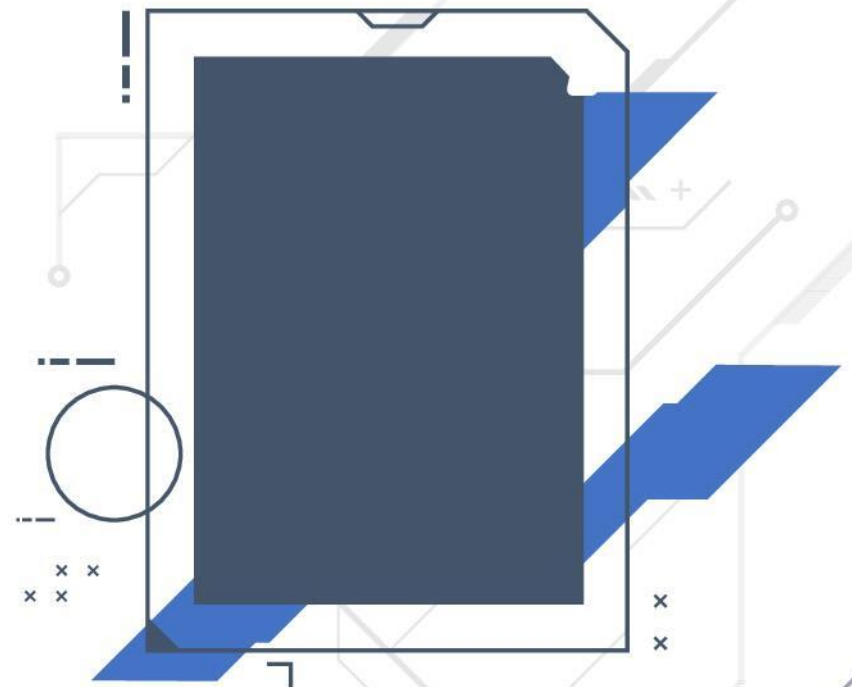



بسم الله الرحمن الرحيم

# گزارش عملکرد

زمستان 1403





01  
مروری سریع بر آنچه  
در سه ماه اخیر انجام  
شد.

