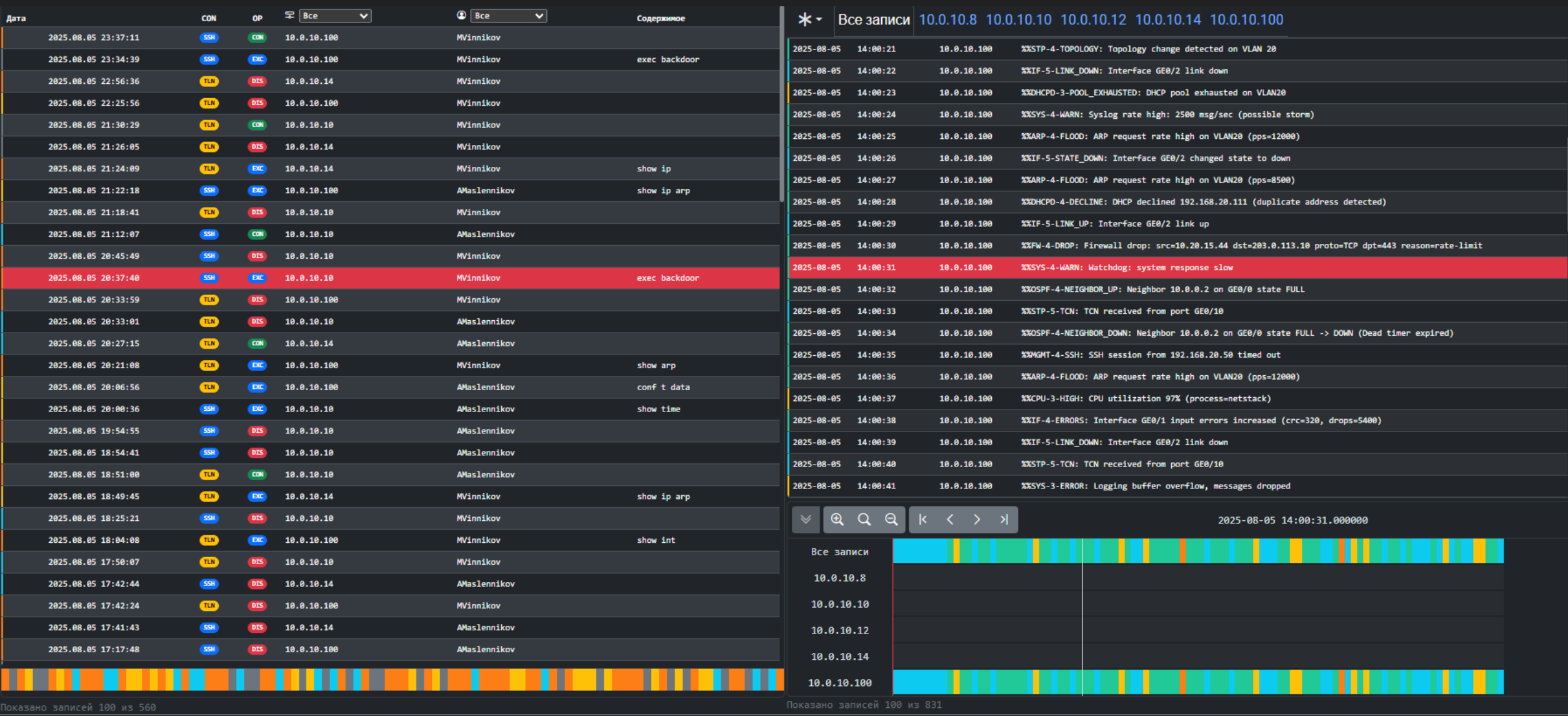
Векторы кибератак



10.0.10.8		SW_HP-A3600-48			-	Hp	✓	🌐			02/03/2026					
10.0.10.9		SW_Huawei-S2326TP-EI_2			-	Huawei	+	🌐			02/03/2026					
10.0.10.10		SW_DLink-3420-52T			-	D-Link	✓	🌐			02/03/2026					
10.0.10.11		SW_Huawei-S2326TP-EI_2			-	Huawei	⚠	🌐			02/03/2026					
10.0.10.12		SW_Juniper_EX2200			-	Juniper	+	🌐			02/03/2026					
10.0.10.13		R_Cisco_1841.unicnet.com			-	Cisco	✓	🌐			02/03/2026					
10.0.10.14		SW_Dlink1210-28ME			-	D-Link	+	🌐			02/03/2026					
10.0.10.17		FW_Fortigate-60C			-	Fortinet	+	🔥			02/03/2026					
10.0.10.100	🔥	SW_Stack_Cisco3850.Unicnet.pro			-	Cisco	+	🌐			02/03/2026					
10.0.17.1		10.0.17.1			-	Не указано	+	⚠			02/04/2026					
10.10.0.1	VR	GW_VN-10.1			-	VipNet	+	🔒			02/04/2026					
10.10.0.2	VR	EI-MES5310			-	Eltex	+	🌐			02/04/2026					
10.10.0.10	VR	UserPc-10.10			-	LinuxPc	+	🖥			02/04/2026					
10.10.0.11	VR	UserPc-10.11			-	LinuxPc	+	🖥			02/04/2026					
10.10.0.12	VR	UserPc-10.12			-	LinuxPc	+	🖥			02/04/2026					
10.10.0.13	VR	UserPc-10.13			-	LinuxPc	+	🖥			02/04/2026					
10.10.0.14	VR	UserPc-10.14			-	LinuxPc	+	🖥			02/04/2026					
10.10.0.15	VR	UserPc-10.15			-	LinuxPc	+	🖥			02/04/2026					
10.10.0.16	VR	UserPc-10.16			-	LinuxPc	+	🖥			02/04/2026					
10.10.0.17	VR	UserPc-10.17			-	LinuxPc	+	🖥			02/04/2026					

Атака 1 — Внутренние и внешние атаки

Суть: подозрительная активность, изменения, странные подключения.



- Сопоставление логов UnicNet и SYSLOG:
 - “кто запускал команды, кто менял доступ/учетки”
 - “что происходило на устройствах в это же время”



Атака 2 — Кража учетных данных устройств

Суть: злоумышленник получил доступ к SSH/Telnet/SNMP

• Ролевая модель

Разделение:

- “оператор видит, но не может выполнять опасные команды”
- “админ может выполнять”
