FORESCOUT

Automated Cybersecurity Across Your Digital Terrain

DO YOU WANT TO BE THE NEXT HEADLINE?

IDENTIFY AND RESPOND TO REAL THREATS WITH

# FORESCOUT

Eduard Serkowitsch
Principal System Engineer

June, 2023

# Case Studies

**KEY BENEFITS**

- Improved ICS visibility and reduced site inspections effort
- Strong improvement of policy compliance & Maintenance scheduling
- Detection of several suspicious process behavioral patterns

# Infrastructure

- **Challenge**

Several land and water infrastructure sites, for example, tunnels, bridges and dams, with various process control and building management systems. Many sites were installed more than a decade ago having outdated asset inventory and showing unexpected behavior. The sites are maintained by collaborating with different system integrators increasing the need for synchronization and coordination.

- **Solution**
  - Started with network assessments at misbehaving sites. **Now a deployment with 24/7 SOC integration across 70 sites & expanding**
  - **Detected policy violations**: unscheduled local maintenance
  - **Investigation of unusual behavior**: Found cause of downtime
  - **Customizations with Forescout Visibility & Threat Detection** Extensibility Framework (SD Scripts), for example, to alert local vs. remote operation of a bridge or to recognize and track behavior of proprietary control system communication incl. Ethernet-only traffic (no TCP/IP).

**KEY BENEFITS**

- Reduced site inspections and improved maintenance
- Easier and effective monitoring of network policies and fulfillment
- Minimized risk of downtime due to misconfigurations, synchronization issues or unscheduled maintenance

# Food Chilean Manufacturer

- **Challenge**

This prospect has no real visibility form the OT network. The current infrastructure is practical unknown for the customer including issues, types of PLC, brands and any risk issue from five food plants

- **Solution**
  - Provided unprecedented information on controllers and plant network hosts via Forescout's **asset discovery capability**
  - Provide **complete visibility form OT devices and full visualization of communications** between devices
  - **Detection of possible operation issues** with Modbus between OT nodes
  - **Found vulnerabilities** in the OT devices and HMI that could impact operation
  - Create a **Site Map according the devices and trace what are the most used or unused resources**

**KEY BENEFITS**

- Provide insights into current vulnerabilities specific to OT
- Improved asset management
- Faster troubleshooting