02  
وضعیت پیشرفت  
دسترسی‌های حائز  
اهمیت

03  
وضعیت کلی  
دسترسی‌ها

04  
تغییرات در مدیریت پروژه

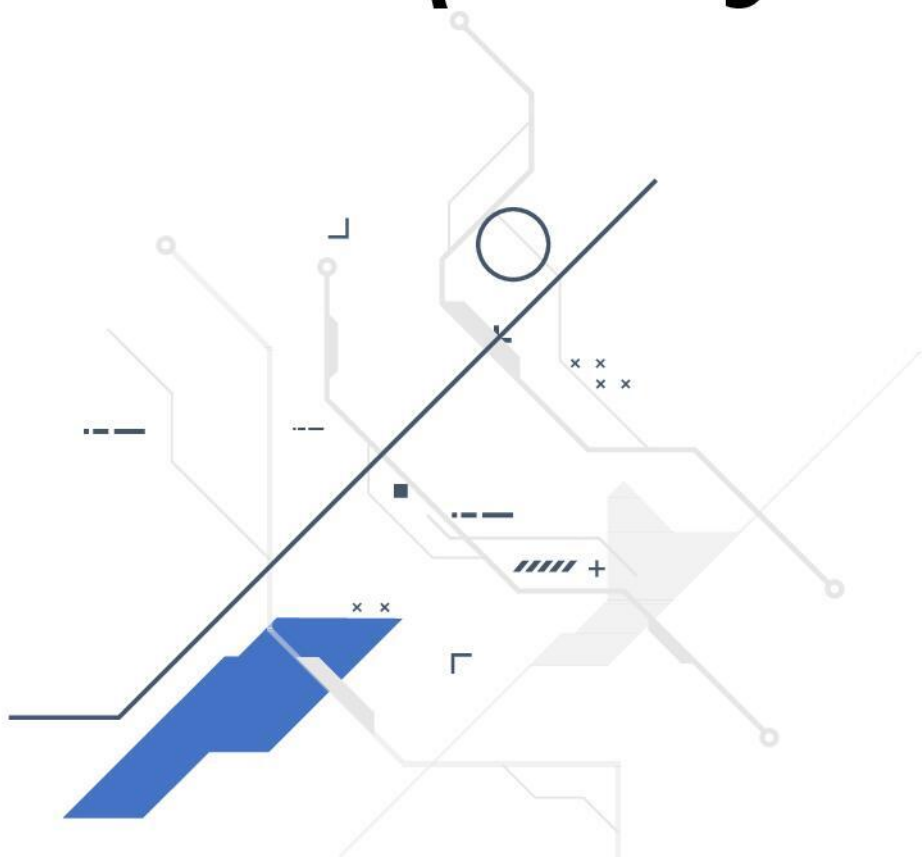
05  
پیشرفت‌ها

07  
پیشنهادهای  
نیازمندی‌ها -

01

# مروری سریع بر آنچه سه ماه اخیر انجام شد.

خلاصه اقدامات و نتایج



# گسترش سطوح دسترسی به صورت دقیق و عمیق

▪ اجرای حملات پیشرفته در سطح اکتیو دایرکتوری به

صورت کامل

▪ پیشرفت در دور زدن سیستم های امنیتی پیشرفته SentinelOne-Sophos-

TrendMicro

▪ تخلیه اطلاعات به صورت دقیق و با کمترین درصد خطا

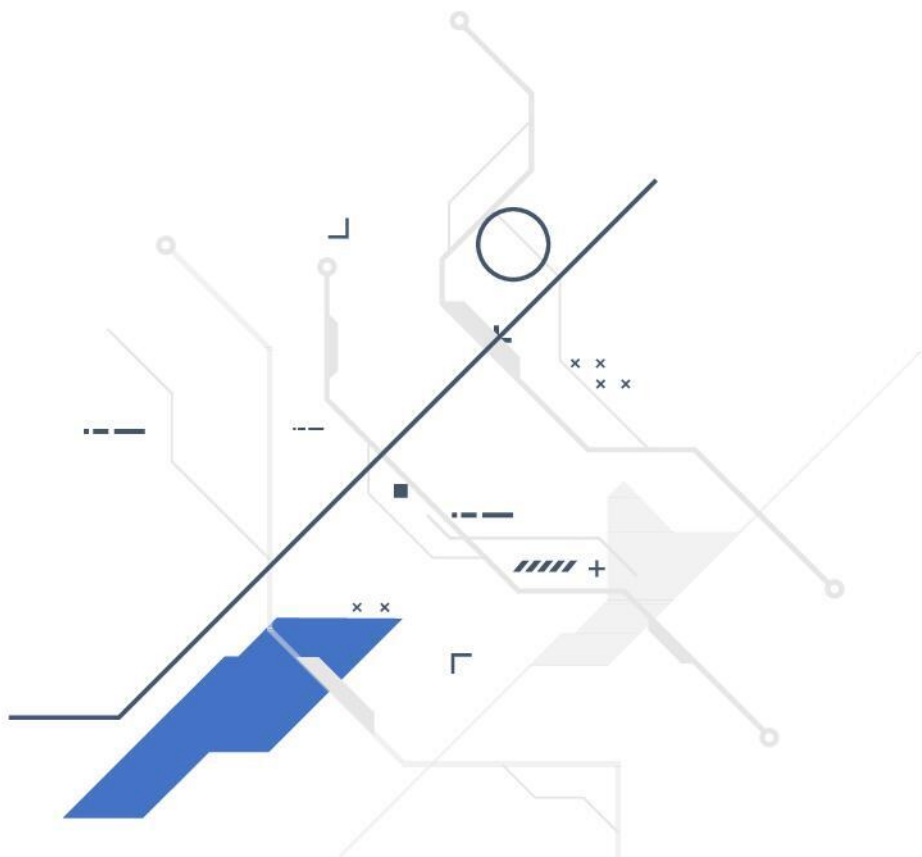
▪ اجرای حملات SupplyChain



02

# وضعیت کلی دسترسی‌ها

حترین وضعیت و نتایج اقدامات صورت گرفته



## هدف Qistas

- دسترسی کامل به تمام زیرساخت شبکه به صورت کامل
- دسترسی به زیرساخت پشتیبان گیری Local + Cloud
- تخلیه داده به صورت مستمر
- اخذ دسترسی از شرکت همکار با استفاده از لینک ارتباطی بین دو شرکت



## هدف Qistas

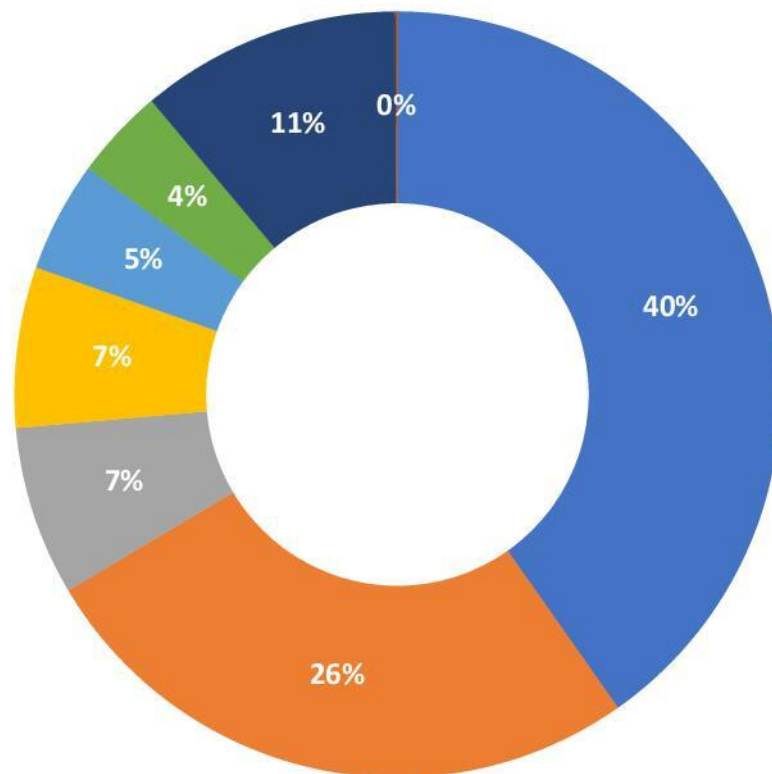
- استخراج کامل پایگاه داده شرکت هدف
- در داده های استخراج شده میتوان به لیست کامل مشتریان (قضات فعال و مشتریان در کشورهای مختلف امارات + اردن و غیره)
- فایل مکالمات صوتی از ابتدای 2023 تا به امروز
- محتویات ایمیل های کارکنان
- تا کنون در گزارش تکمیلی نسخه 4 فایل پیوست حدود 74 گیگ داده تحویل شده است.



# هدف Qistas

## داده های استخراج شده

- |                       |                             |                       |                   |
|-----------------------|-----------------------------|-----------------------|-------------------|
| ■ Mail Files          | ■ Backup File               | ■ Program Files       | ■ Image Files     |
| ■ Miscellaneous Files | ■ Office Files and Document | ■ Audio Files         | ■ Container Files |
| ■ Database Files      | ■ Text Files                | ■ Configuration Files |                   |







# نمونه داده‌های استخراج شده از Qistas

- اطلاعات موجود از قضات کشور اردن و فلسطین
- اطلاعات موجود از وکلا کشور اردن ، کویت ، عربستان سعودی ، امارات در داده های استخراج شده از پایگاه داده موجود در شبکه هدف - اطلاعات شامل نام ، نام خانوادگی ، ایمیل ، شماره تماس میباشد.





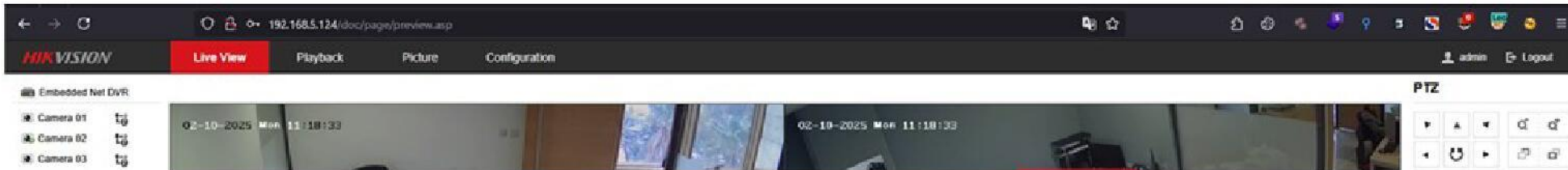
# نمونه داده‌های استخراج شده از Qistas

- اطلاعات موجود از قضات کشور اردن و فلسطین
- اطلاعات موجود از وکلا کشور اردن ، کویت ، عربستان سعودی ، امارات در داده های استخراج شده از پایگاه داده موجود در شبکه هدف - اطلاعات شامل نام ، نام خانوادگی ، ایمیل ، شماره تماس میباشد.



