SIA
SECURITY INDUSTRY ASSOCIATION

SIAWEBINARS
Info for the Security Industry

Best Practices for Monitoring Cyber Threats to Security Solutions

Feb. 4, 2020

Best Practices for Monitoring Cyber Threats to Security Solutions

SIA SECURITY INDUSTRY ASSOCIATION

AXIS COMMUNICATIONS

razberi technologies

Introducing your speakers

Stephen Schwartz,
Vice President of
Development,
Razberi Technologies

Stephen Schwartz currently leads the software design and product development efforts for all Razberi products and has over 30 years experience in high-growth software and hardware companies.

His previous roles include CTO of RFID Global Solution where he led the design and development of products like Visi-Trac asset visibility and Genesta's SyVox voice recognition logistics solution for companies like PepsiCo, Sara Lee / Bimbo, and QuikTrip. Schwartz has also served several roles within Intermec as the Director of Product Management, Systems Engineering Manager, and Senior Systems Architect for their RFID hardware and software business unit fielding solutions to hundreds of Fortune 100 companies globally. In his spare time, he is a contributor and voting member of ETSI EN 302-208, and ANSI X3T6.

Schwartz has a bachelor's degree in Electrical Engineering from the University of Kentucky with graduate studies in engineering from George Mason University and business from Columbia University.

Ryan Zatolokin,
Business Development
Manager/ Senior Technologist,
North America Axis
Communications

Ryan Zatolokin is the business development manager, senior technologist for the business development team of Axis Communications. His primary focus is cybersecurity as well as positioning and promoting Axis technology in conjunction with the hardware and software technologies of eco-system partners.

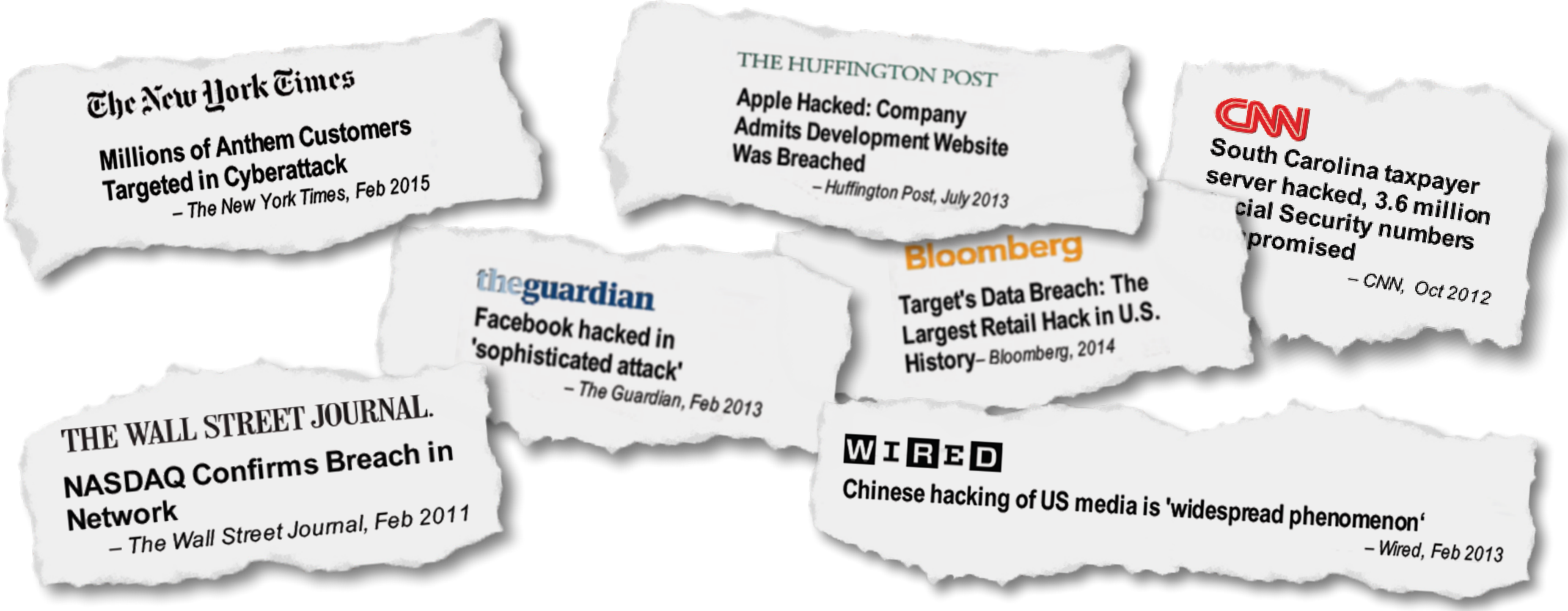
Ryan joined Axis in 2011, as a field sales engineer, bringing more than a decade of experience in network engineering on the systems integrator side of the industry.

Ryan earned his bachelor's degree in Business Administration with a specialty in computer information systems from Eastern Michigan University.