# California Resources (raw material) Corporation

## Challenge

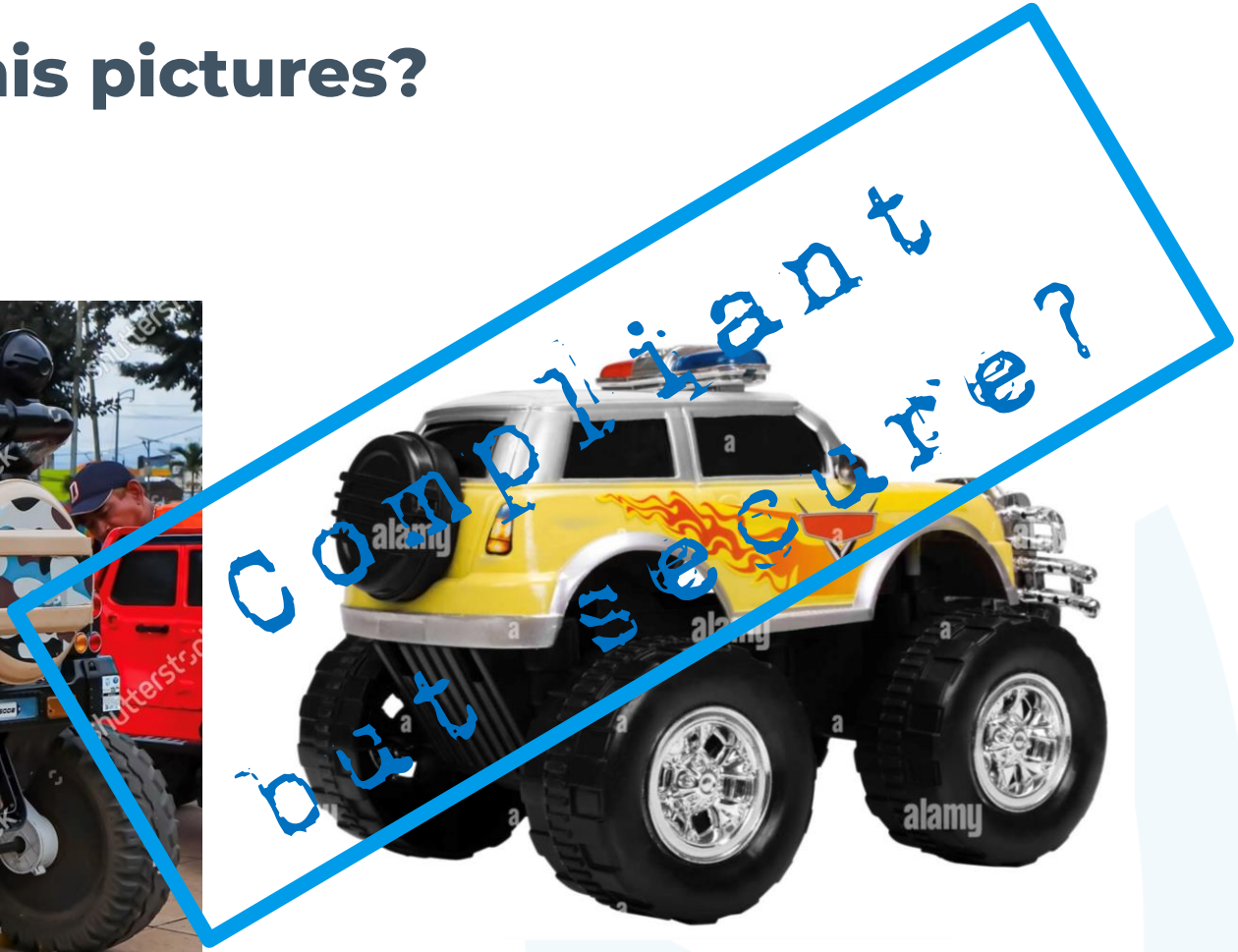
Customer had visibility limitations within their OT environment for their assets and communication patterns. This limitation caused other challenges involving risk management and vulnerabilities that were present. Vulnerability scanner provides little information on OT/ICS devices.

## Solution

- Provided **visibility for all OT devices and their communication patterns passively**
- Identified **network connections to destinations that no longer exist** giving insights into possible configuration errors
- Provides alerting capabilities for **outages and network anomalies**
- Accurately provide quarterly reports for assets and vulnerability trends.