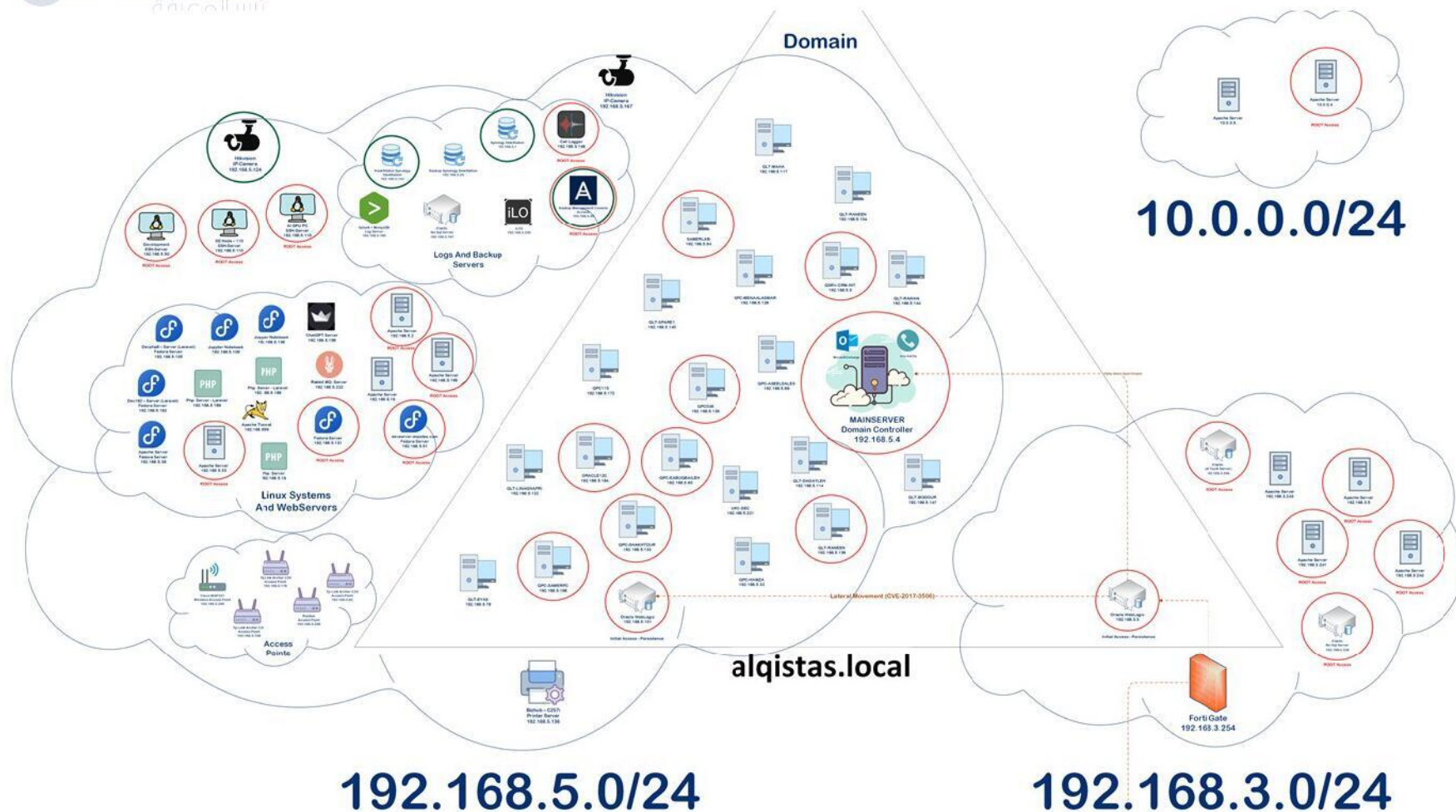
# نمونه داده‌های استخراج شده از Qistas

- لیست کامل کارمندان سازمان
- اطلاعات احراز هویت در تمامی وبسایت های کاری و غیره
- تصاویر دوربین های سازمان به صورت کامل



