Wise-Mon
MONITORING SOLUTIONS

בקרת גישה לרשת

Network Access Control

אתה יודע מי מחובר ברשת ?

רשת הטרוגנית

- יצרני ציוד שונים
- ריבוי סוגי התקנים
  - שעוני נוכחות
  - מכונות מזון

זמינות הרשת

- בכל חדר בארגון קיימת גישה לרשת
- כמעט בכל מסדרון קיים ציוד מחובר לרשת

מצפון תפתח הרעה ???

- **הגנות**
  - פיירוול – מגן מבחוץ פנימה
  - מגן ברמת הרשאות וגישה אפליקטיבית בתוך הארגון
- **חיבורים חדשים בתוך הרשת לא מנוטרים**
- **במידה ומנוטרים – לא מפוקחים**
  - בודקים זמינות רכיבי רשת קריטיים בלבד
  - ניתן לנתק רכיב מחובר ולחבר במקומו התקן לא מורשה

המטרה

- **מניעת גישה לא מורשית לרשת המקומית**
- **אימות ראשוני של רכיבי רשת**
  - האם התחנה ארגונית ?
  - האם ההתקן מוכר ?
- **אימות משני**
  - תקינות רכיבי אבטחה
  - שעות פעילות
  - מיקום פיסי
  - מערכות הפעלה
  - משתמשים

סוגי פתרונות אפשריים

- 802.1x
- Agent base
- Software NAC

802.1x

- תהליך נטמעה מורכב ומסורבל
- מחייב הקמת תשתית ייעודית – CA
- מימוש תעודות ברמת מחשב בלבד
- לא ניתן לנטר / לטפל תחנה בעיתית
- אין קשר למיקום פיסי
- ללא פתרון לחריגים (אורחים) - מחייב השארת פרצות

Agent base

- כיסוי חלקי – מיועד לסביבה מנוטרת בלבד
- שדרוג רכיבי קצה, ביצועים!
- ללא פתרון לחריגים
- כניסות במתג חשופות

Software NAC

- מימוש מיידי ללא שינויים בתשתית הרשת
- משתמש ביכולות מובנות במתגים
- פרוטוקולים סטנדרטיים
- התקנה והטמעה פשוטים

SWAT תפיסה

- ניהול גישה וחיבור התקנים לרשת
- ניהול התקנים שמתחברים ולא מתגים
- כל התקן שמתחבר לרשת מסווג על פי בדיקות FP
- כל התקן חייב להתאים לפרופיל הארגוני על פי סוג הרכיב
- פעולת ברירת מחדל על רכיבים לא מסווגים
- בדיקות בשכבה שניה