- Минимальные полномочия для всех

ПользователиГруппыПрава

Текущие	UserID	Логин	Имя	E-Mail	Группы	Статус	Создано		
Архив	06b83e043976	abramovaa	Alexey Abramov		1	✔	28.08.2025	✔	🗑
	5ca1f8ebf831	admin			3	✔	05.02.2025	✔	🗑
	458d81d8ef0b	adrinskyi	Test		2	✔	07.07.2025	✔	🗑
	b4ae01b4aba0	amaslennikov	Александр Масленников	amaslennikov@unicomm.pro	3	✔	31.01.2025	✔	🗑
	4ab98b77bfdd	mandreev	Max Andreev		2	✔	07.04.2025	✔	🗑
	977f0310ae75	mvinnikov	Макс Винников	mixer57@gmail.com	4	✔	31.01.2025	✔	🗑
	08f19334e9d7	norlov	Nikolay Orlov		3	✔	17.09.2025	✔	🗑
	17672bc4c362	skonstantinov	Semen Konstantinov		2	✔	28.08.2025	✔	🗑
	b46e6e909a8f	slavaqa	Вячеслав Тестович		1	✔	28.03.2025	✔	🗑
	1b3459f9d205	ssarkisyan	Серго Саркисян		3	✔	04.02.2025	✔	🗑
	f3cfb86ab85d	test123	test user	test123@test123.xyz	2	❌	10.07.2025	✔	🗑
	68cf9a35535b	test321	test321 test321	test321@test.xyz	2	❌	14.07.2025	✔	🗑

Владелец	Тип	Порт	Название	Создано / Изменено	
— Добавить новую запись —					
unicnet_admin_group	SNMP v2	—	161	SNMP_V2	08/25/2025 / 08/28/2025
unicnet_superuser_group	SNMP v2	—	161	SNMP_V2	08/25/2025
unicnet_user_group	SNMP v2	—	161	SNMP_V2	08/25/2025
unicnet_admin_group	SNMP v3	—	161	SNMP_V3	Unicnet 08/25/2025 / 08/28/2025
unicnet_superuser_group	SNMP v3	—	161	SNMP_V3	Unicnet 08/25/2025
unicnet_user_group	SNMP v3	—	161	SNMP_V3	Unicnet 08/25/2025
unicnet_admin_group	SSH	—	22	SSH	UnicNet 08/25/2025 / 08/28/2025
unicnet_superuser_group	SSH	—	22	SSH	UnicNet 08/25/2025 / 08/28/2025
unicnet_user_group	SSH	—	22	SSH	UnicNet 08/25/2025 / 08/28/2025
unicnet_admin_group	Telnet	—	23	TelnetAdm	UnicNet 08/25/2025 / 08/28/2025
unicnet_superuser_group	Telnet	—	23	TelnetSup	UnicNet 08/25/2025 / 08/28/2025
unicnet_user_group	Telnet	—	23	TelnetUsr	UnicNet 08/25/2025 / 08/28/2025