# نمونه داده‌های استخراج شده از Qistas

▪ کنترل کامل زیرساخت



# نمونه داده‌های استخراج شده از Qistas

■ لیست کامل اطلاعات رمز عبور

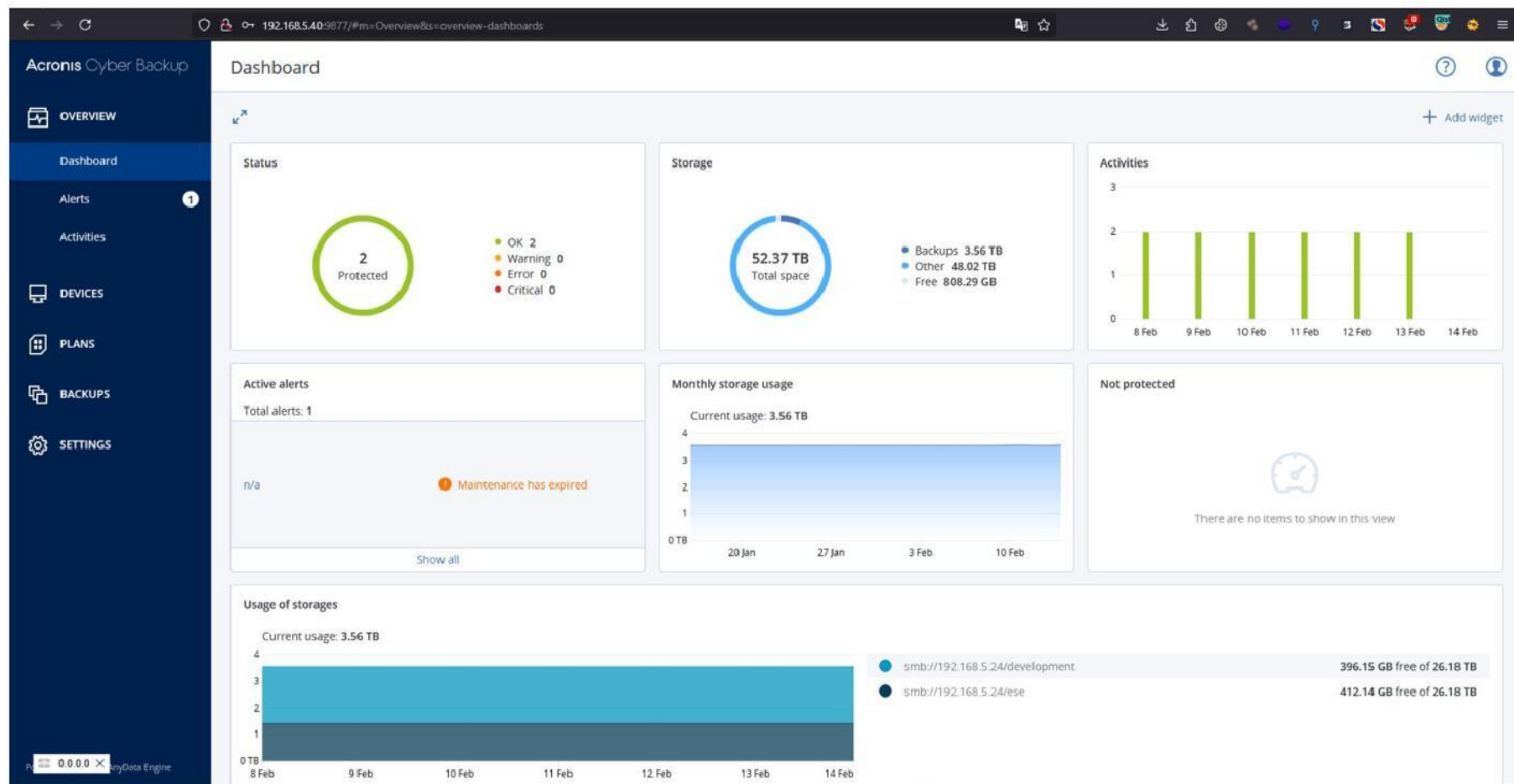
ردیف	عنوان اطلاعات	آدرس سرور یا دامنه
۱	Web Server - Root	۱۹۲.۱۶۸.۳.۵:۲۲
۲	Web Server	۱۹۲.۱۶۸.۳.۲۴۱:۲۲
۳	Web Server	۱۹۲.۱۶۸.۳.۲۴۲:۲۲
۴	V1 Admin	۱۹۲.۱۶۸.۵.۳۳:۲۲
۵	<u>Umniah</u>	۱۹۲.۱۶۸.۵.۲۲۱:۳۳۸۹
۶	Sophos End Point Server - Sophos2	۱۹۲.۱۶۸.۵.۵:۳۳۸۹
۷	Sophos End Point Server - Sophos	۱۹۲.۱۶۸.۵.۵:۳۳۸۹
۸	Sophos End Point Server - Administrator	۱۹۲.۱۶۸.۵.۵:۳۳۸۹





# نمونه داده‌های استخراج شده از Qistas

▪ دسترسی کامل از زیرساخت بکاپ





# نمونه داده‌های استخراج شده از Qistas

▪ دسترسی کامل از زیرساخت بکاپ بر بستر Cloud

KROME

AI Qistas

Manage

AI Qistas

MONITORING

DEVICES

31

MANAGEMENT

SOFTWARE MANAGEMENT

PROTECTION

BACKUP STORAGE

Backups

REPORTS

SETTINGS

1

Search by name and path

Locations

Occupied space: 71.9 GB  
Available space: 9.23 TB

Occupied space: 11.4 GB  
Available space: 0 bytes

Occupied space: 993 GB  
Available space: 0 bytes

Occupied space: 380 GB  
Available space: 0 bytes

Occupied space: 742 GB  
Available space: 0 bytes

Occupied space: 594 GB  
Available space: 0 bytes

Occupied space: 0 bytes  
Available space: 7.52 TB

Add location

Locations

Selected: 1 / Loaded: 29 / Total: 29

Type	Name ↑	Location	Host	Capacity	Number of backups
	//192.168.5.143/WebDB/	//192.168.5.143/WebD...	webdb.alqistas.co...	9.23 TB free of 10.8 TB	1
	\\192.168.5.23\CRM-Backup	//192.168.5.23\CRM-B...		0 bytes free of 6.98 TB	1
	\\192.168.5.23\Domain Bac...	//192.168.5.23/Domai...	MainServer.alqist...	0 bytes free of 6.98 TB	1
	\\192.168.5.23\Oracle DB B...	//192.168.5.23\Oracle ...		0 bytes free of 6.98 TB	1
	\\192.168.5.23\SEV2	//192.168.5.23\SEV2/		0 bytes free of 6.98 TB	1
	\\192.168.5.23\SEV3	//192.168.5.23\SEV3/		0 bytes free of 6.98 TB	2
	\\192.168.5.23\SVE2	//192.168.5.23\SVE2/		7.52 TB free of 7.85 TB	0
	\\192.168.5.23\Web-DB-Bac...	//192.168.5.23\Web-D...		1.60 GB free of 6.98 TB	1
	\\192.168.5.23\Web-Svr-Bac...	//192.168.5.23\Web-Sv...		0 bytes free of 6.98 TB	1
	\\192.168.5.24\CRM-Backup	//192.168.5.24\CRM-B...	192.168.5.24	13.2 TB free of 26.2 TB	1
	\\192.168.5.24\Zoho\	//192.168.5.24\Zoho\	192.168.5.24	26.2 TB free of 26.2 TB	0
	MainServer.alqistas.local: \\...	//192.168.5.24/Domai...	192.168.5.24	23.9 TB free of 26.2 TB	1
	nharam@qistas.com	Cloud storage			0
	qse1.qistas.com: \\192.168...	//192.168.5.24/SEV3/	192.168.5.24	24.4 TB free of 26.2 TB	1
	se.alqistas.com: smb://192...	//192.168.5.24/SEV2/	192.168.5.24	6.56 TB free of 26.2 TB	1
	smb://192.168.5.23/DMS-B...	//192.168.5.23/DMS-B...	192.168.5.23	0 bytes free of 6.98 TB	1

Add location

Add location

Details

Rename

Delete

0.000 X

Byte Platform



# سازمان iblaw

این مجموعه یکی از بزرگترین موسسات حقوقی در اردن میباشد که تشکیل شده از تیم وکلا و مشاورین حقوقی میباشد. این موسسه خدماتی همچون: خدمات تجاری و ثبت شرکت ها، تنظیم دادخواست، مالکیت معنوی و پیش نویس نظارتی و قانون گذاری ارائه میکند و مشتریان آن شامل بخش های خصوصی و دولتی، املاک و مستغلات، سرمایه گذارهای خارجی میباشد. لازم به ذکر است که این موسسه در سال 1997 توسط دکتر صلاح‌الدین البشیر تأسیس شد و تا کنون مشغول به کار در زمینه حقوقی میباشد.