Today's objectives

- Threat landscape
- Understanding the differences between risk, vulnerabilities, threats, and incidents
- Physical security's cyber problem
- Recognizing threats and vulnerabilities
- The targeting of physical security
- Why monitoring is required

High profile breaches make headlines



The New York Times

Millions of Anthem Customers Targeted in Cyberattack
– The New York Times, Feb 2015

THE HUFFINGTON POST

Apple Hacked: Company Admits Development Website Was Breached
– Huffington Post, July 2013

CNN

South Carolina taxpayer server hacked, 3.6 million cial Security numbers promised
– CNN, Oct 2012

theguardian

Facebook hacked in 'sophisticated attack'
– The Guardian, Feb 2013

Bloomberg

Target's Data Breach: The Largest Retail Hack in U.S. History– Bloomberg, 2014

THE WALL STREET JOURNAL.

NASDAQ Confirms Breach in Network
– The Wall Street Journal, Feb 2011

WIRED

Chinese hacking of US media is 'widespread phenomenon'
– Wired, Feb 2013

Threat landscape

Not Petya 2017 – $10 Billion in Damages Worldwide

- > Maersk – $300 Million
- > Merck – $870 Million
- > FedEx – $400 Million
- > Combination of Windows vulnerability combined with ransomware
- > Collateral damage to nation-state target Ukraine from Russian hackers

Mirai/Persiria – Botnet

Devils Ivy – Stack overflow – SOAP

Cybersecurity legislation

California State Bill 327

Starting on January 1st, 2020, any manufacturer of a device that connects “directly or indirectly” to the internet must equip it with “reasonable” security features designed to prevent unauthorized access, modification, or information disclosure. If it can be accessed outside a local area network (LAN) with a password, it needs to either come with a unique password for each device or force users to set their own password the first time they connect. That means no more generic default credentials for a hacker to guess.

NDAA 2018

> Bans on specific manufacturers

> Improve security by default from manufacturer on products

IoT Cybersecurity Improvement Act 2017

> Improve security by default from manufacturer on products

> Contractor to provide “proof” of product without vulnerabilities

Definitions

Risk is the probability that an outside element will exploit a system weakness.

Vulnerability is a system weakness that creates a risk.

A **threat** is anything that could exploit a vulnerability to be destructive or harmful to assets.

An **incident** (or event) occurs when a threat penetrates the security of a network without authorization.

Physical security’s cyber problem

Proliferation of IoT devices used within physical security

Inter -company disconnects between Operations and IT

Lack of IT oversight into physical security networks

Small pool of available cybersecurity professionals

Sophisticated solutions are complex to implement

Slow adoption of best practices by manufacturers and installers

Large and growing vulnerable install base

Hackers leverage adjacent less secure networks to gain corporate access

https://news.milestonesys.com/automating-trust-for-cyber-threatened-surveillance-systems

Poll: Question 1

Given the current threat landscape and economic environment, do you perceive a change in the cyber threats facing your organization?