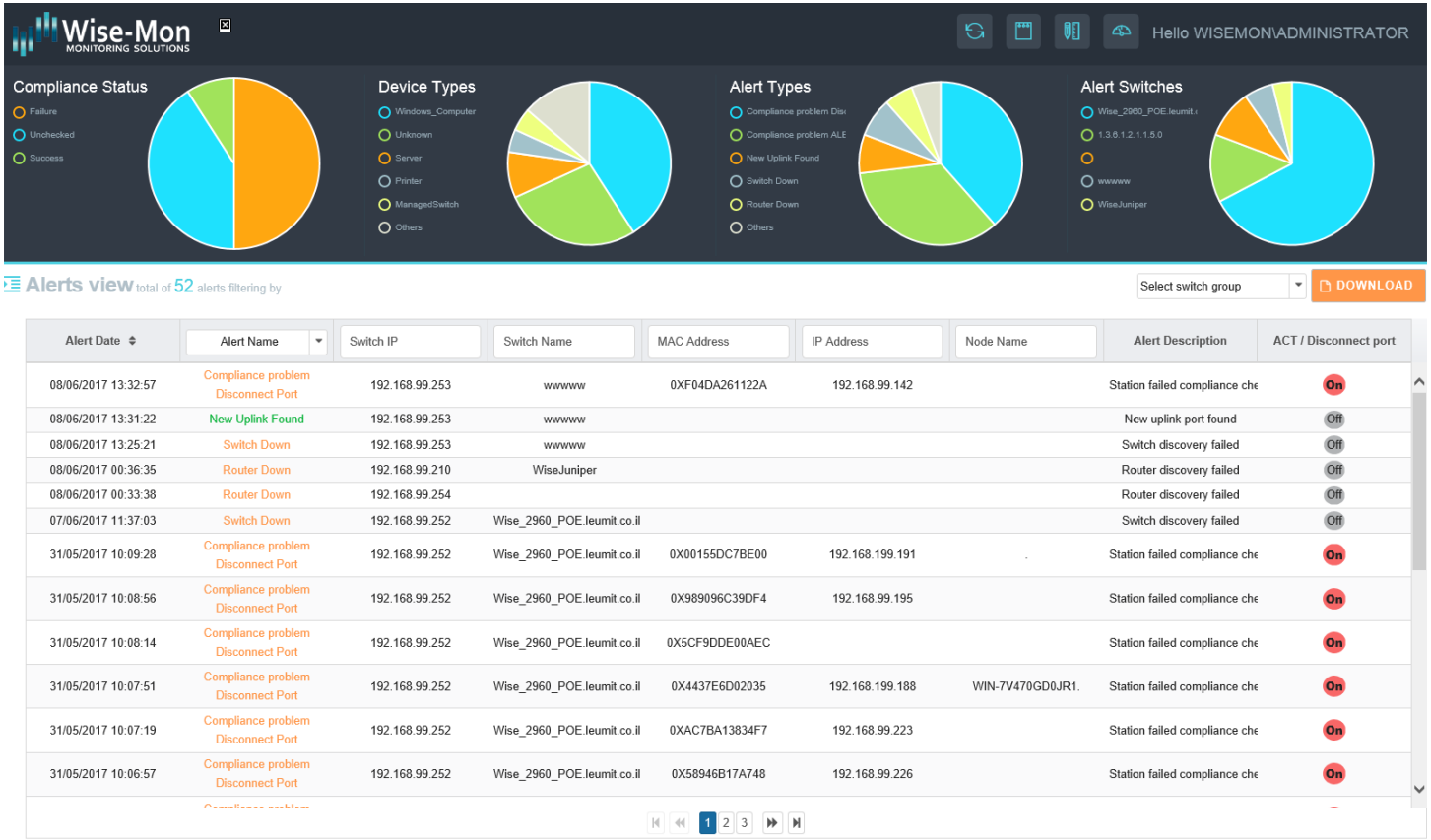
SWAT

- יכולת אכיפה ברמת המתג
  - ניתוק פיזי של התחנה
  - לא בצורה אפליקטיבית או ע"י מערכת ההפעלה
- תמיכה ביצרני ציוד שונים
- מערכת ללא התקנת סוכנים
- קונסול אירועים מרכזי
- קישור למערכות SIEM
- שימוש במגוון פרוטוקולים
  - SNMP
  - WMI
  - TCP

