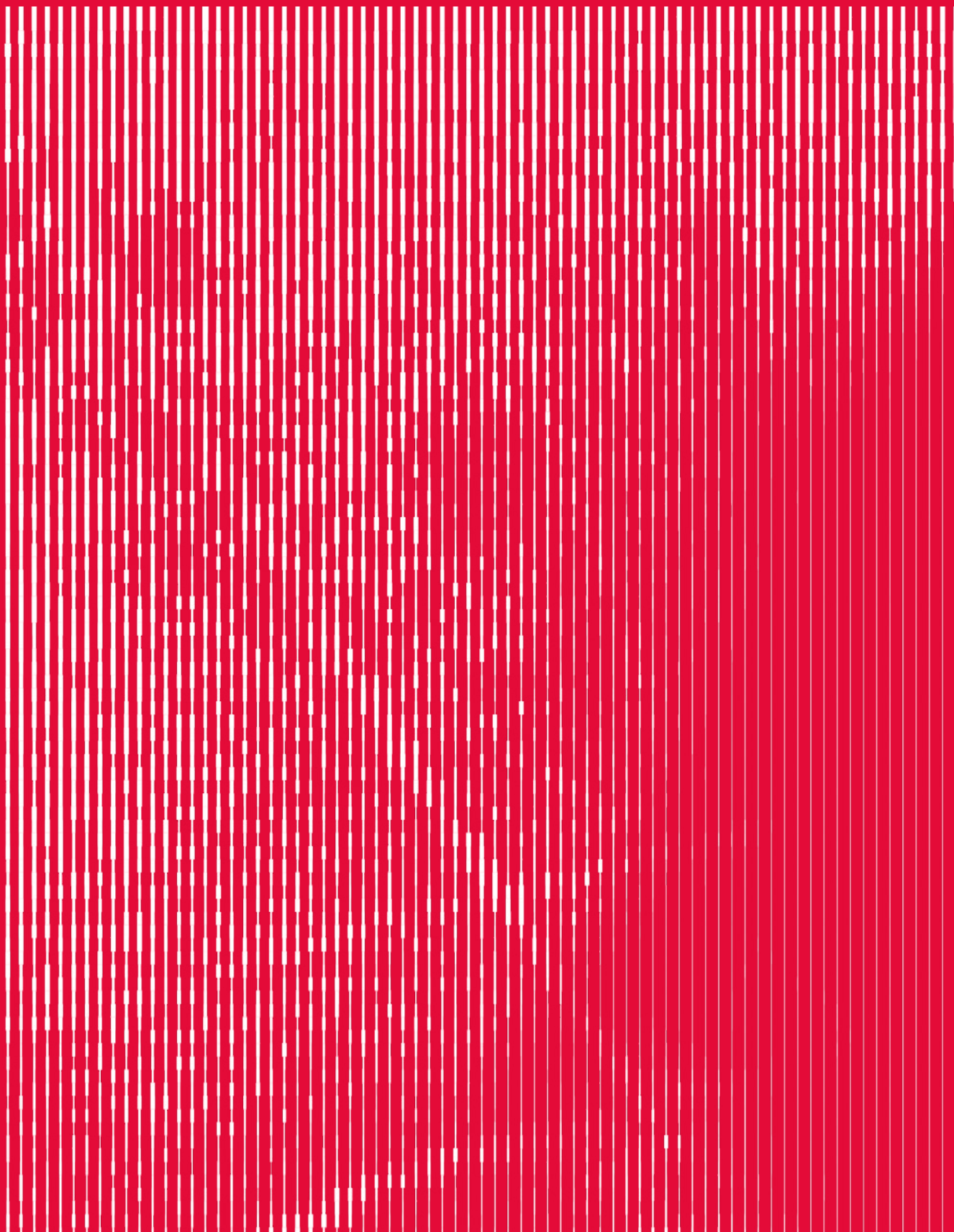


SOC

Riadená služba, ktorá kombinuje automatizovanú
analýzu dát s ľudskými odbornými znalosťami s cieľom
odhaliť a analyzovať narušenia bezpečnosti.



Kvalita SOC sa opiera o dobre vypracovanú stratégiu, vybrané inovatívne technológie, starostlivo definované procesy a predovšetkým o odborné znalosti tímu.

