RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SAT-M03**

Hacking and Protecting Distributed Energy Infrastructure

Gib Sorebo

Security Associate Director
Accenture
@gibsorebo

Aaron Bayles

Senior Manager - OT Security
Accenture
@alxrogan

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

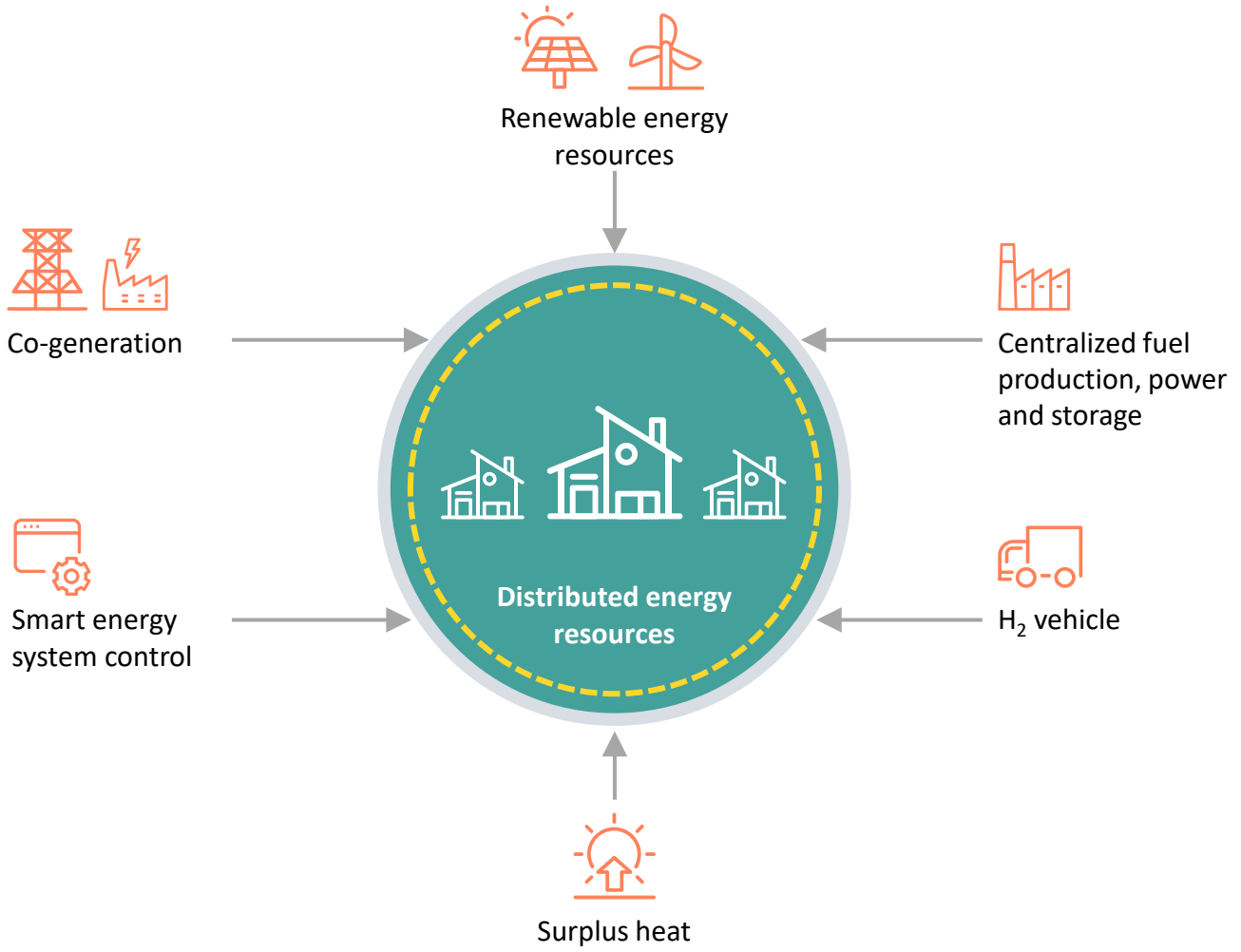
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

accenture

$200 billion Internet of Energy Market by 2024*

* BIS Research
Emerging Technology Market Intelligence

Small Scale Renewable Energy

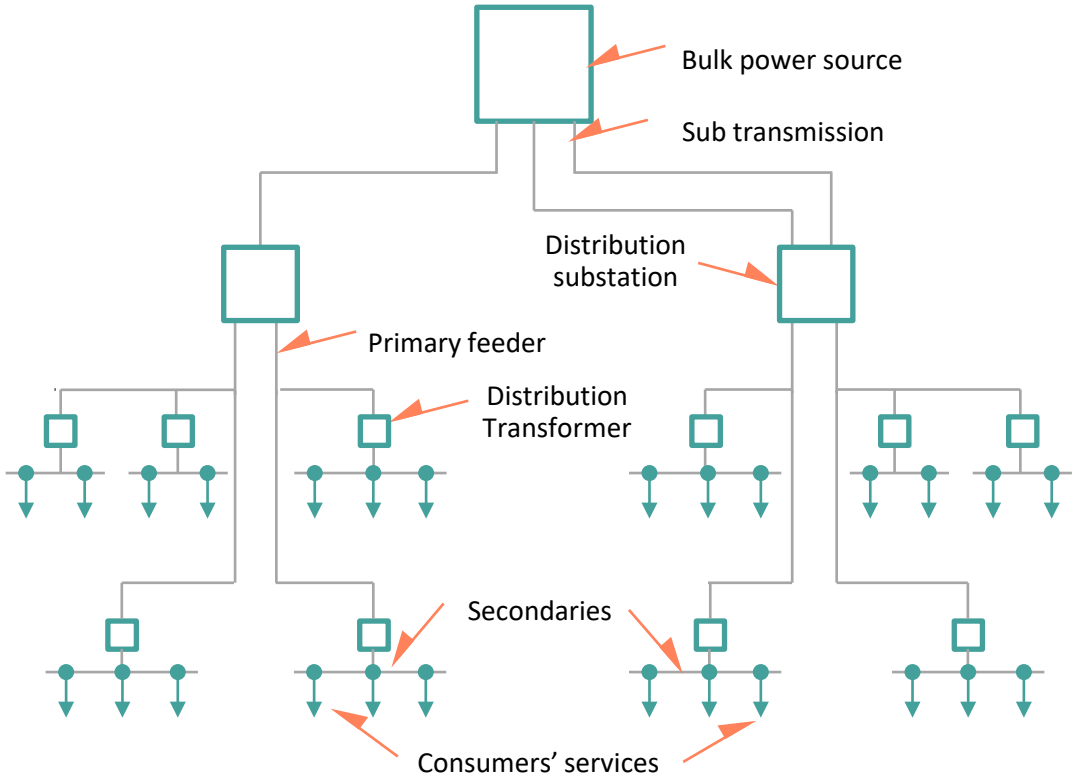


Security

FIRST-OF-A-KIND U.S. GRID CYBERATTACK HIT WIND, SOLAR

Blake Sobczak, E&E News reporter
Published: Thursday, October 31, 2019

A Whole New World…



Residential Customer-owned, internet-connected

Utility-owned, private network connected

Requires A Different Architecture

Distributed energy resources

Internet

OR

Dedicated utility network

Renewables aggregator / inverter manufacturer

Utility

Key Utility stakeholders/buyers:

- Distribution Engineering/Operations
- CISO/SOC Director
- Field Support teams

DERMS/ADMS application

Possible Monitoring tools

Typically, not part of OT/IoT architecture today

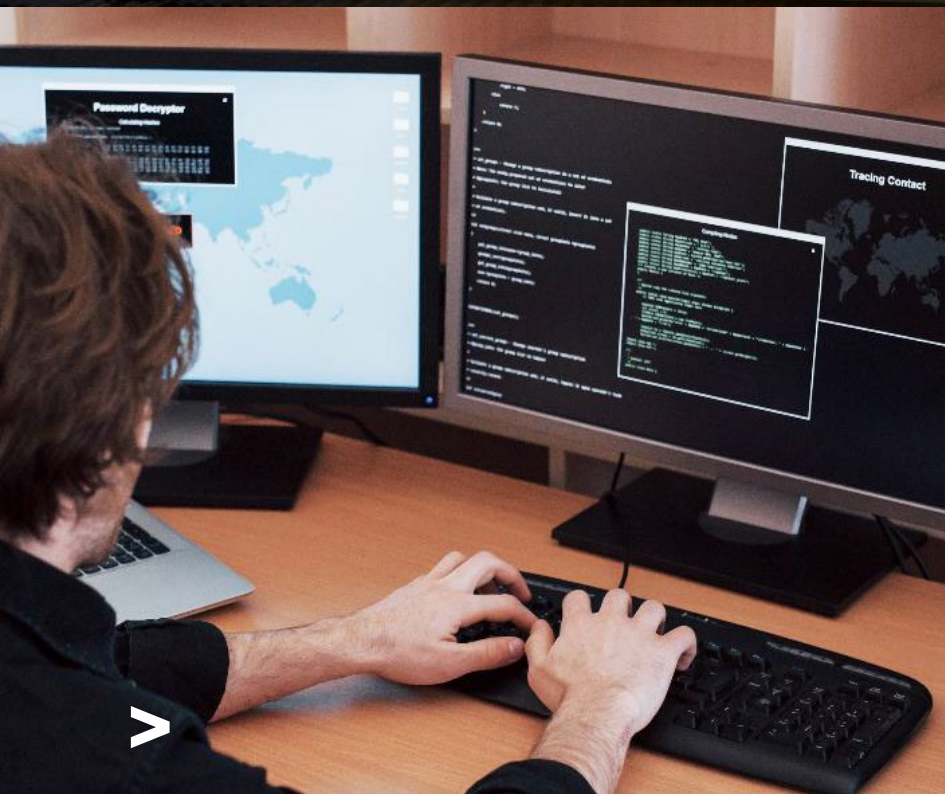
Security Operations Center (SOC)

Distribution control Center

DERMS – Distributed Energy Resource Management System
ADMS – Advanced Distribution Management System
OT – Operations Technology
IoT – Internet of Things

What Needs to be Secured

Securing systems/platforms (e.g., DERMS, ADMS) much like we would any other system	Typical utility practice
Securing connections from generation resources, both utility and third-party owned, to centralized systems/platforms	Typical utility practice
Validating the integrity of the data coming from third-party owned generation sources, aggregators, and inverter vendors	Not a typical utility practice
Detecting anomalous and potentially malicious activities occurring on third-party generation sources and anticipating potential downstream effects	Not a typical utility practice



Do the words SolarWinds ring a bell?

> …**800,000 [of vendor's] microinverters** in Hawaii, each networked to the company's cloud-based monitoring and control systems….[The vendor] is unveiling the latest use of this installed capability: **reprogramming its Hawaiian microinverter fleet en masse**, to help [the utility] ride through solar-influenced disruptions on the edges of its power network."