- ➢ Increase
- ➢ Same
- ➢ Decrease
- ➢ Don't know

Recognizing threats and vulnerabilities

Physical security architecture has evolved to be more IT -centric

Most data breaches are never reported, even less so when not mandated by law

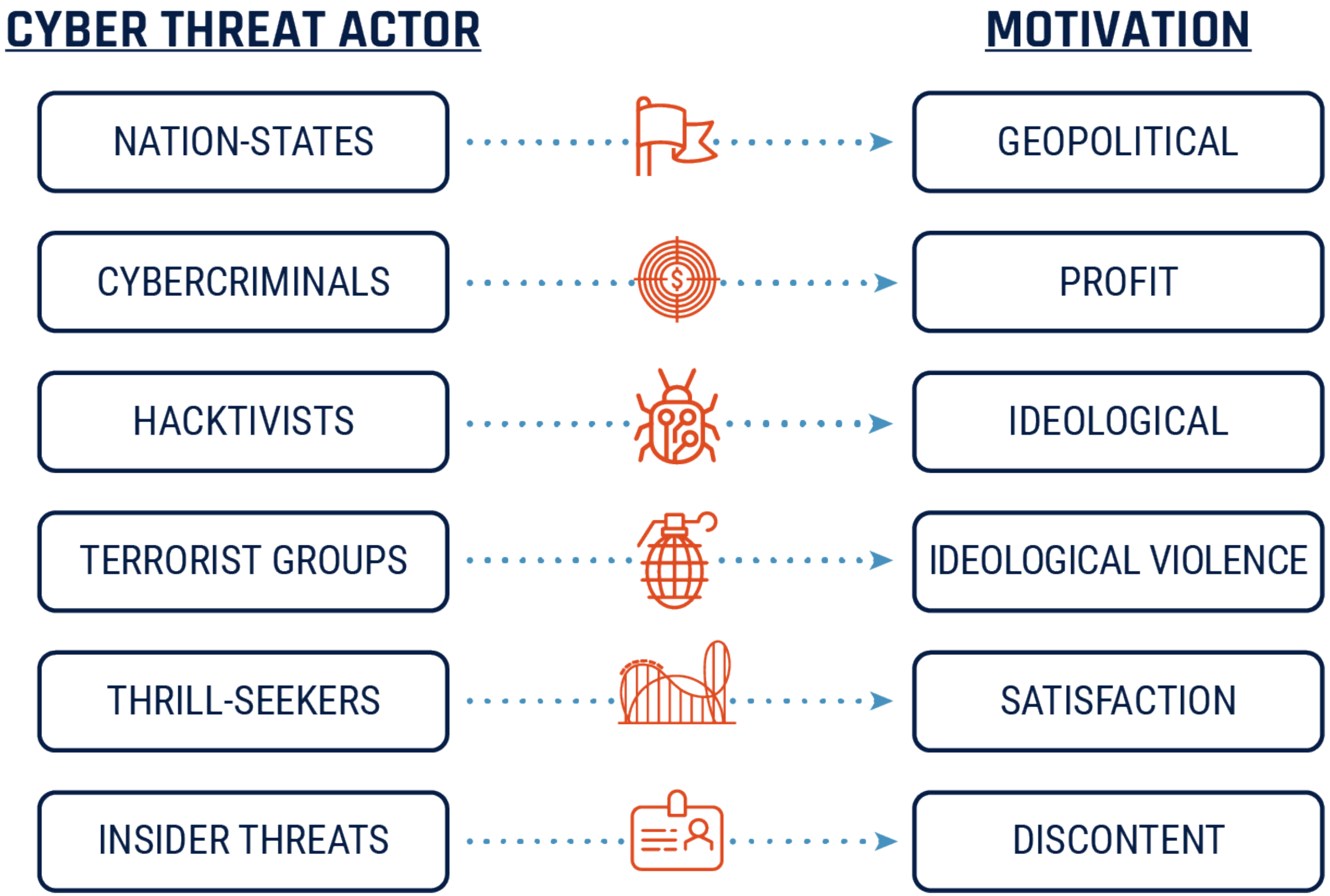
180 million professional video surveillance cameras will be shipped in 2019

Online tools / search engines (e.g. Insecam.org, Shodan) regularly showcase vulnerabilities

Prevailing culture and lack of understanding breed opportunistic hackers who gain entry through adjacent networks