- Abu Dhabi Future Energy Company (Masdar)
- AECOM
- Al-Hikma Pharmaceuticals
- American Bar Association
- Alstom Switzerland LTD Al-Fakher for Tobacco Trading
- Airport International Group (AIG)
- Arabtech Jardaneh
- Aramex
- Arij Company for Media Workshop
- Aqaba Container Terminal Company (ACT)
- Aqaba Development Corporation (ADC)
- Brinks EMEA
- Bureau Veritas
- Chemonics International Inc.
- Campero International
- Corporate Security Solutions, Inc.
- Columbia University Middle East Research Center
- CPCS
- Daimler AG
- Danish Refugee Council
- Development Alternatives, Inc. (DAI)
- Ford Middle East
- Hunland Trade Kft
- International Oil Trading Company
- International Organization for Migration (IOM)
- International Rescue Commission (IRC)
- International Relief and Development (IRD)
- Iraq Foundation
- Islamic Insurance Company
- JA Worldwide ("JAW")
- Jordan Investment Trust P.L.C
- Jordan Taekwondo Federation
- KINGDOM Electricity for Energy Investments (PSC)
- Laboratory Corporation of America (LabCorp)
- United States Agency of International Development (USAID)
- Van Oord Dredging and Marine Contractors
- VTEL Middle East & Africa
- Zain Jordan

- Lutheran Medical Center
- LVMH Holding
- Madaba Institute for Mosaic Art & Restoration
- Mafrag Development Corporation
- Ma'an Development Company (MDC)
- Mashreq bank PSC
- North Development Corporation
- MENA Cleantech AG
- MENA Venture Investments
- Microsoft
- Microsoft Jordan PSC
- Middle East Payment Services (MEPS)
- Mitsubishi Electric Building Techno-Service Co., Ltd
- Mubadala Development Co.
- Nile Projects & Trading Co.
- Nokia Corporation
- Norwegian Refugee Council (NRC)
- Overseas Private Investment Corporation (OPIC)
- Philip Morris International
- Privatization Holding Co. (PHC)
- Ruwwad Micro-Venture Fund
- Solvochem B.V.
- SunEdison LLC
- The European Bank for Reconstruction and Development (EBRD)
- The Housing Bank for Trade and Finance
- The Jordanian Electric Power Co. Ltd. (JEPCO)
- Total Outre Mer S.A.
- True Blue, Inc.
- United Nations Conference on Trade and Development (UNCTAD)

## مشتريان iblaw



# مشتریان iblaw

- مرکز تحقیقات خاورمیانه دانشگاه کلمبیا
- شورای پناهندگان دانمارکی
- بانک اروپا برای بازسازی و توسعه (EBRD)
- بانک مسکن برای تجارت و امور مالی
- شرکت برق اردن برقی با مسئولیت محدود (JEPCO)
- کنفرانس تجارت و توسعه سازمان ملل متحد (UNCTAD)
- آژانس توسعه بین المللی ایالات متحده (USAID)
- شرکت سرمایه گذاری خصوصی در خارج از کشور (PSC)
- خدمات پرداخت خاورمیانه (MEPS)
- پروژه نیل و سرمایه گذاری
- شرکت نوکیا
- شورای پناهندگان نروژی (NRC)
- شرکت انرژی آینده ابوظبی (MASDAR)
- کانون وکلای آمریکا
- گروه بین المللی فرودگاه (AIG)
- شرکت بین المللی تجارت نفت
- سازمان بین المللی مهاجرت (IOM)
- بنیاد عراق
- شرکت بیمه اسلامی
- برق پادشاهی برای سرمایه گذاری انرژی
- شرکت آزمایشگاهی آمریکا (LABCORP)
- مرکز پزشکی لوتران
- بانک مشرق
- نمایندگی مایکروسافت در اردن



# نمونه داده‌های استخراج شده از مشتریان

بسم الله الرحمن الرحيم

بسم الله الرحمن الرحيم

المملكة العربية السعودية

الهيئة العامة للغذاء والدواء

قرار من مجلس الوزراء



قرار رقم : (١٤١)

وتاريخ : ١٤٣٩/٣/١٠ هـ

المملكة العربية السعودية  
الهيئة العامة للغذاء والدواء

قرار من مجلس الوزراء



قرار رقم : (١٠٥)

وتاريخ : ١٤٤٠/٢/١٤ هـ

+

x x  
x x

# نمونه داده‌های استخراج شده از مشتریان iblaw

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



الملك عبدالعزيز آل سعود  
الأمير محمد بن سلمان بن عبدالعزيز آل سعود

مجلس الوزراء

قرار رقم : (١٠٥)  
وتاريخ : ١٤٤٠/٢/١٤ هـ

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



الملك عبدالعزيز آل سعود  
الأمير محمد بن سلمان بن عبدالعزيز آل سعود

مجلس الوزراء

قرار رقم : (١٤١)  
وتاريخ : ١٤٣٩/٣/١٠ هـ

+

x x  
x x



# نمونه داده‌های استخراج شده از مشتریان iblaw

العربية للطيران الأردن  
air arabia jordan

Al Najah Building 47, Shaker Bin Zaid str., Al Shmeisani  
Amman - Hashemite Kingdom of Jordan  
P.O.Box: 923366 Amman, 11192 Jordan  
Tel : +962 6 569 6100  
Fax: +962 6 569 6101

التاريخ : 2017/02/06

الرقم: JAD/RL/CEO013/2017

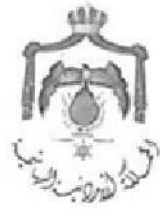






# نمونه داده‌های استخراج شده از مشتریان iblaw

The Hashemite Kingdom Of Jordan  
Civil Aviation Regulatory Commission



المملكة الأردنية الهاشمية  
هيكلة تنظيم الطيران المدني

Ref. : .....