- Greentech Media, February 2, 2015

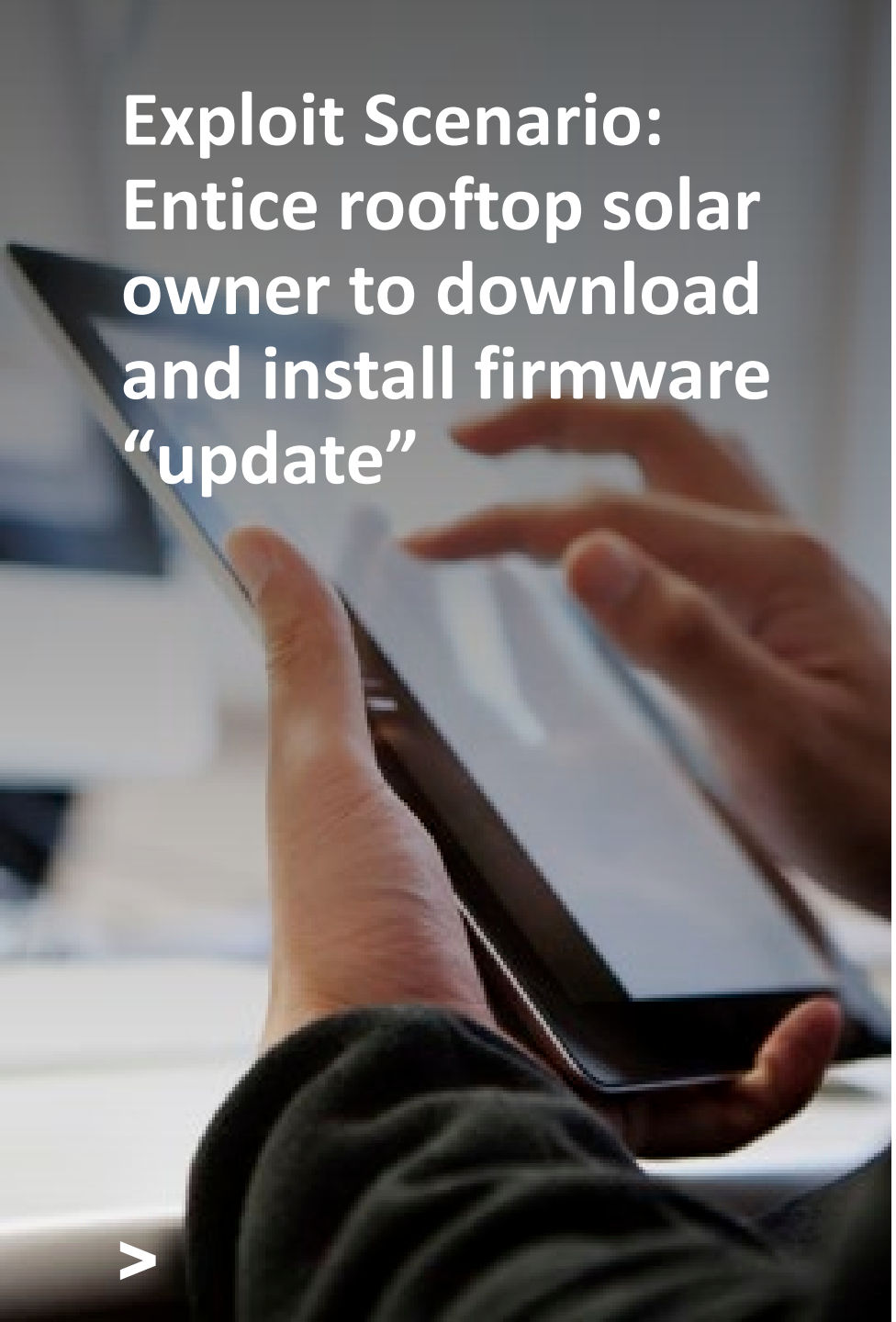
California and Hawaii already feeling impacts of distributed energy resource deployments

RSAConference2022

Exploit Scenarios

Grid Tie with Complete Off-Grid Solution Testbed

Exploit Scenario: Entice rooftop solar owner to download and install firmware “update”



Reply | Delete | Junk | Block | ···

Solar Owner's Toolkit

[redacted]

