

LIVE WEBINAR !

July 8, 2020 10 AM (USA CDT)

Efficient Industrial Cyber Security Programs

How to Get Quick Results without Draining Your Resources

[Technical Webinar]



Ofer Shaked

Co-Founder and CTO
SCADAfence



Clint Schneider

Account Executive
IIoT and Automation at Logic, Inc.



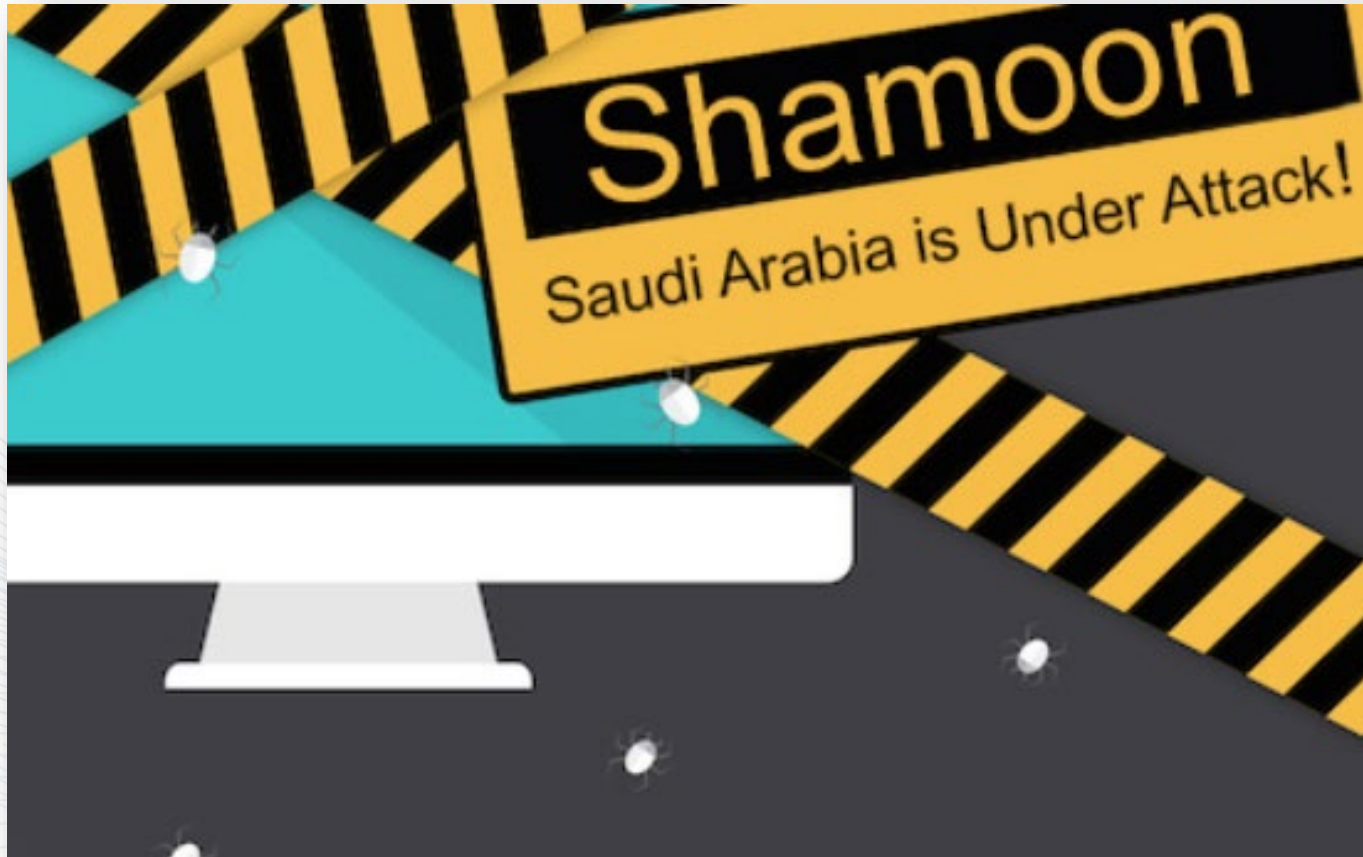
Moderated By:

Michael Yehoshua
VP of Marketing
SCADAfence

Agenda

- Saudi Aramco Under Attack! [Clint Schneider, Account Executive Logic, Inc.](#)
- Understand the Adversaries' Perspective - [Ofer Shaked, Co-Founder and CTO, SCADAfence](#)
- Checklist and KPIs for Industrial Cyber Security - [Ofer Shaked](#)
- Commonly Used Tools - [Ofer Shaked](#)
- Live Demo - [Ofer Shaked](#)
- Efficient Industrial Cyber Security Program Review - [Ofer Shaked](#)
- Q&A - [Michael Yehoshua, VP of Marketing, SCADAfence](#)

Saudi Aramco Under Attack



Presented By :
Clint Schneider
Account Executive –IIoT and Automation at Logic, Inc.