- Назначение наборов учетных данных группам пользователей

Контроль:

- Нулевое доверие



Атака 3 — Кража учетных данных ПО

Суть: злоумышленник пытается использовать UnicNet как “панель управления сетью”.

- аудит действий в ПО кто запускал пакетные команды, когда, на какие устройства
- ограничение по группам и учеткам

Суть:
UnicNet не должен быть “супер-ключом от всего”, доступ должен быть сегментирован.

Чётные данные ⚙ Настройки

Логин

amaslennikov

✓

Имя

Александр Масленников

✓

Пароль

✖

✓

E-Mail

amaslennikov@unicomm.pro

✓

Группы

unicnet_admin_group ✖

unicnet_superuser_group ✖

unicnet_user_group ✖

+

▼

Статус

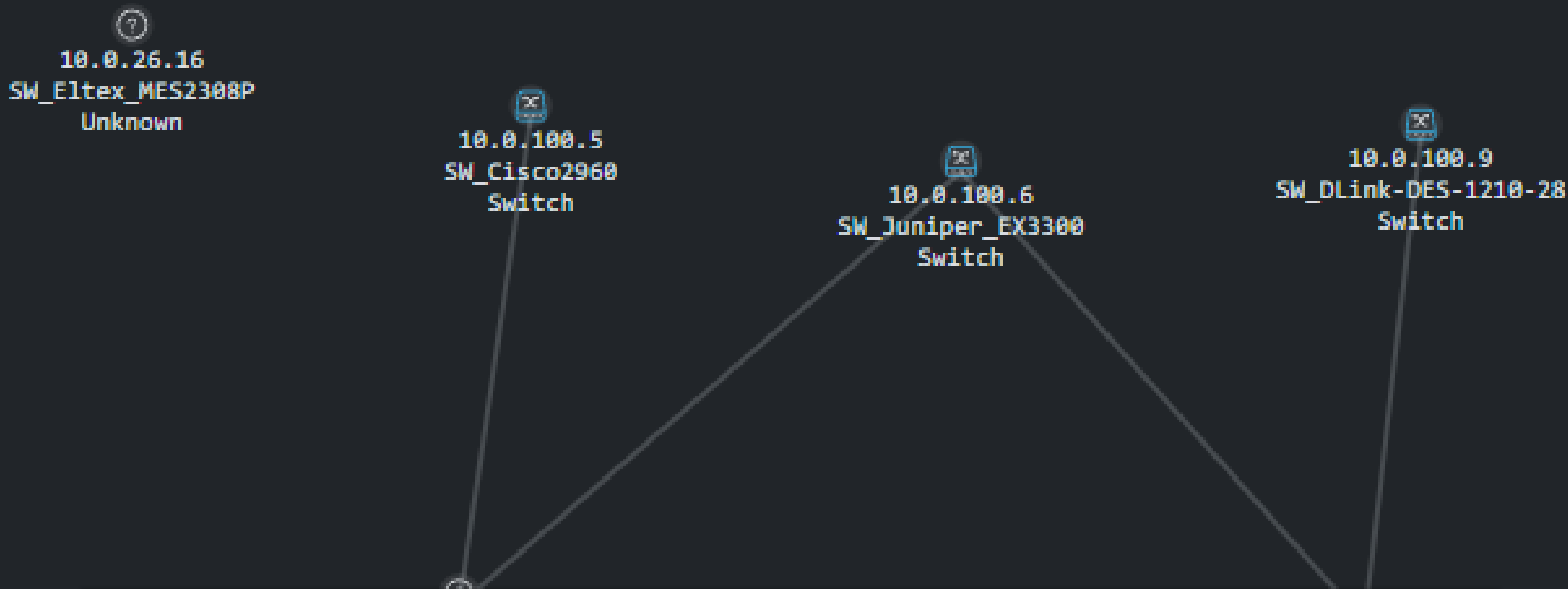
●

Создано

31.01.2025

Логин	Группы	Статус
abram	1	✓
adm	3	✓
adrin	2	✓
amasler	3	✓
mandr	2	✓
mvinn	4	✓
norl	3	✓
skonsta	2	✓
slav	1	✓
ssarki	3	✓
test	2	✖
test321	2	✖