IT-based system adoption exponentially creates further vulnerabilities

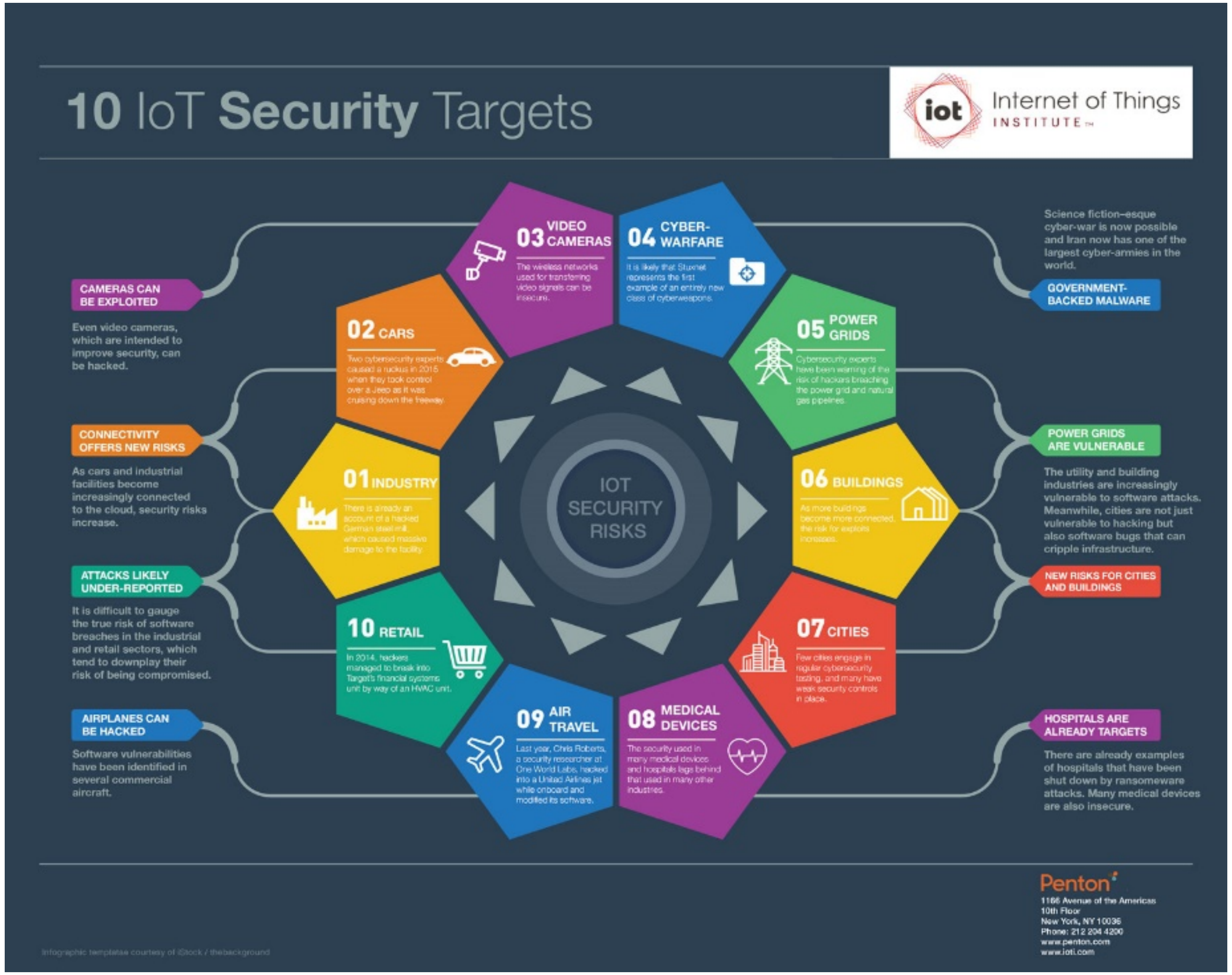
Threat actors



CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

https://vividcomm.com/2019/04/15/threat-actors/

Top IoT security targets



01 INDUSTRY

There is already an account of a hacked German steel mill, which caused massive damage to the facility.

02 CARS

Two cybersecurity experts caused a ruckus in 2015 when they took control over a Jeep as it was cruising down the freeway.

03 VIDEO CAMERAS

The wireless networks used for transferring video signals can be insecure.

04 CYBER-WARFARE

It is likely that Stuxnet represents the first example of an entirely new class of cyberweapons.

05 POWER GRIDS

Cybersecurity experts have been warning of the risk of hackers breaching the power grid and natural gas pipelines.

06 BUILDINGS

As more buildings become more connected, the risk for exploits increases.

07 CITIES

Few cities engage in regular cybersecurity testing, and many have weak security controls in place.

08 MEDICAL DEVICES

The security used in many medical devices and hospitals lags behind that used in many other industries.

09 AIR TRAVEL

Last year, Chris Roberts, a security researcher at One World Labs, hacked into a United Airlines jet while onboard and modified its software.

10 RETAIL

In 2014, hackers managed to break into Target's financial systems unit by way of an HVAC unit.

CAMERAS CAN BE EXPLOITED

Even video cameras, which are intended to improve security, can be hacked.

CONNECTIVITY OFFERS NEW RISKS

As cars and industrial facilities become increasingly connected to the cloud, security risks increase.

ATTACKS LIKELY UNDER-REPORTED

It is difficult to gauge the true risk of software breaches in the industrial and retail sectors, which tend to downplay their risk of being compromised.

AIRPLANES CAN BE HACKED

Software vulnerabilities have been identified in several commercial aircraft.

Science fiction–esque cyber-war is now possible and Iran now has one of the largest cyber-armies in the world.

GOVERNMENT-BACKED MALWARE

POWER GRIDS ARE VULNERABLE

The utility and building industries are increasingly vulnerable to software attacks. Meanwhile, cities are not just vulnerable to hacking but also software bugs that can cripple infrastructure.

NEW RISKS FOR CITIES AND BUILDINGS

HOSPITALS ARE ALREADY TARGETS

There are already examples of hospitals that have been shut down by ransomeware attacks. Many medical devices are also insecure.

Infographic templates courtesy of iStock / thebackground

Penton
1166 Avenue of the Americas
10th Floor
New York, NY 10036
Phone: 212 204 4200
www.penton.com
www.ioti.com

https://www.iotworldtoday.com/2016/07/27/10-most-vulnerable-iot-security-targets/