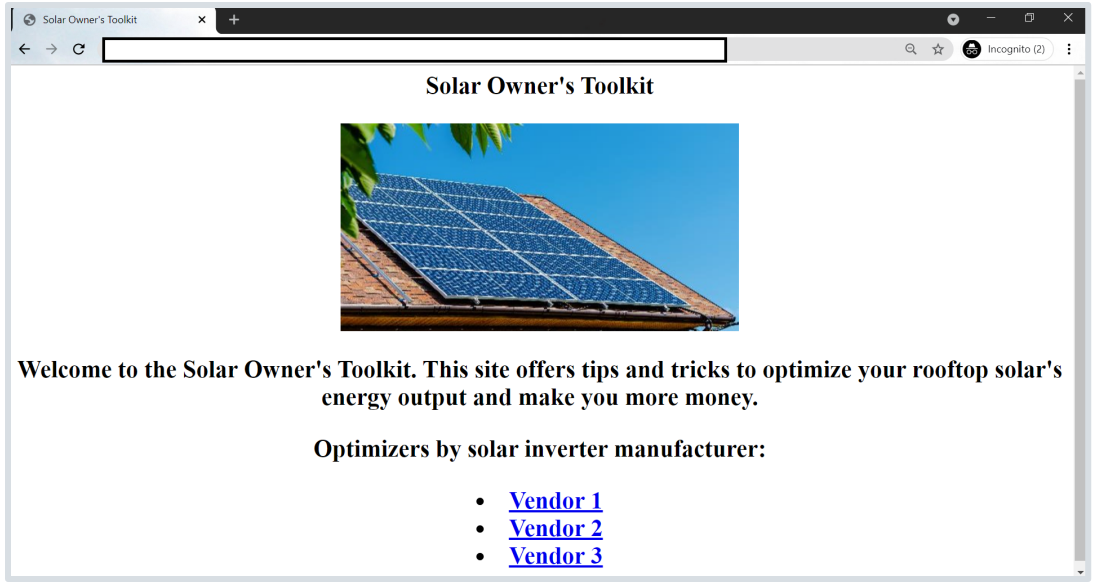
Tue 11/23/2021 4:30 PM

To: You

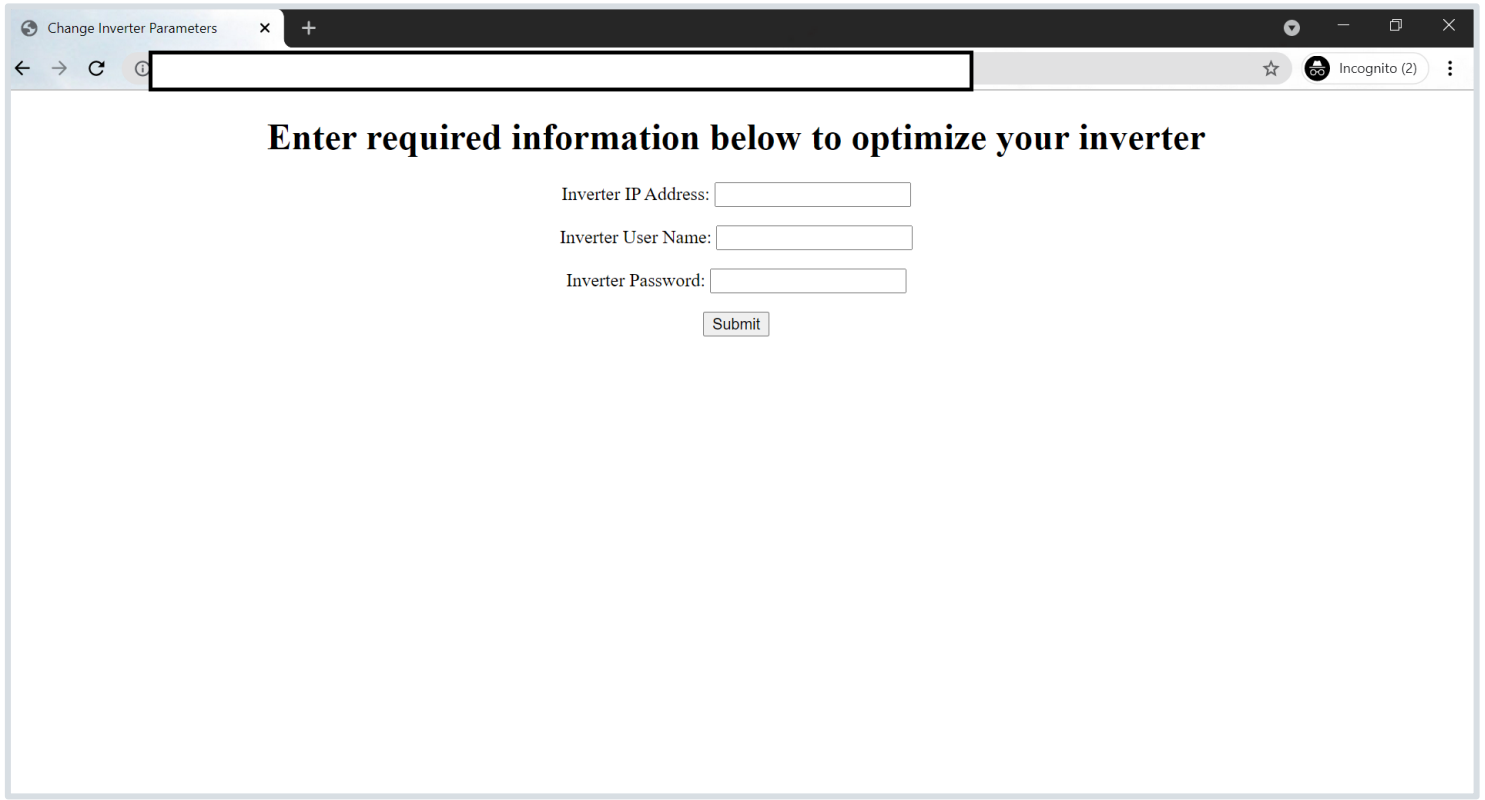
Dear Rooftop Solar Owner,

As a valued XYZ Energy customer and someone who is dedicated to cleaner energy, we occasionally will recommend resources to help you get more out of your rooftop solar deployment. Today’s resource is the Solar Owner Toolkit, which offers tips and tricks to optimize your solar output. The site can be found here.