Date : .....

الرقم : ٥٨٩ / ٥٠٠٦ / ١٢

التاريخ : ٨ / ٢ / ٢٠١٧

سري وعاجل

سعادة مدير عام شركة العربية للطيران الأردن





# نمونه داده‌های استخراج شده از مشتریان iblaw

عطوفة الكابتن هيثم مستو المحترم  
رئيس مجلس المفوضين  
هيئة تنظيم الطيران المدني

الإشارات:

- كتابكم رقم 492/5006/12 المستلم بتاريخ 2017/02/05

الموضوع: حرس الجو - توقيع الاتفاقية





# نمونه داده‌های استخراج شده از مشتریان iblaw

التاريخ : ٢٠١٧/١٢/١٩

سري وعاجل

سعادة مدير عام الشركة الأردنية للطيران  
سعادة مدير عام شركة العربية للطيران الأردن





# نمونه داده‌های استخراج شده از مشتریان iblaw



الأردن  
هيئة الاستثمار

رقم: C/118 / 21412  
تاريخ: C.19 1914

السادة شركة مايكروسوفت / الاردن م. خ

# نمونه داده‌های استخراج شده از مشتریان iblaw

The Hashemite Kingdom of Jordan  
Investment Commission



المملكة الأردنية الهاشمية  
هيئة الاستثمار

رخصة ممارسة نشاط اقتصادي  
License of practicing economic activity

Investor No.	77
License No.	5613111303
License Class	First
License for	2019

رقم المستثمر	٧٧
رقم الرخصة	٥٦١٣١١١٣٠٣
فئة الرخصة	الاولى
رخصة لعام	٢٠١٩



# نمونه داده‌های استخراج شده از مشتریان iblaw





# استخراج اطلاعات زیرساخت iblaw

## Servers Details

### Servers Information:

Server Name	Server IP	Server Functionality
DC01	192.168.0.2	Primary Domain Controller
DC02	192.168.0.3	Secondary Domain Controller
Mail	192.168.0.4	Exchange Server
FileSRV01	192.168.0.6	File Server
AppSRV	192.168.0.7	Application Server (Time Sheet)
OracleSRV	192.168.0.8	Oracle Application (Qistas)
SophosFireWall	192.168.0.5:4433	Firewall \ Network Gateway
Conference Sys PC	192.168.4.230	Conference Sys Management
Surveillance DRV	192.168.0.12	Cameras Control System
Veeam SERVER	11.12.13.14	Veeam Backup SERVER
SyncServer	192.168.0.239	SyncSERVER
Synology DiskA	11.12.13.110	DiskA
Synology DiskB	11.12.13.111	DiskB
Synology DrHome	192.168.30.30	DrHome

### IBLAW Internet Link Information:

Info	Value
Domain Name	iblaw.com.jo
ISP	DamaMax
Customer ID	2910-150-04
Link Type	Fiber Link 50M
IP Range	82.212.94.91 – 82.212.94.94
Network	82.212.94.89 /29
WAN IP (Registered Domain)	82.212.94.90
Gateway	82.212.94.89
Subnet Mask	255.255.255.248
DNS 1	82.212.67.100
DNS 2	82.212.67.101





سویس للصرافة

## صرافی Swiss Exchange

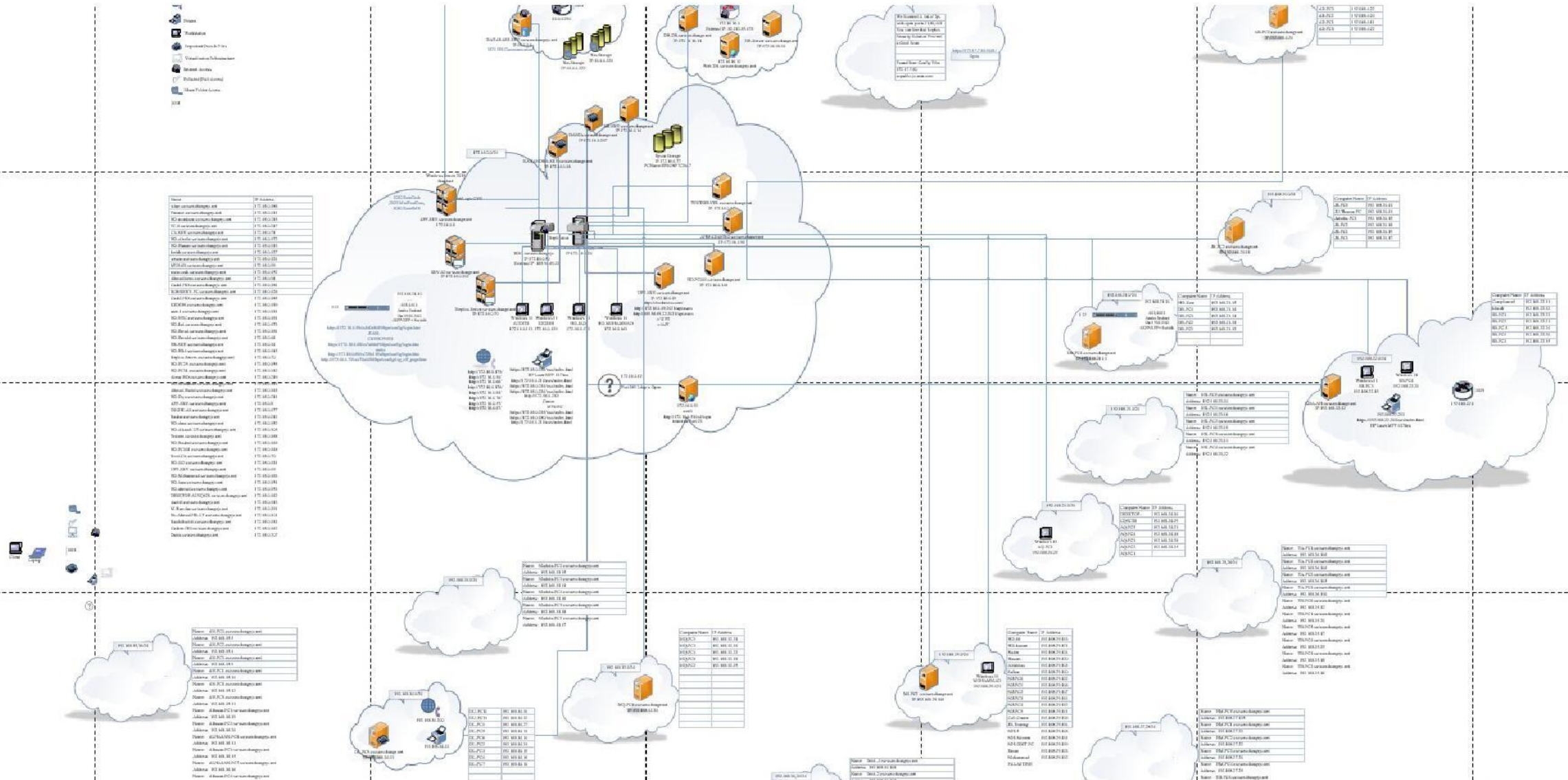
- ایجاد حساسیت در شبکه هدف و لزوم به توقف موقت اقدامات
- طی بررسی های انجام شده بر روی شبکه هدف تغییرات بسیاری در شبکه رخ داده است. به عنوان مثال تغییر در زیرساخت، خاموش کردن سرورهای بلا استفاده و غیره.
- تغییر زیرساخت هدف و ایجاد محدودیت به دسترسی تنها از کشور اردن.
- در زمان توقف اقدام به توسعه ابزارهای لازم انجام شد.
- افزایش و گسترش دسترسی در حال انجام می باشد.