#SimpleSecureVideo

Simplify

Intelligent Video Surveillance Server Appliances

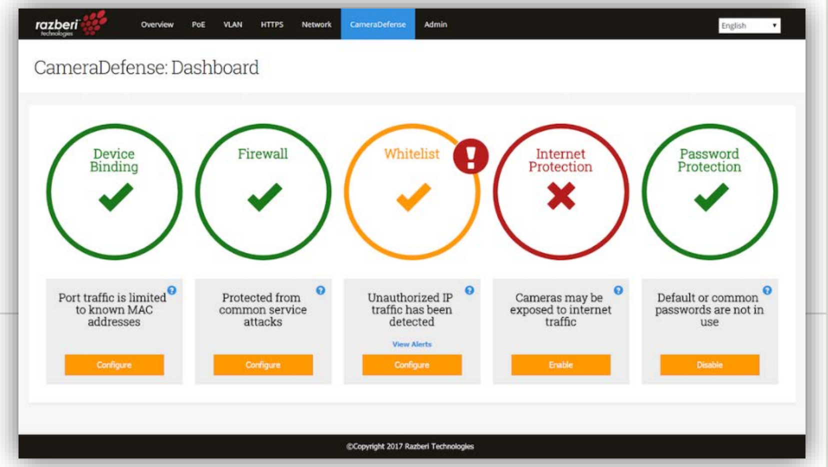
+

Automated Cybersecurity Software

+

Health Monitoring Software

Automate



CameraDefense: Dashboard

Port traffic is limited to known MAC addresses

Protected from common service attacks

Unauthorized IP traffic has been detected

Cameras may be exposed to internet traffic

Default or common passwords are not in use

©Copyright 2017 Razberi Technologies

MVP @ ISC WEST
SECURITY SALES & INTEGRATION
2019

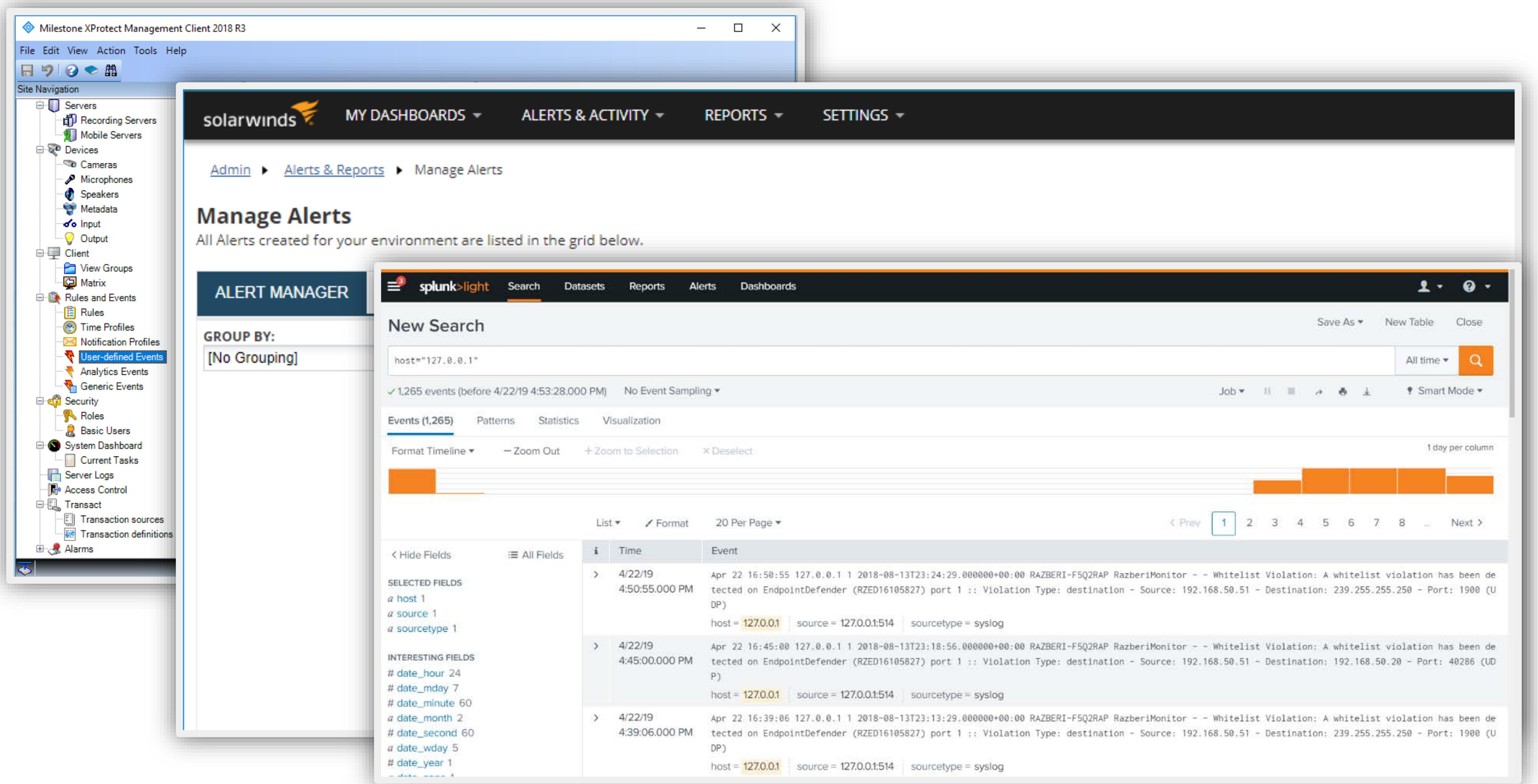
SIA NEW PRODUCT SHOWCASE
WINNER
Cybersecurity
Razberi Technologies:
Razberi EndpointDefender
2019 ISC WEST

Razberi CameraDefense™

Award -Winning, Automated IoT Cybersecurity Software

Blocks	unauthorized devices
Closes	unused network ports
Restricts	device traffic to known networks
Enforces	password complexity
Denies	un-needed network services
Monitors	alerts for threat detection displayed on simple dashboard

Integrate



Manage Alerts

All Alerts created for your environment are listed in the grid below.