Ofer Shaked – Speaker Profile

- Co-Founder & CTO of SCADAfence
- 13 years background in SCADA / Industrial Security
- Ex-officer in the Israeli Intelligence Elite Cyber Unit
- Architect in the OTCSA
- Advisory Board member at ManuSec
- Speaker at ICS Security Conferences



Recap from Previous Webinar

A well-prepared network is...

Very difficult to attack

Slows down the attackers,
allows the defenders to
respond

If attacked, it results in
minimal damage and
quick recovery

The Adversaries' Perspective (Simplified)

Find a way in

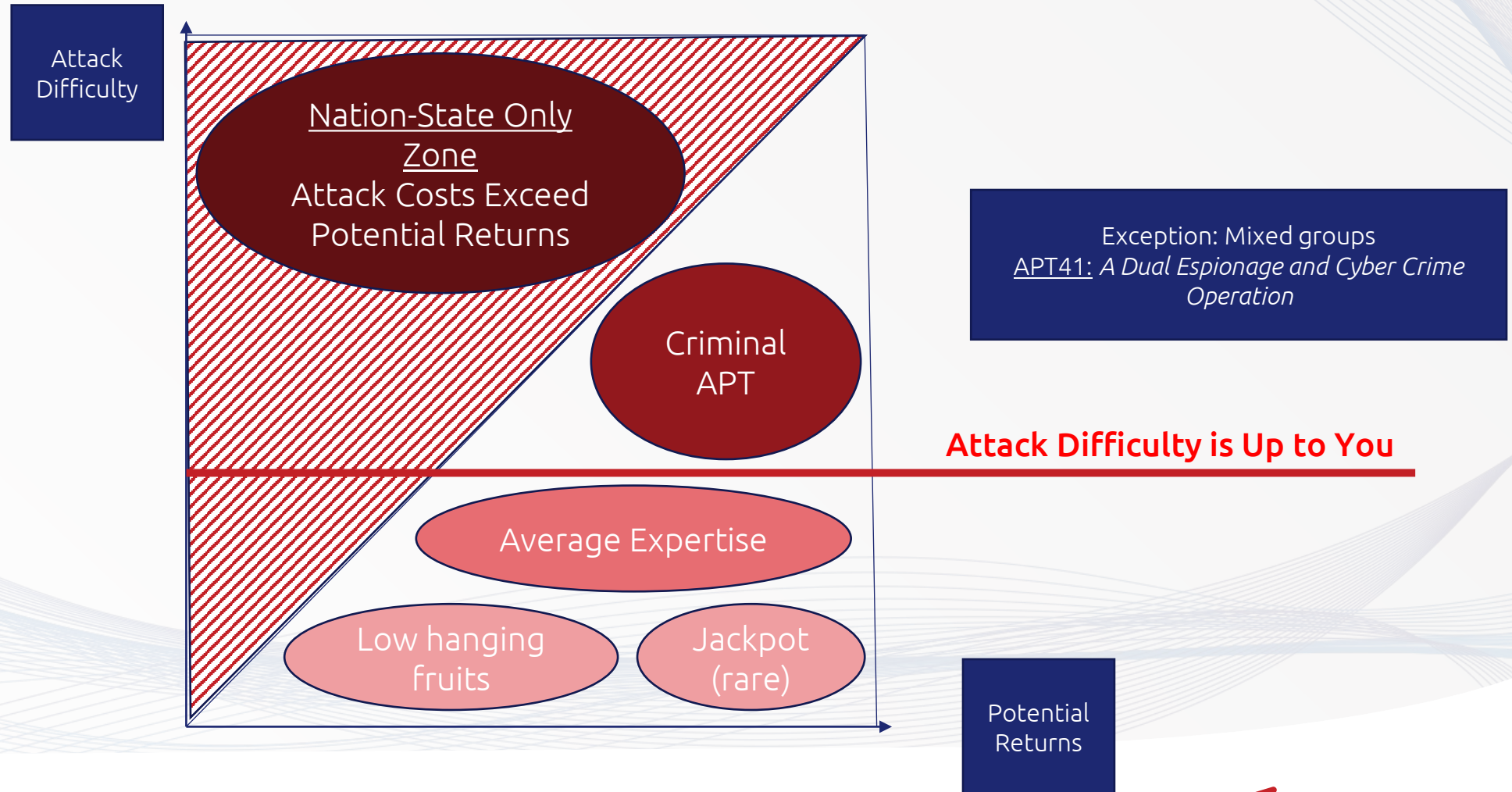


Propagate until
you reach the
target assets