Poskytujeme komplexné služby SOCaaS pre korporácie a veľké organizácie s cieľom chrániť ich IT infraštruktúru prostredníctvom odborného a nepretržitého monitorovania, ktoré priebežne zmierňuje aktuálne hrozby a rieši prevenciu nových incidentov.

Naša filozofia prístupu “defence in depth” skúma viaceré parametre, čím výrazne zvyšuje šance na odhalenie potenciálne nebezpečných útokov skôr, ako spôsobia nenapraviteľné škody.

Zároveň týmto prístupom výrazne zvyšujeme šance na proaktívne odhalenie skutočne nebezpečných útokov.

PRIAMA SLUŽBA, KTORÁ KOMBINUJE
AUTOMATIZOVANÚ ANALÝZU ÚDAJOV
S ODBORNOU KVALIFIKÁCIOU NA
DETEKCIU, ANALÝZU A PREVENCIU
NARUŠENIA BEZPEČNOSTI

Vytvárame komplexné služby SOCaaS pre korporácie a veľké organizácie na ochranu ich IT infraštruktúry prostredníctvom odborného a nepretržitého monitorovania, ktoré neustále reaguje na novo prichádzajúce aktuálne hrozby a zabraňuje vzniku nových bezpečnostných incidentov.

- DEFCON
2.miesto

Náš tím to dokázal počas DEFCON 2022. V simulovanej vojnovej hre pre obranné tímy OpenSOC sa naši experti umiestnili na druhom mieste.
- Štruktúrovaný
report

Poskytujeme podrobné mesačné súhrnné správy sumarizujúce zásahy a činnosti centra SOC a podrobné dôkazy o pokusoch o narušenie bezpečnosti.
- Tím svetovej
kvality

Vďaka certifikátom ISO 27k a NSA SK je náš tím zdatný v rozpoznávaní a prevencii narušení bezpečnosti a v poskytovaní rýchleho riešenia.
- Maximum
zabezpečení

Sme držiteľmi medzinárodne uznávanej akreditácie TF-CSIRT a máme viac ako 9 rokov skúseností v poskytovaní špičkovej bezpečnosti.
- 30 + 30
minúty

Garantujeme maximálne 30 minút na registráciu alebo monitorovanie incidentu a následne maximálne 30 minút na reakciu.

Služby SOCaaS	Monitorovanie bezpečnosti a vyhľadávanie hrozieb
	Forenzná analýza
	Pokročilé vyšetrovanie a podpora LE
	Podpora riadenia bezpečnosti a poradenstvo
	Dodržiavanie predpisov
	Návrh a implementácia
	Podpora NOC/SD/infraštruktúry

Fáza 1

Analýza prichádzajúcich protokolov

Zisťovanie hrozieb

Monitorovanie SIEM

Školíme najlepšie systémy SIEM vo svojej triede, aby ste sa naučili štandardy fungovania vášho IT prostredia. Zhromažďuje protokoly a udalosti z vašich infraštruktúrnych zariadení, ktoré sú následne šifrované, aby sa mohli prenášať na účely automatizovaného odhaľovania a vyšetrovania útokov.

Tím SOC je okamžite upozornený na anomálie a poskytuje ochranu v reálnom čase pred doteraz neznámymi hrozbami.

Fáza 2

Kvalifikácia ľudí

Analýza nebezpečných hrozieb

Reakcia na hrozby

Tím následne vykoná hĺbkovú analýzu upozornení SIEM a z údajov extrahuje závažné hrozby.

Sme v pohotovosti 24 hodín denne, 7 dní v týždni, 365 dní v roku, pričom plynulo kombinujeme priebežné vyšetrowanie všetkých vznikajúcich útokov s informovaným rozhodovaním s cieľom zablokovat hackerov a minimalizovat škody na vašej infraštruktúre.

Stage 3

Upozornenia klientov

Správy

Monitorovanie hackerov

Upozornenia na hrozby budú doručené len v prípade potreby. Každý mesiac vám bude poskytnutá prispôsobená správa, ktorá poskytne prehľad vašej aktuálnej IT infraštruktúry a súhrn všetkých zistených, analyzovaných a odvrátených narušení.

V prípade, že došlo k narušeniu bezpečnosti, útoku, sú poskytované komplexné správy. Udržiavame tiež úzky kontakt s orgánmi činnými v trestnom konaní, aby sme pomohli pri pátraní po hackeroch a podporili vašu spoločnosť.