GROUP BY: [No Grouping]

New Search

```
host="127.0.0.1"
```

✓ 1,265 events (before 4/22/19 4:53:28.000 PM) No Event Sampling

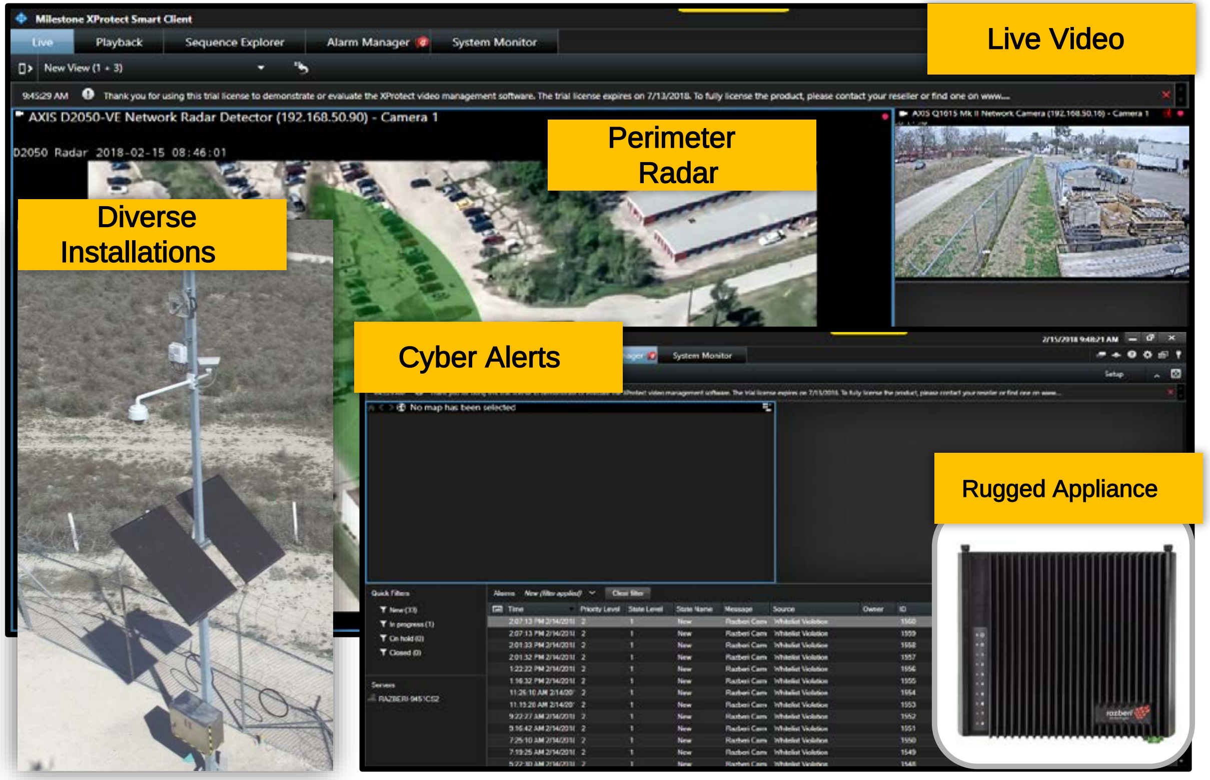
SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # date_hour 24
- # date_mday 7
- # date_minute 60
- a date_month 2
- # date_second 60
- a date_wday 5
- # date_year 1

i	Time	Event
>	4/22/19 4:50:55.000 PM	Apr 22 16:50:55 127.0.0.1 1 2018-08-13T23:24:29.000000+00:00 RAZBERI-F5Q2RAP RazberiMonitor - - Whitelist Violation: A whitelist violation has been detected on EndpointDefender (RZED16105827) port 1 :: Violation Type: destination - Source: 192.168.50.51 - Destination: 239.255.255.250 - Port: 1900 (UDP) host = 127.0.0.1 source = 127.0.0.1:514 sourcetype = syslog
>	4/22/19 4:45:00.000 PM	Apr 22 16:45:00 127.0.0.1 1 2018-08-13T23:18:56.000000+00:00 RAZBERI-F5Q2RAP RazberiMonitor - - Whitelist Violation: A whitelist violation has been detected on EndpointDefender (RZED16105827) port 1 :: Violation Type: destination - Source: 192.168.50.51 - Destination: 192.168.50.20 - Port: 40286 (UDP) host = 127.0.0.1 source = 127.0.0.1:514 sourcetype = syslog
>	4/22/19 4:39:06.000 PM	Apr 22 16:39:06 127.0.0.1 1 2018-08-13T23:13:29.000000+00:00 RAZBERI-F5Q2RAP RazberiMonitor - - Whitelist Violation: A whitelist violation has been detected on EndpointDefender (RZED16105827) port 1 :: Violation Type: destination - Source: 192.168.50.51 - Destination: 239.255.255.250 - Port: 1900 (UDP) host = 127.0.0.1 source = 127.0.0.1:514 sourcetype = syslog

SIA SECURITY INDUSTRY ASSOCIATION AXIS COMMUNICATIONS razberi technologies

Collaborate



9:45:29 AM Thank you for using this trial license to demonstrate or evaluate the XProtect video management software. The trial license expires on 7/13/2018. To fully license the product, please contact your reseller or find one on www....