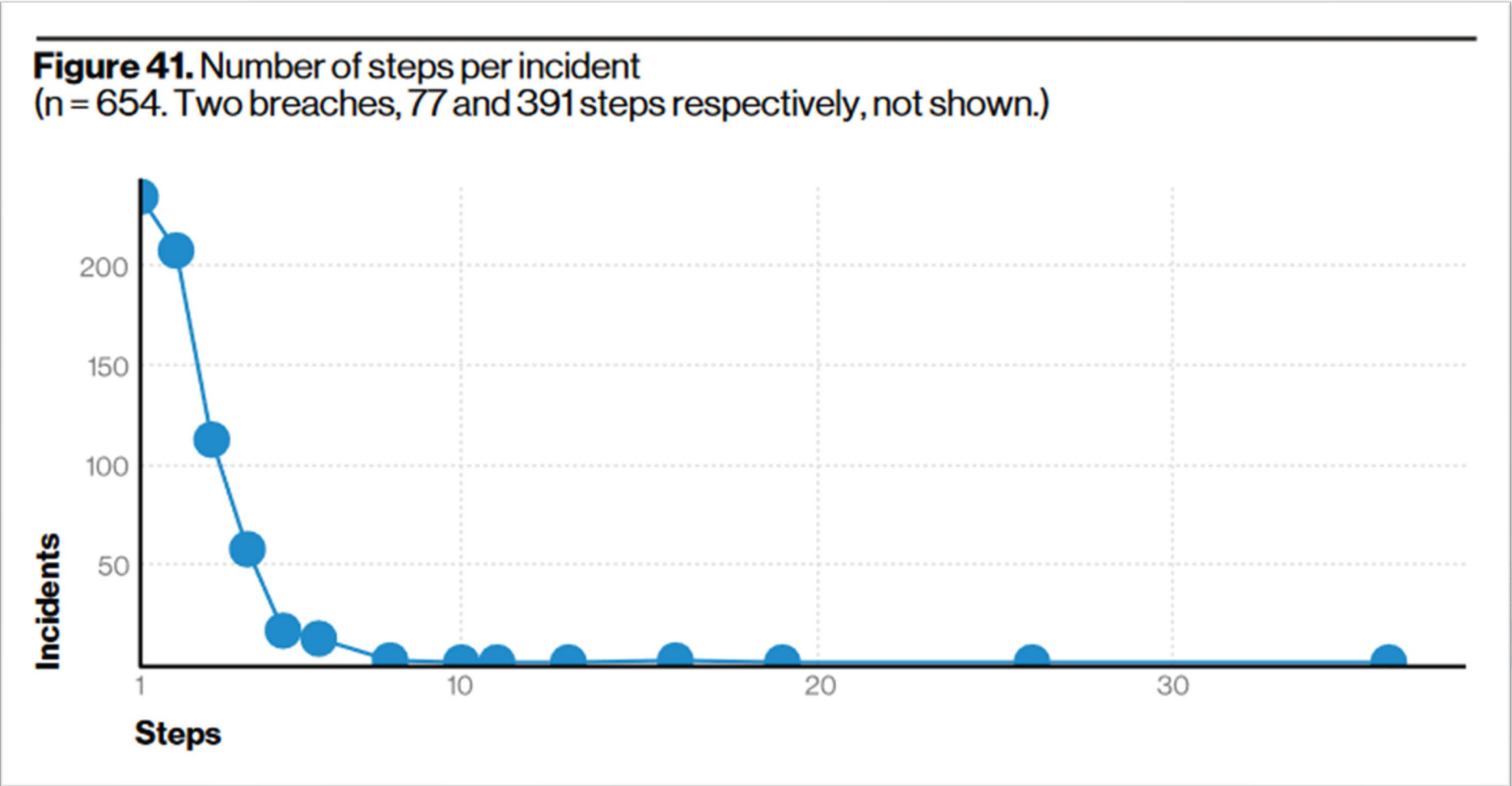
Perform the
malicious action

How Criminals vs. Nation-State Select their Targets




Tested in the Real World

Credit: Verizon 2020 Data Breach Investigations Report




Conclusion

Cyber attackers behavior can be explained by the simple “Expected Return” formula



Expected Return Formula

$$= \sum R_i \times P_i$$


Change the formula and control your defensive future

$\left[\begin{array}{l} R_i = \text{Return Expectation} \\ P_i = \text{Return Probability} \\ \text{Credit: EduCBA} \end{array} \right]$

Checklist and KPIs for an Industrial Cyber Security Program

Should we copy KPIs from IT Security?