# کنترل کامل زیرساخت



# شبکه GOV

■ در پروژه نفوذ به زیرساخت GOV از 3 جهت به شبکه زیرساخت دولتی دسترسی وجود دارد.

■ 1. از طریق شبکه IJL

■ 2. از طریق شبکه JEDCO

■ 3. از طریق شبکه CSB

■ مشکلات در شبکه GOV

■ استفاده از TrendMicro

■ پایش و تست نفوذ شبکه به صورت مستمر

■ عدم امکان استفاده از آسیب پذیری های پابلیک

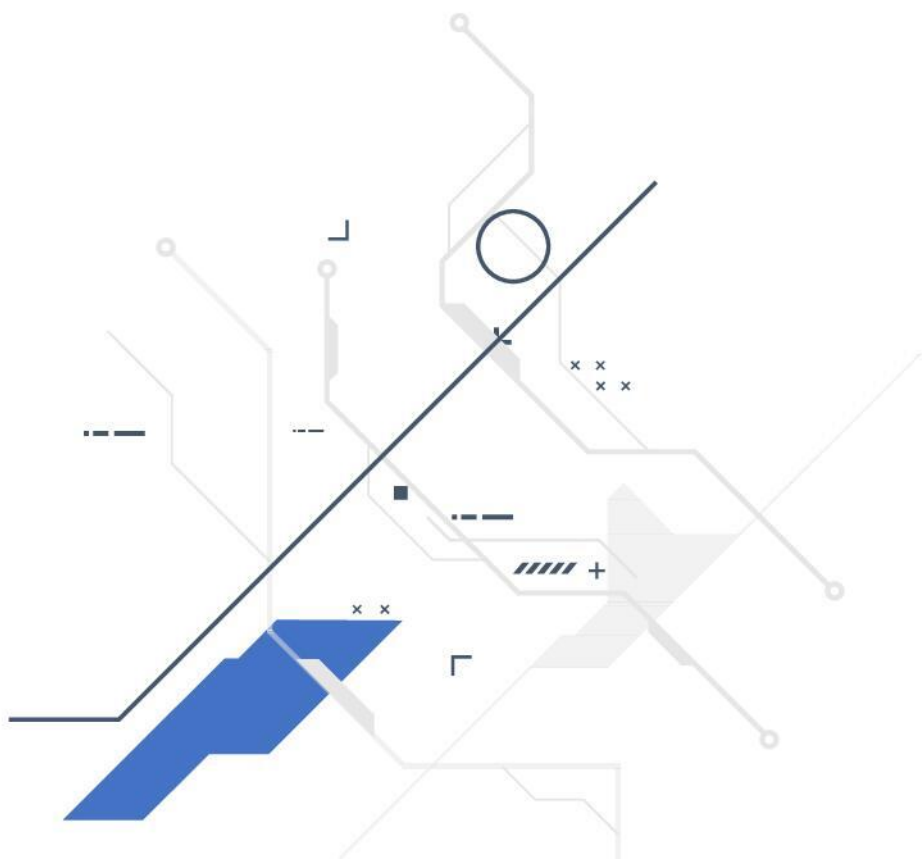
■ حساسیت در اتصال



04

# تغییرات در مدیریت پروژه

---





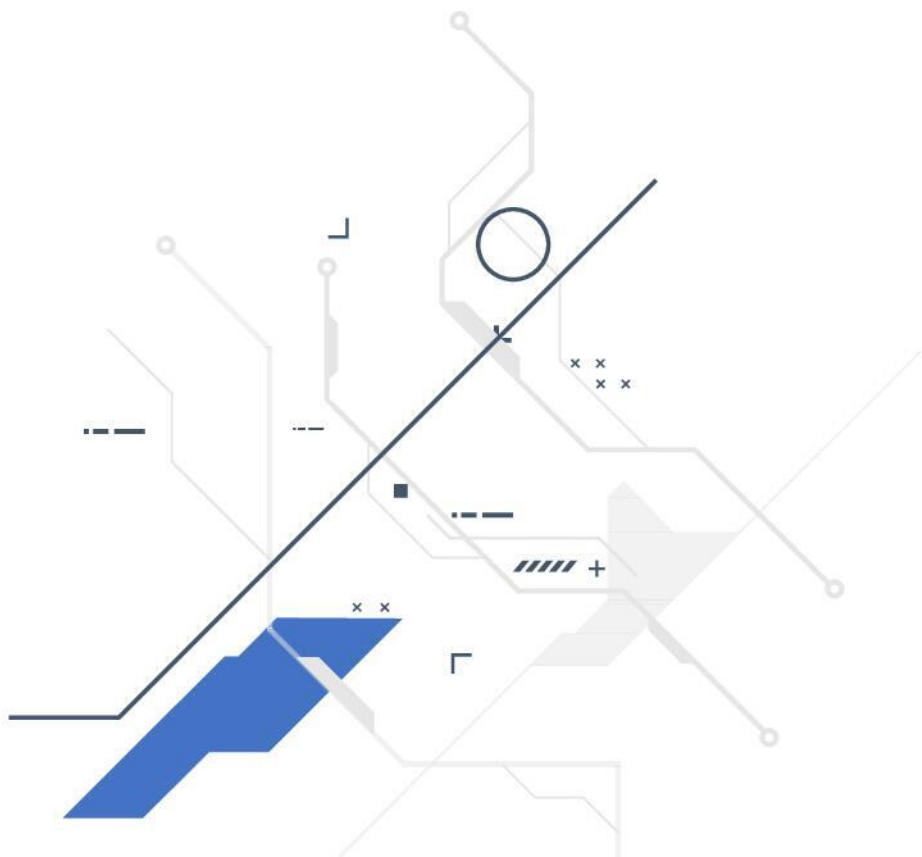
- تخلیه پروژه های قدیمی و تمام شده از مدیریت پروژه
- جمع آوری اطلاعات قدیمی و پشتیبان گیری از سامانه مدیریت پروژه
- ایجاد محدودیت بیشتر در داده های ثبت شده در سامانه مدیریت پروژه