AXIS D2050-VE Network Radar Detector (192.168.50.90) - Camera 1

D2050 Radar 2018-02-15 08:46:01

AXIS Q1615 Mk II Network Camera (192.168.50.16) - Camera 1

2/15/2018 9:48:21 AM

Time	Priority Level	State Level	State Name	Message	Source	Owner	ID
2:07:13 PM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1560
2:07:13 PM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1559
2:01:33 PM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1558
2:01:32 PM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1557
1:22:22 PM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1556
1:16:32 PM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1555
11:26:10 AM 2/14/20'	2	1	New	Razberi Cam	Whitelist Violation		1554
11:13:28 AM 2/14/20'	2	1	New	Razberi Cam	Whitelist Violation		1553
9:22:27 AM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1552
9:16:42 AM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1551
7:25:10 AM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1550
7:19:25 AM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1549
5:22:30 AM 2/14/201	2	1	New	Razberi Cam	Whitelist Violation		1548

Outdoor Camera

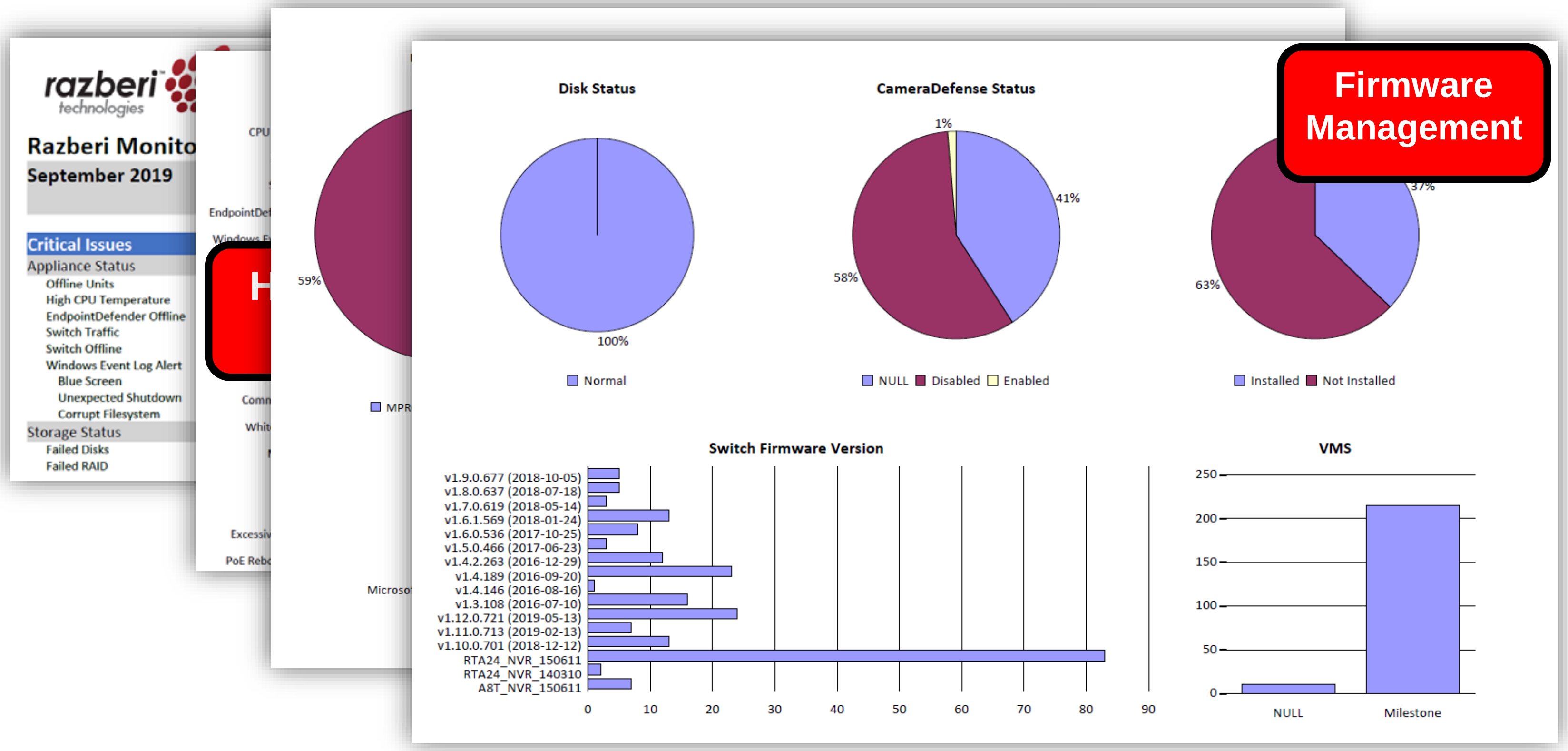
Perimeter Radar

SIA SECURITY INDUSTRY ASSOCIATION

AXIS COMMUNICATIONS

razberi technologies

Report



Razberi Monito
September 2019

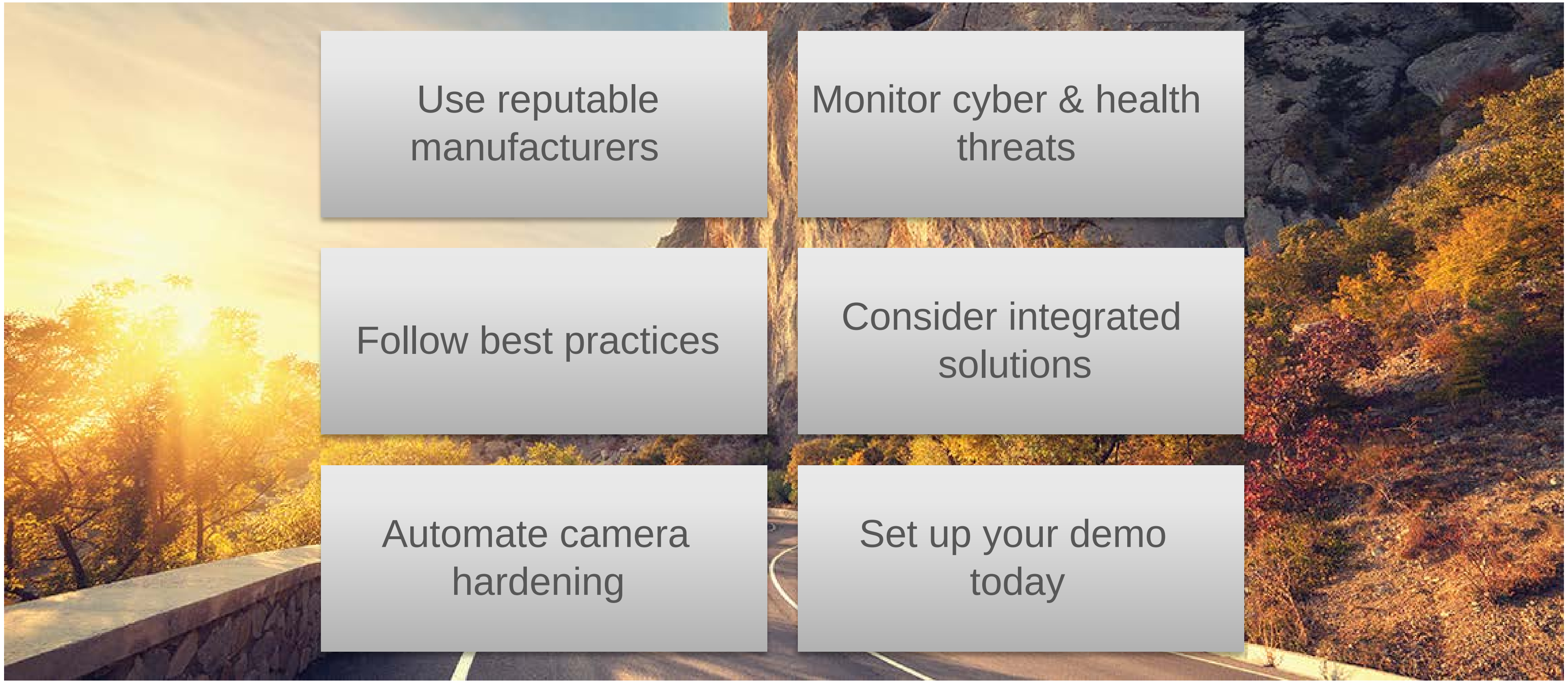
Critical Issues
Appliance Status
- Offline Units
- High CPU Temperature
- EndpointDefender Offline
- Switch Traffic
- Switch Offline
- Windows Event Log Alert
  - Blue Screen
  - Unexpected Shutdown
  - Corrupt Filesystem

Storage Status
- Failed Disks
- Failed RAID

Firmware Management

Cybersecurity is a **process**, not a feature.

Summary



Use reputable manufacturers

Monitor cyber & health threats

Follow best practices

Consider integrated solutions

Automate camera hardening

Set up your demo today

Poll: Question 2

Are you interested in having a conversation with Axis Communications and Razberi Technologies?

> Yes, please contact me

> No, not at this time

Thank You

#SimpleSecureVideo

SIA SECURITY INDUSTRY ASSOCIATION

AXIS COMMUNICATIONS

razberi™ technologies