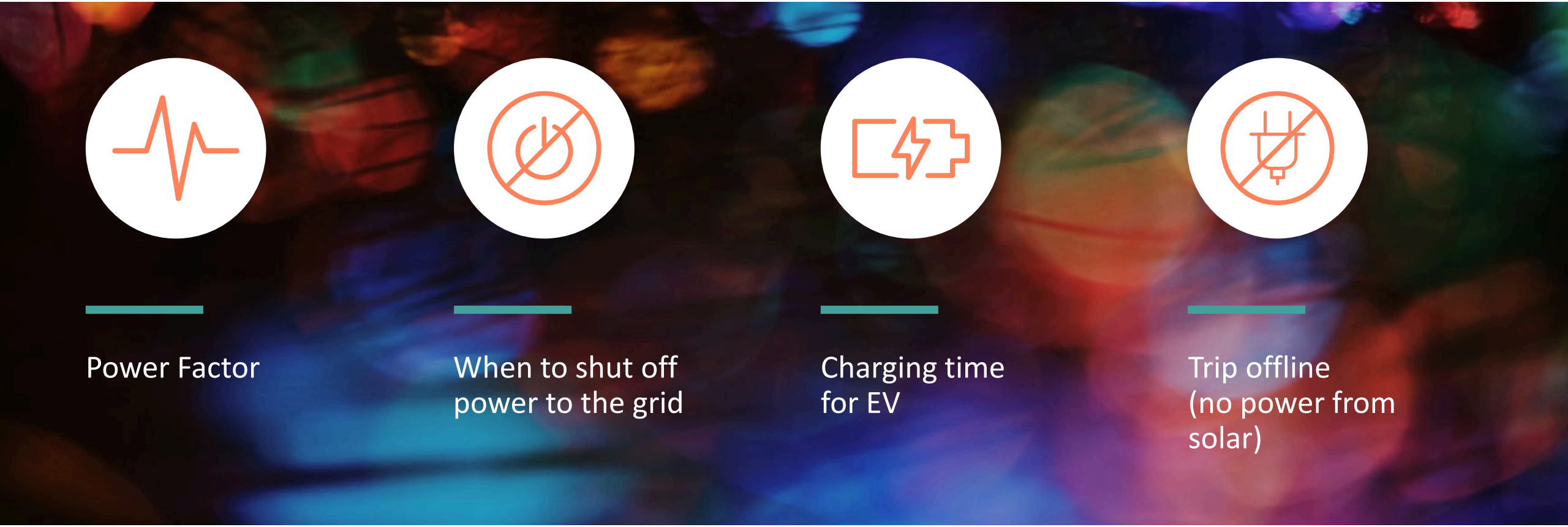
Sincerely,
XYZ Energy



A Simple Example



Here's What the Script Can Change



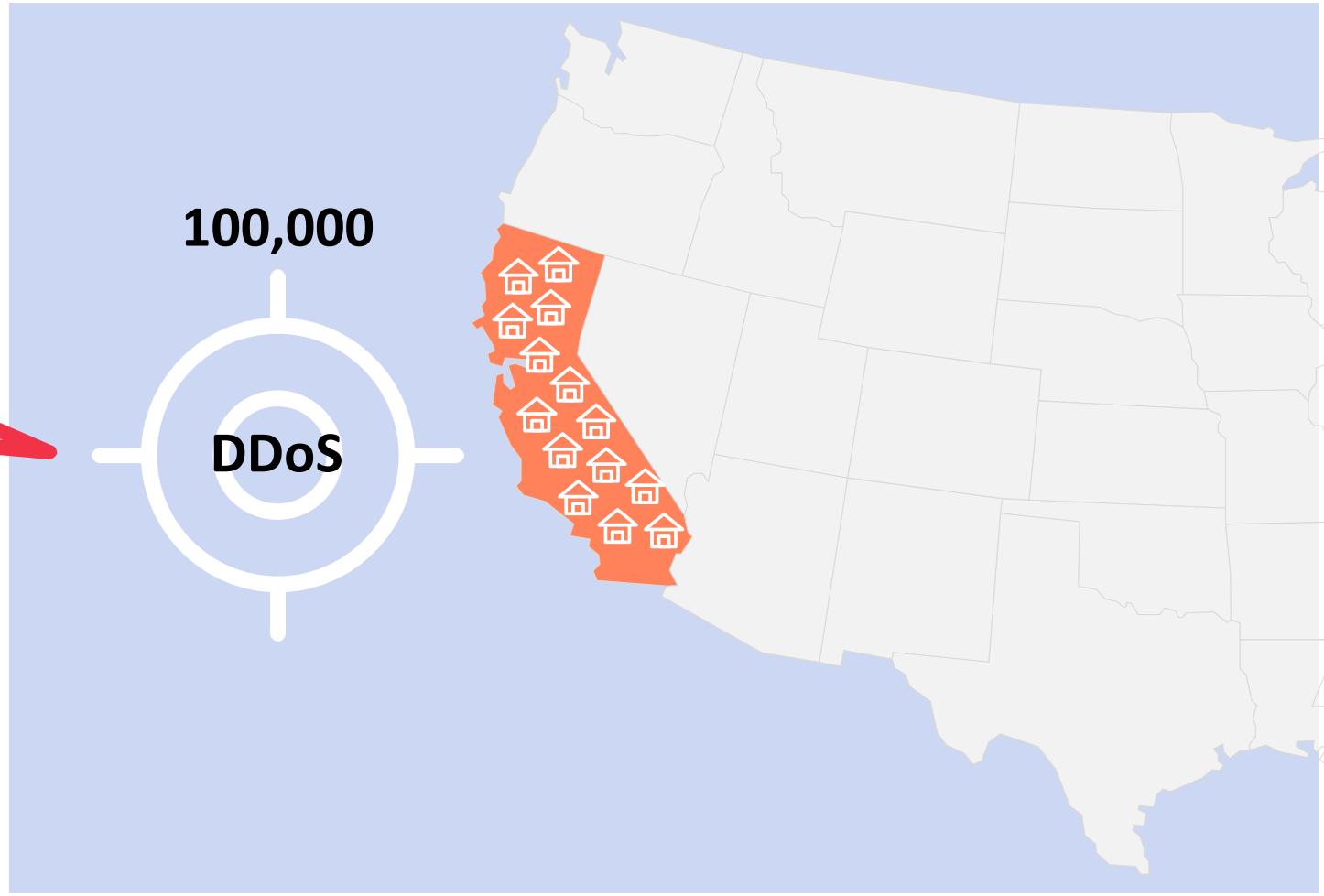
Power Factor

When to shut off power to the grid

Charging time for EV

Trip offline (no power from solar)

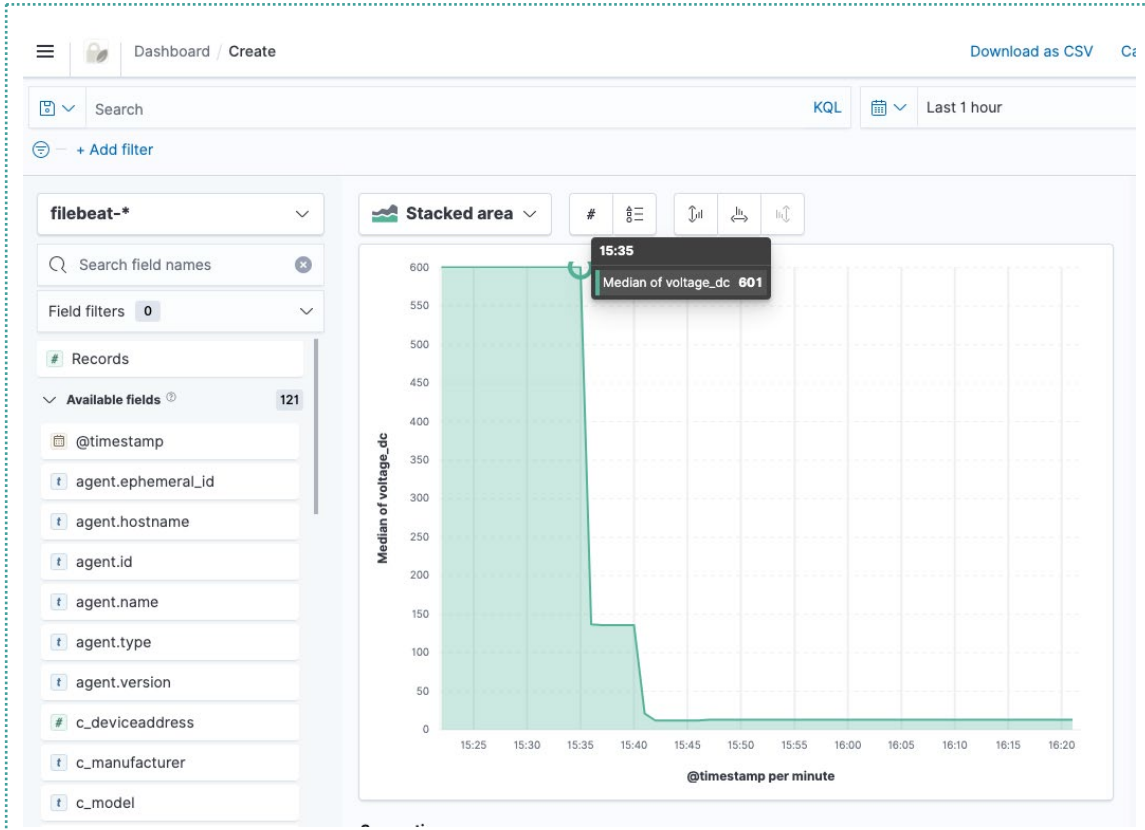
What Could Happen If This Attack Scaled



Electric Vehicle Charging Manipulation

Attacker gains access to utility supervisory control and data acquisition (SCADA) system to monitor the peak load or changes the Distributed Energy Resource Management System (DERMS) control settings so that when the system load is above a certain limit, it sends a command to all vehicles to charge at the same time.