פונקציונאליות

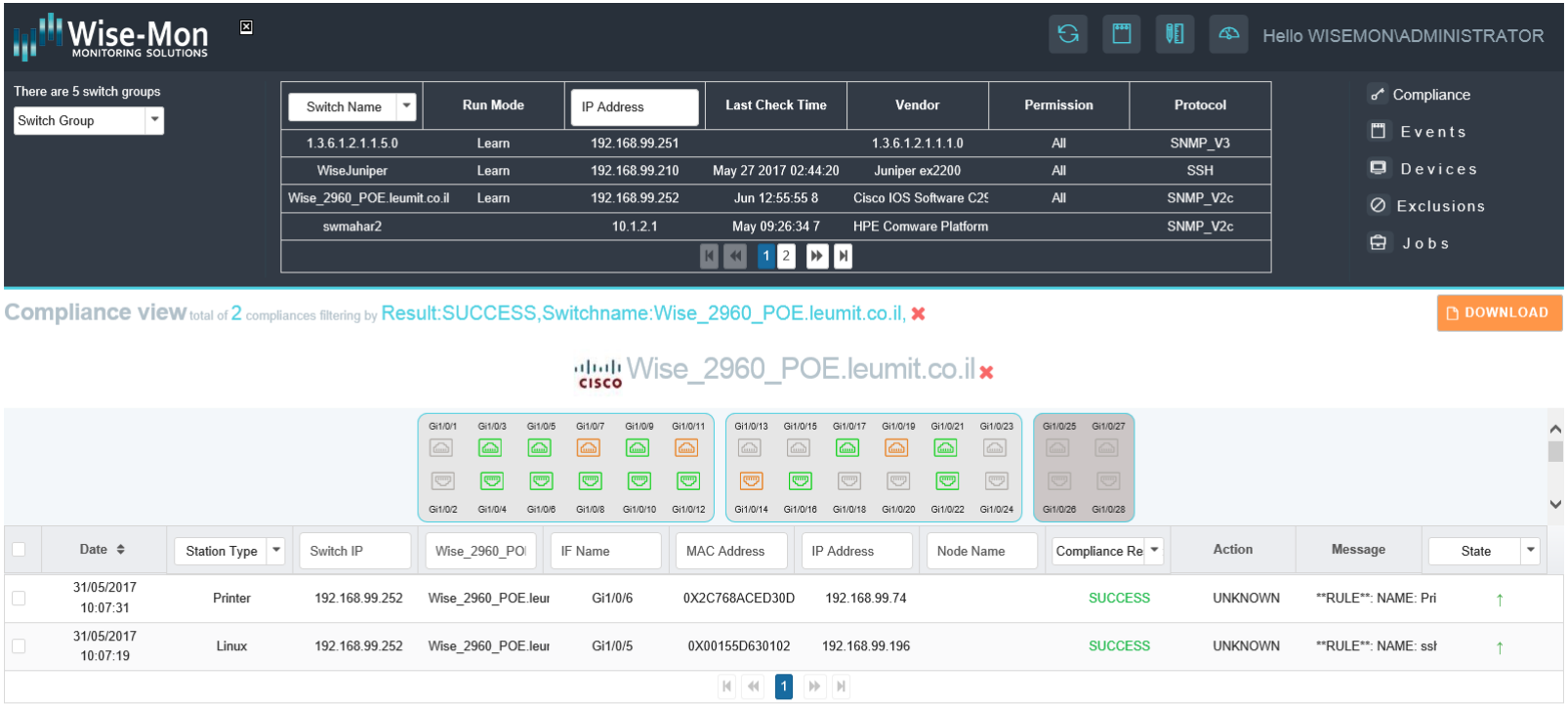
- **סיווג התקנים המחוברים לרשת על פי בדיקת Finger Print**
- **Agent less – לא מצריך התקנה בתחנות קצה**
- **ביזור – Probe מרוחק לניהול רכיבי רשת**
  - תמיכה בארגון מרובה סניפים
- **תמיכה ביצרני ציוד רשת שונים**
- **ניהול מדיניות ע"פ אזורים**
  - ניתן לאגד קבוצת מתגים תחת אותה מדיניות
  - אכיפת מדיניות כפי שהוגדרה ע"י מנהל הרשת