Každý z našich analytikov SOC má znalosti v oblasti normy ISO 27K a týchto zásad spoločnosti Binary Confidence:

Správa systému

Porozumenie príkazom a skriptom systému Linux

Vytváranie sietí

Znalosť firewallov, IP adries a smerovacích protokolov

Základy programovania a skriptovania

Všeobecné znalosti programovacích a skriptovacích jazykov

Kryptografia

Znalosť kryptografických algoritmov a schopnosť ich implementácie

Skenovanie zraniteľností a penetračné testovanie

Znalosť techník infiltrácie

Vniknutie

Znalosť vektora útoku a automatizovaných nástrojov, ktoré možno použiť

Bezpečnosť a opravovanie

Pochopenie zásad opravovania a osvedčených postupov na zvýšenie bezpečnosti

Monitorovanie

Školenie OSSEC a syslog

Sieťové kontroly

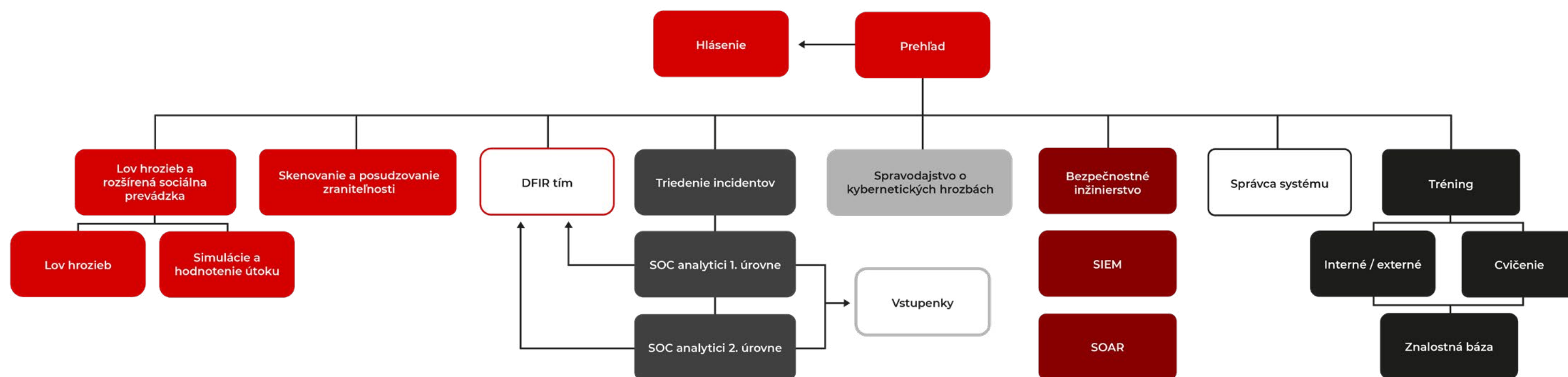
Školenie o technológiách Snort a Suricata

Nástroje a postupy CDC

Školenie OTRS a analógové školenie

Bezpečnostné normy a politiky

Každý z našich analytikov SOC má znalosti v oblasti normy ISO 27K a zásad spoločnosti Binary Confidence



SOC Manager

Náš SOC manager, ktorý má viac ako 15 rokov skúseností v oblasti bezpečnostných operačných centier, pracoval v uznávaných organizáciách vrátane NATO a EÚ. Ako certifikovaný pracovník pre riešenie incidentov, vyniká v strategickom riadení, vedení tímu a zabezpečovaním bezproblémových operácií.

SIEM & Monitoring Expert

Náš expert na SIEM spravuje konfiguráciu, analýzu, nasadenie a podporu systémov. To zahŕňa bezpečnostné riešenia integráciu, vývoj obsahu, analýzu protokolov a riešenie problémov.

CSIRT Leader

Vedúci tímu reakcie na incidenty riadi riadenie bezpečnostných incidentov, najmä v prípade závažného porušenia ochrany údajov. Vďaka silným väzbám na orgány činné v trestnom konaní a právnych expertov náš tím CSIRT spolupracuje so spravodajskými agentúrami na vypátraní a zadržení útočníka.

Threat Hunter

Naši lovci hrozieb sú proaktívni obrancovia, ktorí používajú údaje SIEM na odhaľovanie skrytého škodlivého softvéru. Vyhodnocujú podozrivé vzorce aktivít s cieľom nájsť útočníkov. Proaktívne neutralizujú pokročilé hrozby a opravujú zraniteľnosti, aby zabránili budúcim útokom.