How to Detect



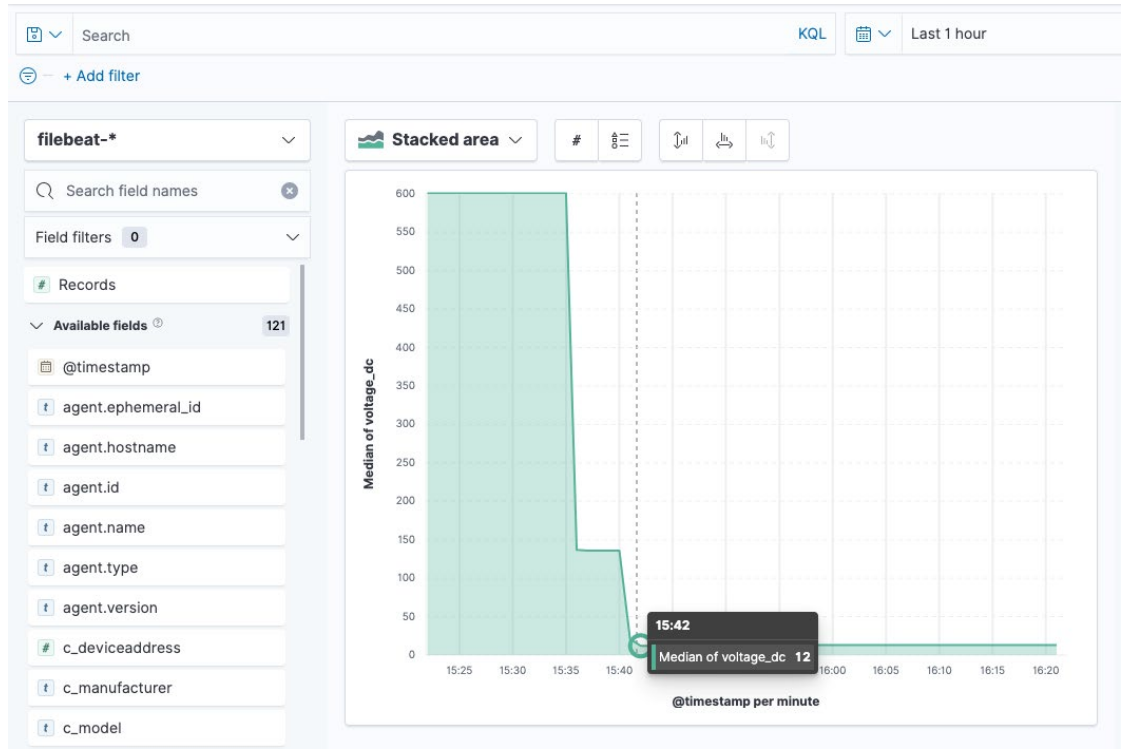
Scenario 1

A single solar station receives traffic from an unknown address, and soon after stops reporting generation data.

An alert is created noting the correlation between physical disconnect and unknown traffic.

Some time later, when more devices receive traffic from similar addresses and go offline, the managed security center issues a high warning for a crypto locker outbreak, altering utilities, manufacturers, and customers to the new threat.

How to Detect



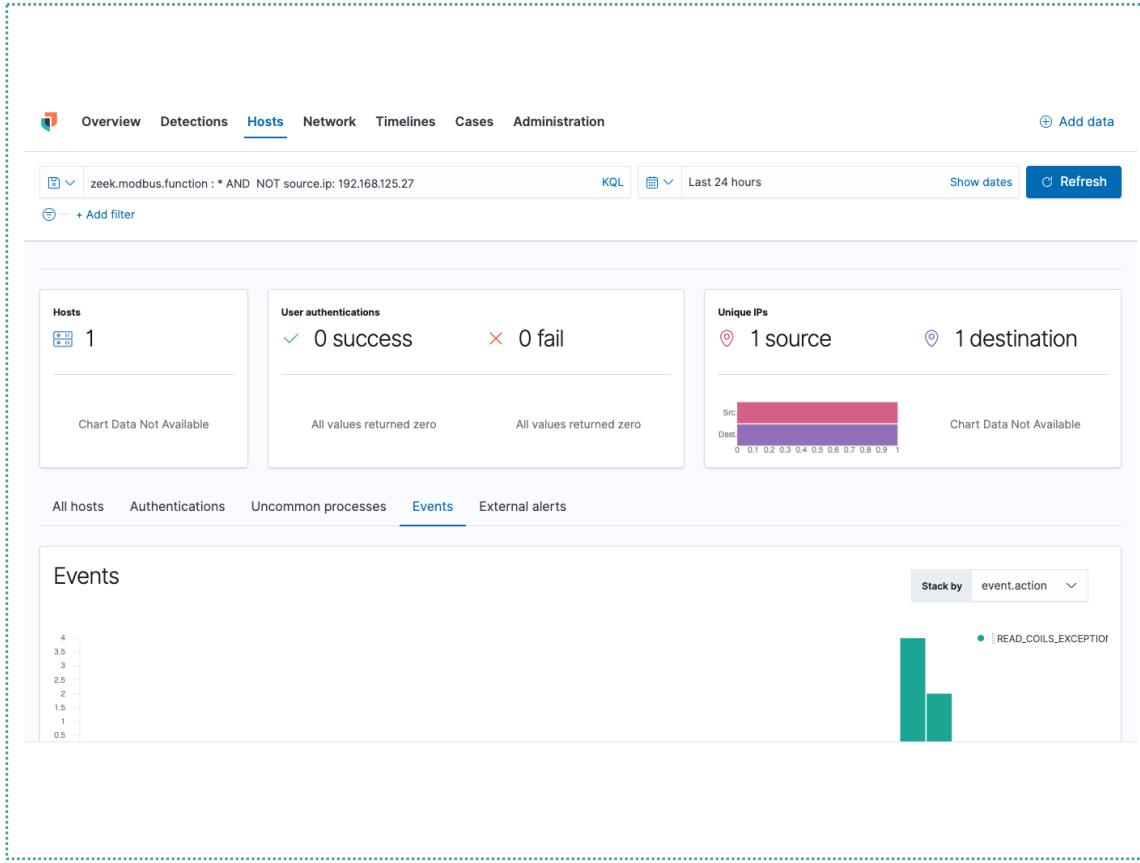
Scenario 1

A single solar station receives traffic from an unknown address, and soon after stops reporting generation data.

An alert is created noting the correlation between physical disconnect and unknown traffic.

Some time later, when more devices receive traffic from similar addresses and go offline, the managed security center issues a high warning for a crypto locker outbreak, altering utilities, manufacturers, and customers to the new threat.

How to Detect



Scenario 1

A single solar station receives traffic from an unknown address, and soon after stops reporting generation data.

An alert is created noting the correlation between physical disconnect and unknown traffic.

Some time later, when more devices receive traffic from similar addresses and go offline, the managed security center issues a high warning for a crypto locker outbreak, altering utilities, manufacturers, and customers to the new threat.