05

# پیشرفت‌ها

---



- تکمیل شبکه آزمایشگاه
- نصب ماشین‌های بروز EDR و ضدبدافزارهای مطرح
  - Sophos
  - TrendMicro
  - CrowdStrike
  - SentinelOne
- بروزرسانی سامانه CCTV - افزودن دسترسی های VNC
- افزایش توانمندی در نفوذ به اهداف
- بقای دسترسی بهت

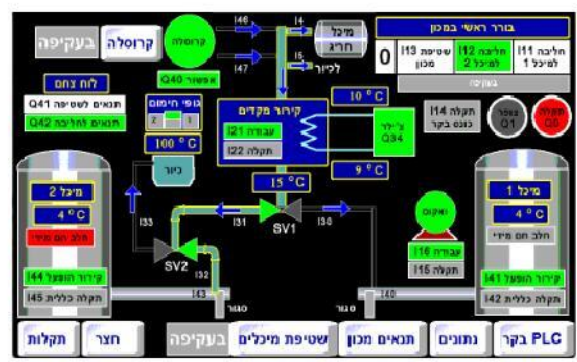


- Home
- CCTV
- VNC/SCADA

- Access List
- Bookmarks
- Servers
- Exploit
- Proxy Manager

Home / Explore

2.55.70.160



Datalist :

ip: 2.55.70.160  
Port : 5900  
Username : empty  
Password : 0

Active

46.210.113.178

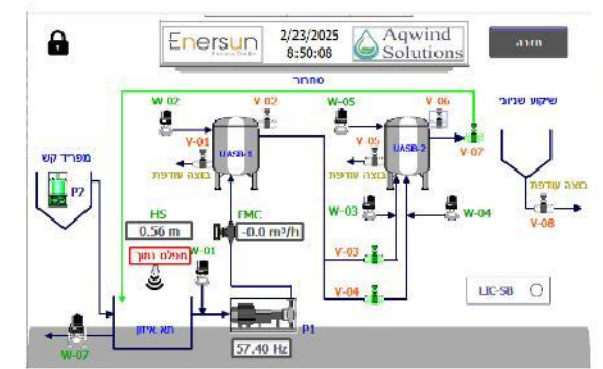


Datalist :

ip: 46.210.113.178  
Port : 5900  
Username : empty  
Password : 2322

Active

46.210.118.112



Datalist :

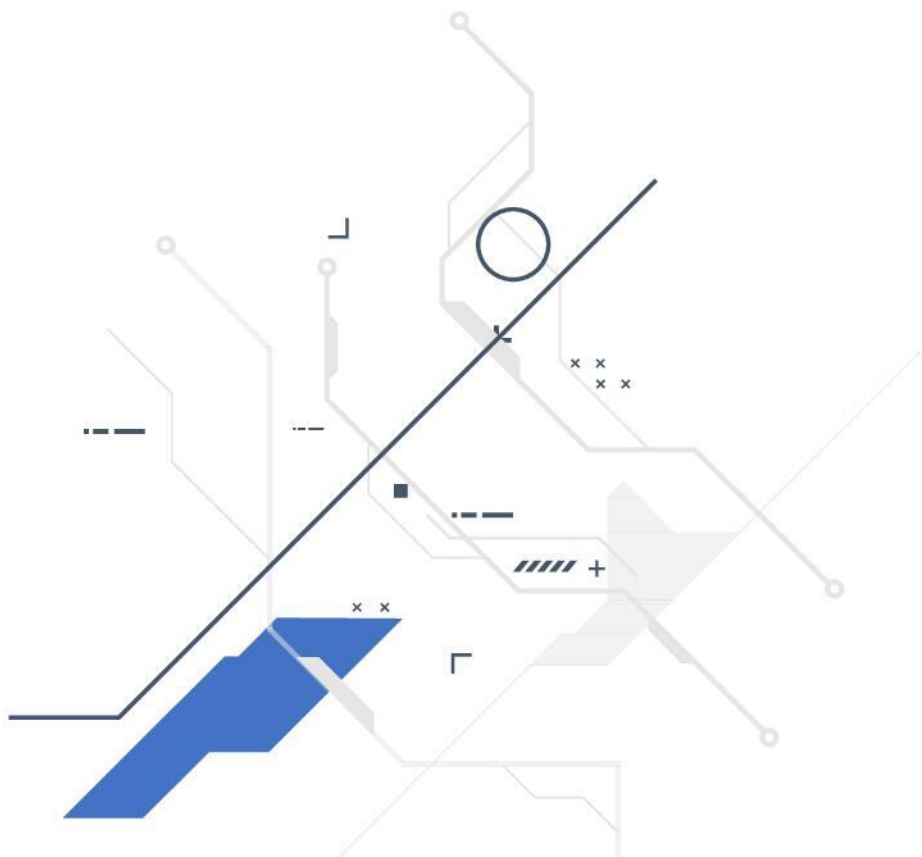
ip: 46.210.118.112  
Port : 5900  
Username : empty  
Password : 2468

Active

06

# پیشنهادات و نیازمندی‌ها

---



# نیازمندی ها

✓ تخصیص تلفن همراه + سیم کارت خارجی

✓ تجهیزات:

✓ هارد SSD + مانیتور

✓ سرویس کولینگ تجهیزات (CPU)

# و من الله التوفيق

---

زمستان 1403