2025.08.05 12:52:23	TLN	CON	10.0.10.14	MVinnikov	
2025.08.05 12:49:36	SSH	CON	10.0.10.14	AMaslennikov	
2025.08.05 12:49:32	SSH	EXC	10.0.10.10	AMaslennikov	show time
2025.08.05 12:44:56	SSH	EXC	10.0.10.100	AMaslennikov	show arp
2025.08.05 12:44:24	TLN	EXC	10.0.10.14	MVinnikov	exec backdoor
2025.08.05 12:28:07	SSH	DIS	10.0.10.10	AMaslennikov	
2025.08.05 12:12:18	SSH	CON	10.0.10.14	AMaslennikov	
2025.08.05 12:11:48	SSH	EXC	10.0.10.14	AMaslennikov	show arp
2025.08.05 11:55:29	SSH	EXC	10.0.10.100	AMaslennikov	show version
2025.08.05 11:40:32	SSH	CON	10.0.10.100	MVinnikov	
2025.08.05 11:33:14	SSH	CON	10.0.10.10	MVinnikov	
2025.08.05 11:28:35	SSH	EXC	10.0.10.100	MVinnikov	show ip
2025.08.05 11:22:22	SSH	EXC	10.0.10.100	MVinnikov	set desc
2025.08.05 11:01:45	SSH	DIS	10.0.10.10	AMaslennikov	
2025.08.05 10:52:37	TLN	CON	10.0.10.100	AMaslennikov	
2025.08.05 10:42:36	TLN	EXC	10.0.10.10	AMaslennikov	exec backdoor
2025.08.05 10:33:30	TLN	CON	10.0.10.100	AMaslennikov	
2025.08.05 10:13:38	SSH	CON	10.0.10.10	MVinnikov	
2025.08.05 10:04:45	TLN	DIS	10.0.10.10	AMaslennikov	
2025.08.05 09:53:03	SSH	DIS	10.0.10.100	AMaslennikov	
2025.08.05 09:52:04	TLN	DIS	10.0.10.14	AMaslennikov	
2025.08.05 09:45:52	TLN	CON	10.0.10.100	MVinnikov	
2025.08.05 09:37:04	TLN	EXC	10.0.10.14	MVinnikov	set interface t
2025.08.05 09:34:38	TLN	DIS	10.0.10.14	MVinnikov	
2025.08.05 09:18:48	SSH	CON	10.0.10.100	AMaslennikov	
2025.08.05 08:51:27	SSH	CON	10.0.10.10	MVinnikov	
2025.08.05 08:36:37	TLN	DIS	10.0.10.14	AMaslennikov	
2025.08.05 08:32:28	SSH	EXC	10.0.10.100	MVinnikov	conf t data
2025.08.05 08:28:14	SSH	EXC	10.0.10.10	AMaslennikov	show ip arp
2025.08.05 08:12:45	TLN	DIS	10.0.10.10	AMaslennikov	
2025.08.05 08:00:34	SSH	CON	10.0.10.14	AMaslennikov	



Атака 4 — Скан сети и поиск неучтенного оборудования

Суть: в сети появляются “левые” устройства: rogue switch, Wi-Fi, “серый” маршрутизатор.

- скан диапазона → найдено новое устройство
- ARP таблицы / MAC на порту → где физически сидит
- L2 топология → “новая ветка”
- теги:
 - отметить как unknown
 - переместить в группу “на проверку”

Решение

- пакетно отключить порт(ы) / перевести в quarantine VLAN
- создать регламент: “ежедневный скан + отчет по новым устройствам”

VR

 Виртуальное

🔥

 Подозрительное

🗑

 Удалённое

10.0.10.100

Suspect

00af1f432a00

WS-C3850-24P-E

Switch

Редактирование задачи

SCAN 10.0.10.2-15+100

Приоритет: Критический Тип: Дискаверинг Режим: Обновить все

Начальный IP		Конечный IP-адрес	
+	0.0.0.0	0.0.0.0	
1	10.0.10.2	10.0.10.15	
2	10.0.10.100	10.0.10.100	
3	10.0.17.1	10.0.17.1	

Закреть