How to Detect

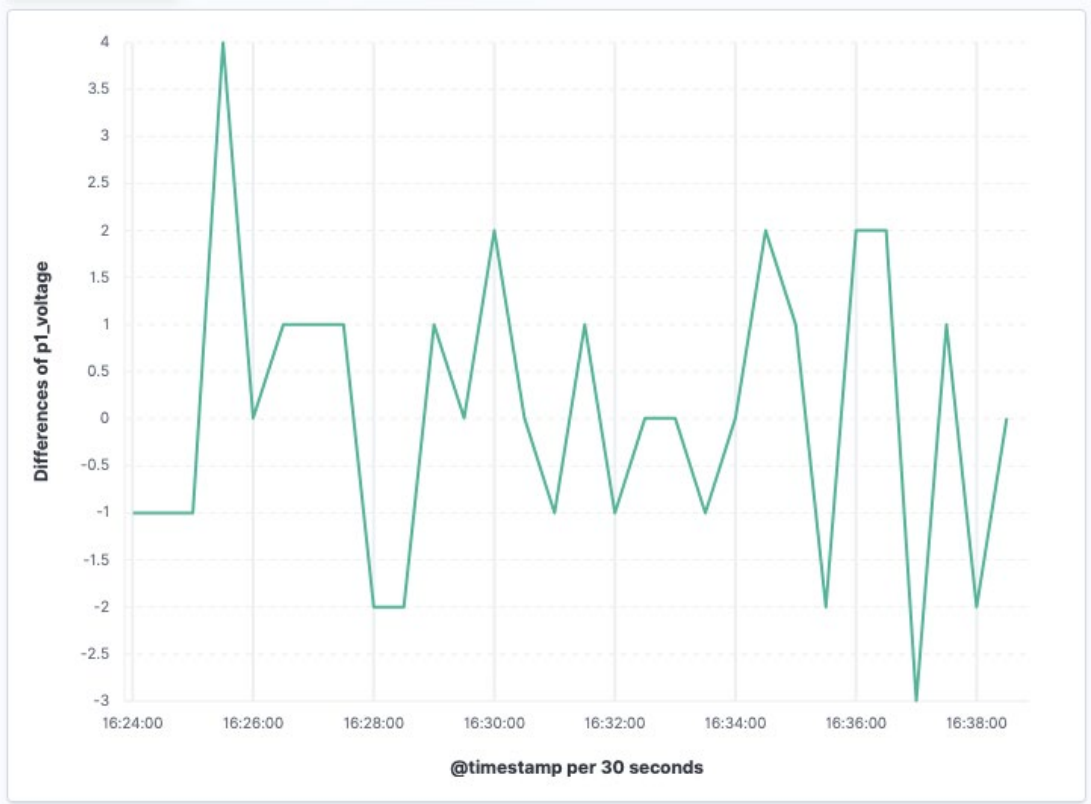
Scenario 1

A single solar station receives traffic from an unknown address, and soon after stops reporting generation data.

An alert is created noting the correlation between physical disconnect and unknown traffic.

Some time later, when more devices receive traffic from similar addresses and go offline, the managed security center issues a high warning for a crypto locker outbreak, altering utilities, manufacturers, and customers to the new threat.

How to Detect

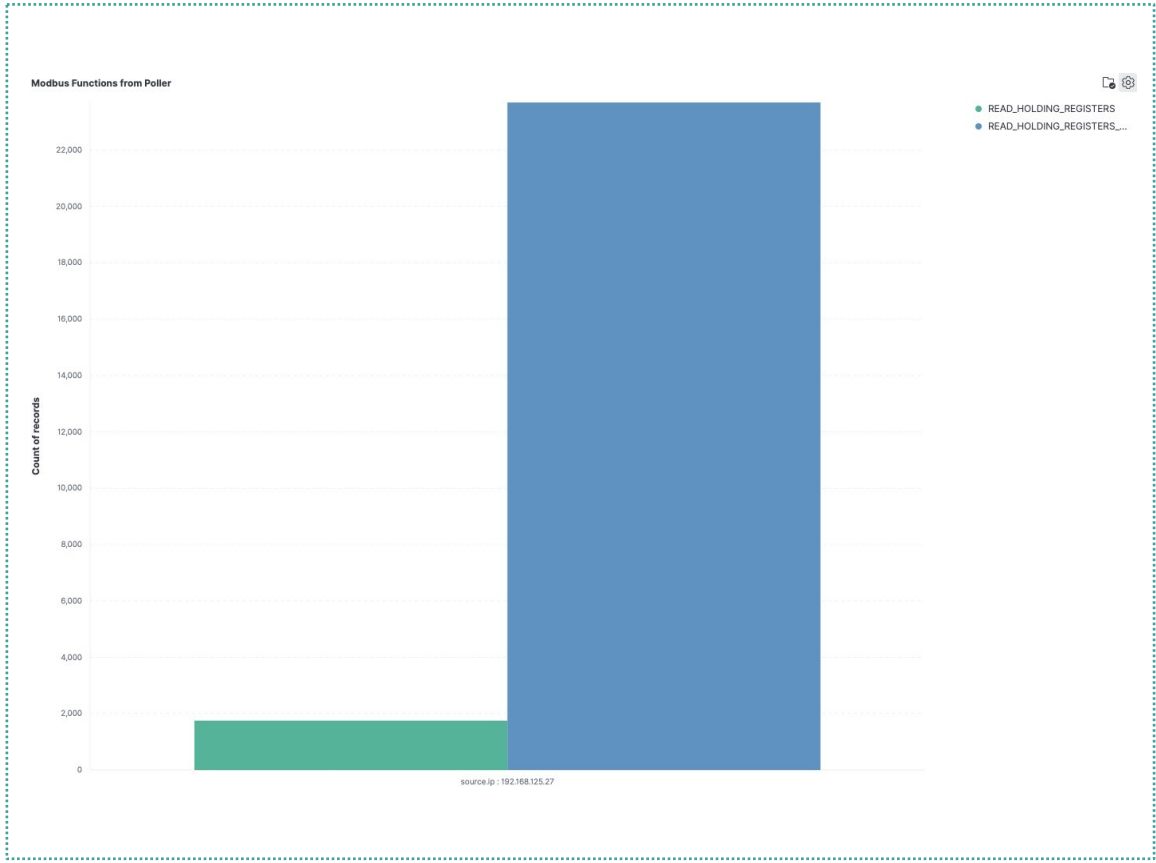


Scenario 2

Monitoring a geographic group of DERMS devices is showing that the ride through safety conditions programmed into inverters across the area are being changed repeatedly just below notification thresholds.

After checking with the utility energy management system (EMS) group, and validating that no such utility actions are planned, the managed services team can alert the utility and government agencies to a probable large-scale event targeting and tampering of DERMS devices.