SOC Security Manager

Manažér bezpečnosti SOC je zodpovedný za vytváranie a udržiavanie obranných stratégií, politik a postupov. Zabezpečuje technické vedenie, dohliada na prevádzkové udalosti, kultivuje štruktúrované a komunikatívne tímové prostredie.

SOC Analysts

Oddelenia SOC, ktoré ako prvé reagujú na upozornenia SIEM, sú analytici v prvej línii detekcie hrozieb, analýzy a reakcie na incidenty. Sú primárne zodpovedné za nahlasovanie kybernetických hrozieb a vykonávanie akýchkoľvek zmien potrebných na ochranu infraštruktúry.

Threat Intelligence Expert

Náš expert na analýzu zraniteľnosti a dodržiavanie predpisov posúdi technológiu, systémy, zariadenia a aplikácie v rôznych prostrediach. Proaktívne spolupracuje s SOC tímom pri analýze, určovaní priorít a blokovaní bezpečnostných incidentov. Rieši všetky zraniteľnosti vrátane ich zabezpečenia.

Head of Implementation

Náš špecialista na informačné technológie je zodpovedný za hodnotenie, údržbu a zlepšovanie informačných systémov. Analyzuje a odporúča riešenia na optimalizáciu bezpečnosti siete a zároveň chráni vzdialené routery a firewally.



Upozornenie

Vyhľadávanie hrozieb
Nástroj na registráciu ticketu: monitorovanie / sms / mail / telefón

Vybavovanie ticketov

Maximálny čas:
30 minút registrácia a 30 minút odpoveď

Triage

Protokol: zdroj, história udalostí, zdrojová IP adresa
Zabbix: CPU, pamäť, sieťová prevádzka

Informovať zákazníka

Zákazník informovaný o upozornení do 60 minút.
Hlásenie bezpečnostných incidentov, prevádzkových incidentov a výpadkov.

Správa obsahuje:

- Názov incidentu, číslo ticketu a dotknuté zariadenie
- Čas incidentu
- Cieľ incidentu
- Zdroj škodlivej činnosti
- Stručný opis incidentu a rizika (ak je k dispozícii)
- Záznam o našich činnostiach s časovou pečiatkou

Komunikácia

Všetky informácie a komunikácia

Aktívna reakcia

Tím CSIRT
Druhá línia / kontaktná osoba CERT

Záver

Zmiernenie a uzavretie incidentu

Subject: # BIC-35 - Windows failed login - User01
Incident Reference Number: BIC-35
Site name: ABC-UK Offices Status: New Incident category: Other Date and time: 2023-09-29 16:01:33 Description of the incident: Windows failed login - jsmith Impact: Medium
Actions: 2022-09-29 16:00:00 – Incident ticket created 2022-09-29 16:05:00 – Notification sent
Response : We are experiencing a large number of unsuccessful login attempts by “User01” against “dduser.abc.eu”. This is most likely an unchanged expired password. Please check, and get in contact.

Example Monthly Status Report

Executive Summary - Overall situation: stable
Three incidents registered during January, one security breach detected. Security incident report in attachment.

Devices Summary

Number of Logs: 105 754 650

Total Volume of Logs Received: 243.2 GB

Security Devices

Name	Number of Logs	Volume of Logs	Incidents
Suricata	250 000 000	130 GB	1
Fortiweb	1 000 000	900 MB	0
Sophos UTM	50 000 000	27 GB	0

Network Devices

Name	Number of Logs	Volume of Logs	Incidents
CISCO Aironet	750 000	100 MB	0
SW1	500	200 KB	0
SW2	1500	1 MB	0

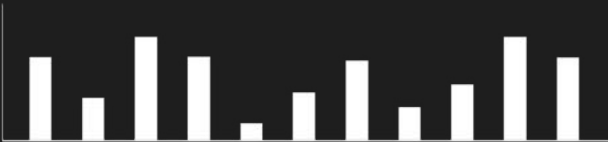
Endpoints

Name	No. Windows Logs	No. DLP Logs	Volume	Incidents
ADC01	80 000 000	200	45 GB	0
webster	21 000 000	500	25 GB	1
webster-backup	4 000 000	30	15 GB	0