קונסול התראות - SWAT



Alert Date	Alert Name	Switch IP	Switch Name	MAC Address	IP Address	Node Name	Alert Description	ACT / Disconnect port
08/06/2017 13:32:57	Compliance problem Disconnect Port	192.168.99.253	wwwww	0XF04DA261122A	192.168.99.142		Station failed compliance che	On
08/06/2017 13:31:22	New Uplink Found	192.168.99.253	wwwww				New uplink port found	Off
08/06/2017 13:25:21	Switch Down	192.168.99.253	wwwww				Switch discovery failed	Off
08/06/2017 00:36:35	Router Down	192.168.99.210	WiseJuniper				Router discovery failed	Off
08/06/2017 00:33:38	Router Down	192.168.99.254					Router discovery failed	Off
07/06/2017 11:37:03	Switch Down	192.168.99.252	Wise_2960_POE.leumit.co.il				Switch discovery failed	Off
31/05/2017 10:09:28	Compliance problem Disconnect Port	192.168.99.252	Wise_2960_POE.leumit.co.il	0X00155DC7BE00	192.168.199.191		Station failed compliance che	On
31/05/2017 10:08:56	Compliance problem Disconnect Port	192.168.99.252	Wise_2960_POE.leumit.co.il	0X989096C39DF4	192.168.99.195		Station failed compliance che	On
31/05/2017 10:08:14	Compliance problem Disconnect Port	192.168.99.252	Wise_2960_POE.leumit.co.il	0X5CF9DDE00AEC			Station failed compliance che	On
31/05/2017 10:07:51	Compliance problem Disconnect Port	192.168.99.252	Wise_2960_POE.leumit.co.il	0X4437E6D02035	192.168.199.188	WIN-7V470GD0JR1.	Station failed compliance che	On
31/05/2017 10:07:19	Compliance problem Disconnect Port	192.168.99.252	Wise_2960_POE.leumit.co.il	0XAC7BA13834F7	192.168.99.223		Station failed compliance che	On
31/05/2017 10:06:57	Compliance problem Disconnect Port	192.168.99.252	Wise_2960_POE.leumit.co.il	0X58946B17A748	192.168.99.226		Station failed compliance che	On

SWAT


Wise-Mon
MONITORING SOLUTIONS
Hello WISEMON\ADMINISTRATOR
There are 5 switch groups
Switch Group
Switch Name
Run Mode
IP Address
Last Check Time
Vendor
Permission
Protocol
1.3.6.1.2.1.1.5.0 Learn 192.168.99.251 1.3.6.1.2.1.1.1.0 All SNMP_V3
WiseJuniper Learn 192.168.99.210 May 27 2017 02:44:20 Juniper ex2200 All SSH
Wise_2960_POE.leumit.co.il Learn 192.168.99.252 Jun 12:55:55 8 Cisco IOS Software C2 All SNMP_V2c
swmahar2 10.1.2.1 May 09:26:34 7 HPE Comware Platform SNMP_V2c
Compliance
Events
Devices
Exclusions
Jobs
Compliance view total of 2 compliances filtering by Result:SUCCESS,Switchname:Wise_2960_POE.leumit.co.il,
DOWNLOAD
Wise_2960_POE.leumit.co.il
Date
Station Type
Switch IP
Wise_2960_PO
IF Name
MAC Address
IP Address
Node Name
Compliance Re
Action
Message
State
31/05/2017 10:07:31 Printer 192.168.99.252 Wise_2960_POE.leu Gi1/0/6 0X2C768ACED30D 192.168.99.74 SUCCESS UNKNOWN **RULE**: NAME: Pri
31/05/2017 10:07:19 Linux 192.168.99.252 Wise_2960_POE.leu Gi1/0/5 0X00155D630102 192.168.99.196 SUCCESS UNKNOWN **RULE**: NAME: ssl

ניהול והתראות

- **קישור למערכות צד שלישי**
  - שליחת מייל
  - שליחת SMS
  - העברת התראות ל SOC על בסיס SNMP או SYSLOG
- **קישור לשרת אנטי וירוס ארגוני**
- **קישור לשעוני נוכחות**

אכיפה

- **בדיקה ראשונית מהירה (עד 20 שניות) לאיתור כתובת MAC חדשה**
- **תגובות בעקבות אירוע:**
  - ניתוק התחנה -הגדרת הפורט במתג (למשך מספר דקות)
  - בידוד התחנה ע"י הזזת הפורט ל VLAN מיוחד
  - התראה
  - הרצת סקריפט

לקוחות נבחרים SWAT