How to Detect

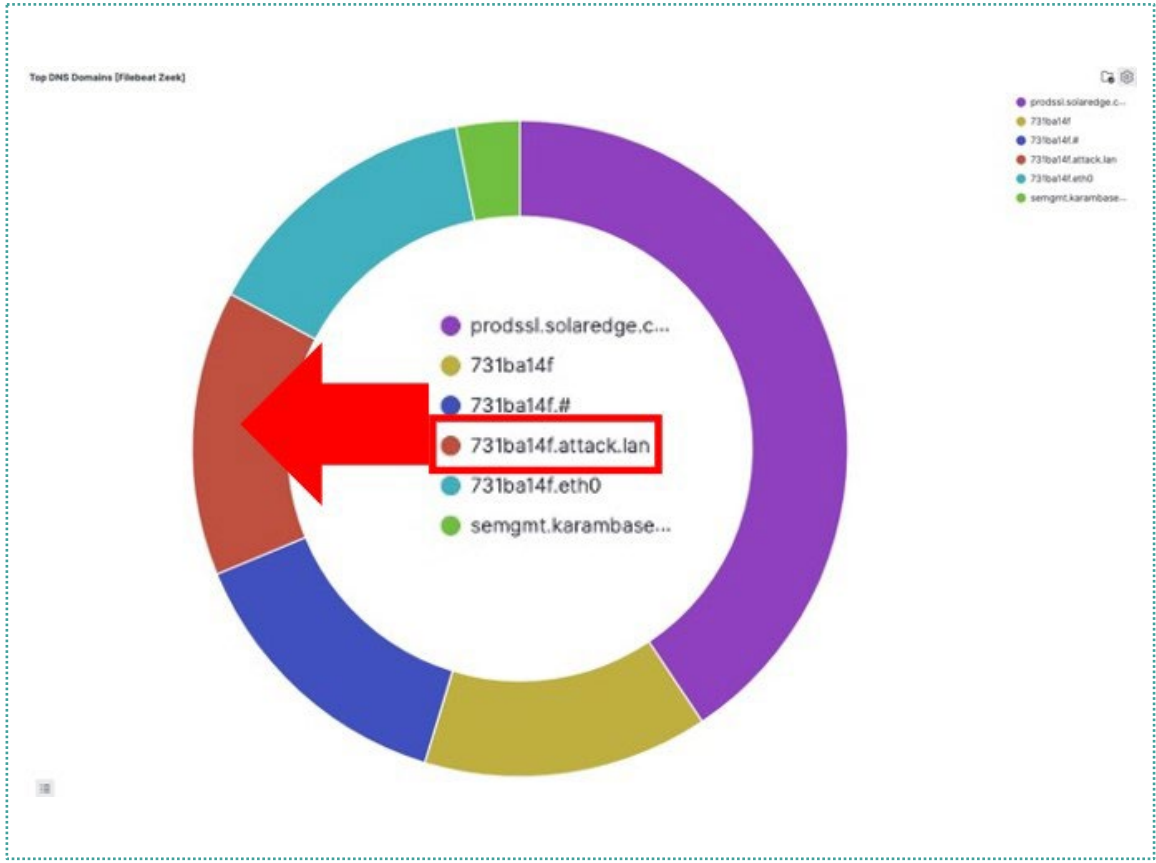


Scenario 2

Monitoring a geographic group of DERMS devices is showing that the ride through safety conditions programmed into inverters across the area are being changed repeatedly just below notification thresholds.

After checking with the utility EMS group, and validating that no such utility actions are planned, the managed services team can alert the utility and government agencies to a probable large-scale event targeting and tampering of DERMS devices.

How to Detect



Scenario 2

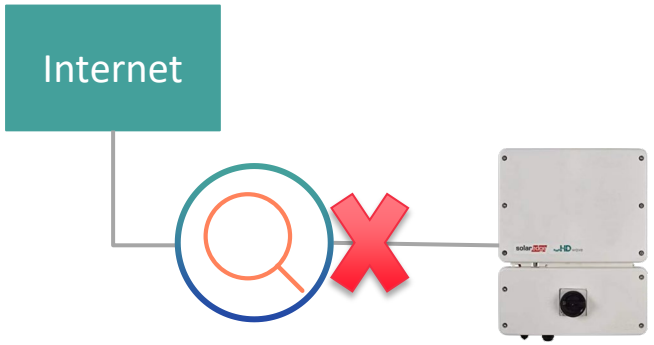
Monitoring a geographic group of DERMS devices is showing that the ride through safety conditions programmed into inverters across the area are being changed repeatedly just below notification thresholds.

After checking with the utility EMS group, and validating that no such utility actions are planned, the managed services team can alert the utility and government agencies to a probable large-scale event targeting and tampering of DERMS devices.

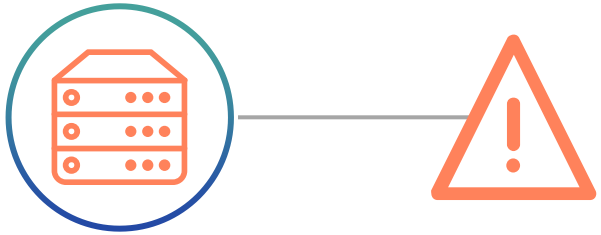
How to Prevent

Require digital signatures and verification when updating firmware

Deploy inline detection and blocking capabilities co-located with the distributed energy resource



Generate warning when inverter owners attempt to make atypical configuration changes



Require aggregators and product vendors to validate data before sending to utility

Apply What You've Learned Today (For Utilities)

Next week you should:

- Understand how data flows from third-party owned distributed energy resources (DER) to utility systems

In the next three months, you should:

- Examine those data flows to look for suspicious or unexplained behavior in the data and develop detection criteria
- Talk to your DER vendors about how they build protection into their products

In the next six months, you should

- Work with aggregators, inverter vendors, and others to deploy threat detection and response capabilities to detect and thwart attacks on DERs

Apply What You've Learned Today (For Distributed Energy Resource Owners)

Next week you should:

- Review the configuration of your system to better understand potential threat vectors leveraging hardening guidance where available and review energy bill and credit statements for unexpected charges or credits

In the next three months, you should:

- Where possible, work with your utility, solar aggregator, or inverter vendor to better understand how they might be able to detect threats to your system and how you can help with the response

In the next six months, you should

- Apply additional hardening and other guidance provided by utilities and others to better prevent, detect, and respond to attacks

RSAConference2022

Questions?

Gib Sorebo – gilbert.n.sorebo@accenture.com

Aaron Bayles – aaron.bayles@accenture.com