KPIs	Result
Level of Preparedness - % Devices Fully Patched	
# of Unidentified Devices	
# of Intrusion Attempts	
# of Security Incidents	
MTTD - Mean Time to Detect	
MTTR - Mean Time to Resolve	
MTTC - Mean Time to Contain	

Checklist and KPIs for an Industrial Cyber Security Program

IT Security metrics are good for measurement of mature programs



Early on, these metrics can't be measured



Which metrics are important early on?

Checklist and KPIs for Starting an Industrial Cyber Security Program

Category	KPIs
Basics	Do you have a person who is responsible for cyber security, with adequate experience and training, that reports to a C-level executive?
	Do you have an automated, updated asset inventory?
	Do you have automated, updated network diagrams?
	Do you have automated mapping of all interfaces between your network and the external (untrusted) world?

Checklist and KPIs for Starting an Industrial Cyber Security Program

Category	KPIs
Vulnerability Management	Do you have a method to automatically detect vulnerabilities?
	Do you have a method to prioritize vulnerabilities?
	Do you have a process to mitigate vulnerabilities and install patches?
	Do you currently have vulnerabilities in externally facing services?
	Do you do a periodical security assessment using an external consultant?

Checklist and KPIs for Starting an Industrial Cyber Security Program

Category	KPIs
Threat Detection and Prevention	Do you have tools to detect and prevent attacks on networks and endpoints?
	Do you have playbooks and policies for handling common attack scenarios?
	Do you have a person who is responsible to handle security alerts in a timely fashion, with periodical performance reviews?

Checklist and KPIs for Starting an Industrial Cyber Security Program

Category	KPIs
Network Separation and Segmentation	Do you have a firewall between the IT and OT networks?
	Are your OT network devices isolated from the external world using a DMZ?
	Do you have internal OT network segmentation to prevent malware from spreading?
	Do you have monitoring to make sure that your segmentation remains intact over time?
	Do you have a secure, monitored remote access solution with 2 factor authentication?

Checklist and KPIs for Starting an Industrial Cyber Security Program

Category	KPIs
Governance, Regulations & Security Frameworks	Do you use a base framework? (corporate policy or common standards such as NIST-CSF, IEC-62443, etc.)
	Do you have centralized monitoring of your security status across all the sites under your jurisdiction?
	Do you have manual or automated methods to detect whenever a network or an asset isn't adhering to your cyber security policy?

Commonly Used Tools in Industrial Security Programs

Category	Tool 1	Tool 2	Tool 3
Basics	Asset Management	Network Management	Network Mapping
Vulnerability Management	Passive/Active Vulnerability Scanners	Risk-Based Vulnerability Prioritization	Patch Management
Threat Detection and Prevention	Endpoint Protection	Network Threat Detection	Network Anomaly Detection
Network Separation and Segmentation	Dedicated Firewalls	Switch/Router built-in capabilities (VLANs, ACLs)	VPN for Remote Access with 2FA (2-Factor Authentication)
Governance & Compliance	Questionnaire-based compliance platforms	Automation-based compliance platforms	-

A decorative graphic on the left side of the image consists of several overlapping, rounded rectangular brush strokes. The strokes are arranged diagonally from the top-left towards the bottom-right. The colors of the strokes transition from a bright red at the top, through shades of pink and purple, to a vibrant blue at the bottom. The background is a solid, dark navy blue.

Live Demo

Efficient Industrial Cyber Security Program Review

Step 1:

- Understand what needs to be protected



Step 2:

- Deploy threat detection tools, and respond to incidents



Step 3:

- Start a vulnerability management process



Step 4:

- Separate and segment your networks



Step 5:

- Deploy centralized governance and automated measurement tools

Checklist and KPIs for a Mature Industrial Cyber Security Program

Once your cyber security machine is up and running, you can start measuring and improving it!

KPIs	Result
Level of Preparedness - % Devices Fully Patched	
# of Unidentified Devices	
# of Intrusion Attempts	
# of Security Incidents	
MTTD - Mean Time to Detect	
MTTR - Mean Time to Resolve	
MTTC - Mean Time to Contain	
Etc...	



Q&A

Thank you.



OFER SHAKED
Co-Founder and CTO,
SCADAfence
Ofer@scadafence.com



CLINT SCHNEIDER
Account Executive –
IIoT and Automation at Logic, Inc.
clint@logic-control.com



Thank You!

SCADAfence is here to assist you
in your journey.