Honeypots

Name	Number of Logs	No. Alerts	Volume of Logs	Incidents
H001	500	0	20 KB	0
H002	150	90	35 KB	0
H003	2 000	1 500	100 KB	0

Logs in Time



Top Log Hosts



Security Events

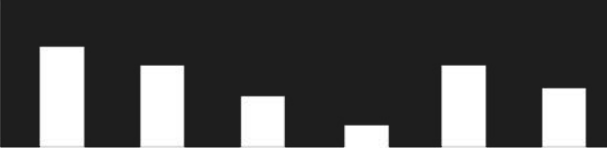
Incident Table

ID	Incident Name	Severity	Status	Root Cause
INC-13	Trojan found in Chrome plugin	Medium	Resolved	Blacklist not effective -> fw upgrade
INC-14	Phishing followed by malware execution	High	Info needed	Unknown
INC-15	Linux Kernel vulnerability CVE-2022-0847 (Dirty Pipe)	High	Resolved	Unpatched Linux Kernel versions

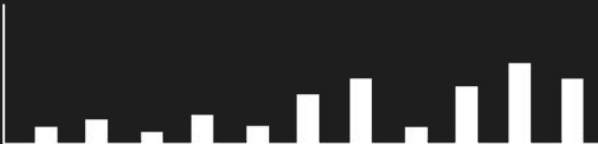
Incident History



Volume History



SIEM Alerts in Time



Top SIEM Alerts

Signal Rule	Count
Antivirus rule match	5 000
Access to site known to contain malware	2 000
Successful login outside business hours	1 500

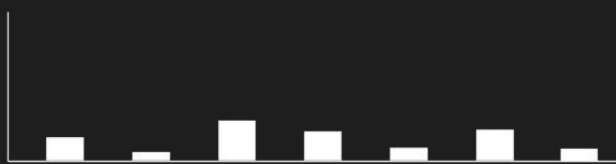
DLP Server



DLP Device Types



DLP Device Types



DLP Connected Devices

Time	User	Device Type	Device Name
01.01.2022 09:30:00	M.Edwards	USB Modem	HUAWEI Mobile Connect - 4G Modem
01.01.2022 14:50:00	S.Parker	Additional Keyboard	HID Keyboard Device
02.01.2022 11:20:00	D.Robinson	Webcam	Logitech Camera

Availability

Availability: 99.96 %

Downtime: 15 Minutes

Incident ID	Incident Name	Start	End	Duration	Root Cause
INC-16	Missing logs from Fortiweb	18.01.2022 13:15:00	18.01.2022 13:30:00	15 Minutes	Firewall Upgrade

Vulnerability Management

Vulnerability Summary:

Several High severity vulnerabilities detected in PC network, caused mainly by hosts with missing important patches.
Multiple servers with CVE-2022-0847 vulnerability, caused by unpatched Linux Kernel versions.

Report per Device

Security Devices

Device Name: Webster

IP Address: 192.168.24.12

Status: High

▼

Incidents

ID	Incident Name	Severity	Status	Root Cause
INC-15	Linux Kernel vulnerability CVE-2022-0847 (Dirty Pipe)	High	Resolved	Unpatched Linux Kernel versions

Number of Logs: 21 000 000

No. DLP Logs: 500

Volume of Logs: 25 GB

Logs in Time

Period	Logs
1	1000000
2	1500000
3	1800000
4	1200000
5	800000
6	1600000
7	1700000
8	1100000
9	2000000
10	1600000
11	1300000
12	1000000

Authentication Failure

Location	Count
North America	1000000
Europe	800000
Asia	600000
Africa	400000
Oceania	200000

Kontaktujte Nás

Slovanet je jedným z najväčších telekomunikačných operátorov na Slovensku.

Sme slovenská spoločnosť, ktorá prichádza na náš trh s najnovšími technologickými inováciami. Na našich chodbách sa môžete stretnúť so zakladateľmi a súčasnými majiteľmi spoločnosti. Ponúkame jedinečnú atmosféru, ľudský prístup a priateľské vzťahy.

Poskytujeme širokú škálu telekomunikačných služieb a komplexných riešení pre firmy. Pôsobíme v rôznych segmentoch zákazníkov - od domácností a malých firiem až po veľké korporácie.

slovanet.net

info@slovanet.net

+421 2 208 28 111