# Definitions and Regulations

# What‘s wrong in this pictures?



# What is Profile, Risk and Acceptance

Profile


THREAT ACTOR = SOMEONE WHO WANTS TO PUNCH YOU IN THE FACE

THREAT = THE PUNCH BEING THROWN

VULNERABILITY = YOUR INABILITY TO DEFEND AGAINST THE PUNCH

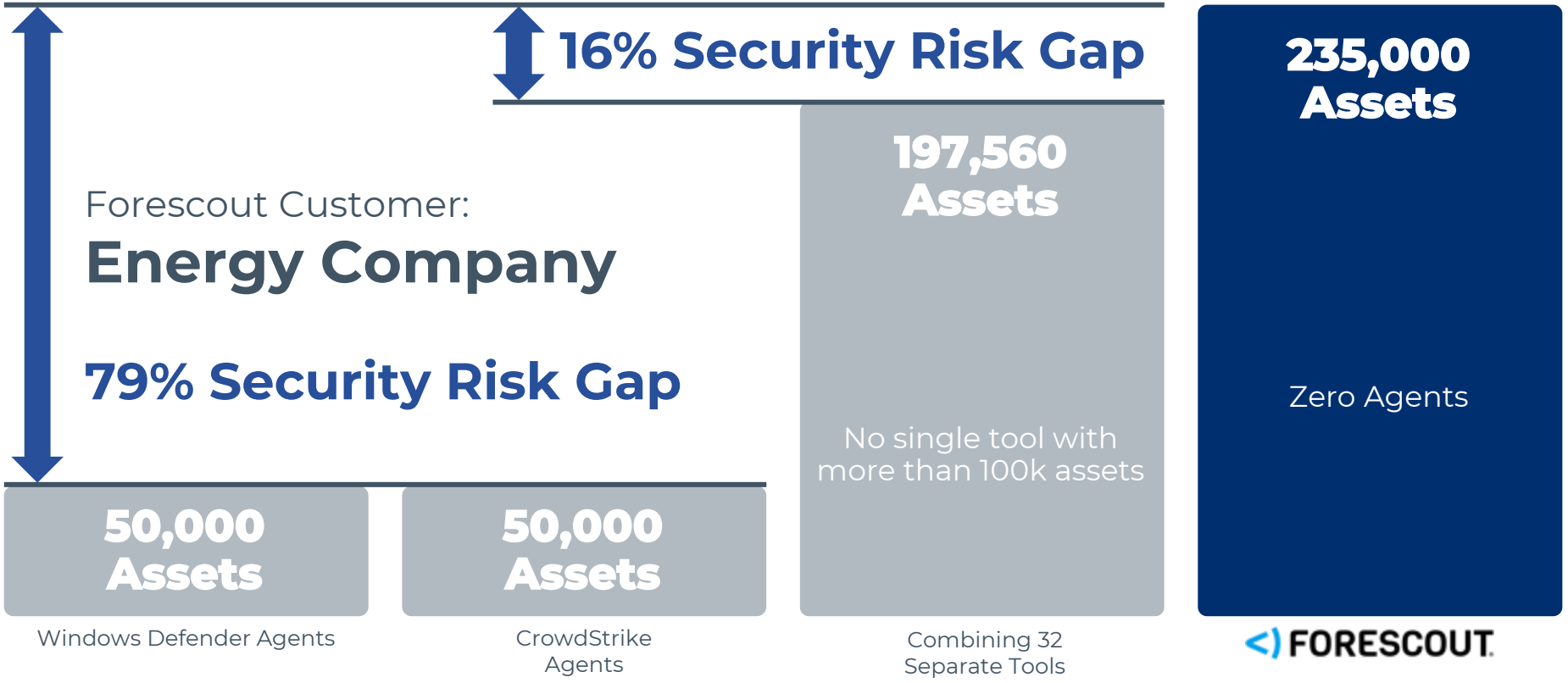
RISK = THE LIKELIHOOD OF GETTING PUNCHED IN THE FACE

ACCEPTABLE RISK = YOUR WILLINGNESS TO BE PUNCHED IN THE

# Real World

# Real-World Example

Rapid time to value for a holistic view of all devices



# Today’s SOC Reality

**450**

alerts per hour [1]

**28%**

of alerts are simply never addressed [1]

**45%**

of alerts are false positives [2]

**75%**

of enterprises spends an equal amount, or more time, on false positives than on legitimate attacks. [3]

1 “The State of Security Operations”, Forrester 2020
2 “The Voice of the Analysts: Improving Security Operations Center Processes Through Adapted Technologies” IDC InfoBrief
3 “Reaching the Tipping Point of Web Application and API Security”, 2021, ESG

# 1

## Detection* per hour

High fidelity
High confidence

FORESCOUT

*** Detection**: A SOC-actionable probable threat that warrants human investigation

Based on aggregate data from a 1-year period (Dec 2021-2022),
across 31 enterprises, representing a range of company sizes and industries.

vs

# 450

## Alerts per hour

Low fidelity
Low confidence

## TYPICAL SOC

11,000 alerts per day = 450 alerts per hour
Source: “The 2020 State of Security Operations”, Forrester Consulting

The actual number of alerts a SOC receives depends on a many factors including the number, type and location of security controls deployed, the tuning of those controls (which is a function of analyst capacity, risk tolerance and level of expertise), and the number of employees / devices, and industry.

# The Forescout Offerings in 2023

## Network Security

- Network Access Control
- Network Segmentation Management
- Zero Trust

## Forescout eXtended Detection & Response XDR

- Threat Detection & Investigation
- Threat Hunting
- Incident Response

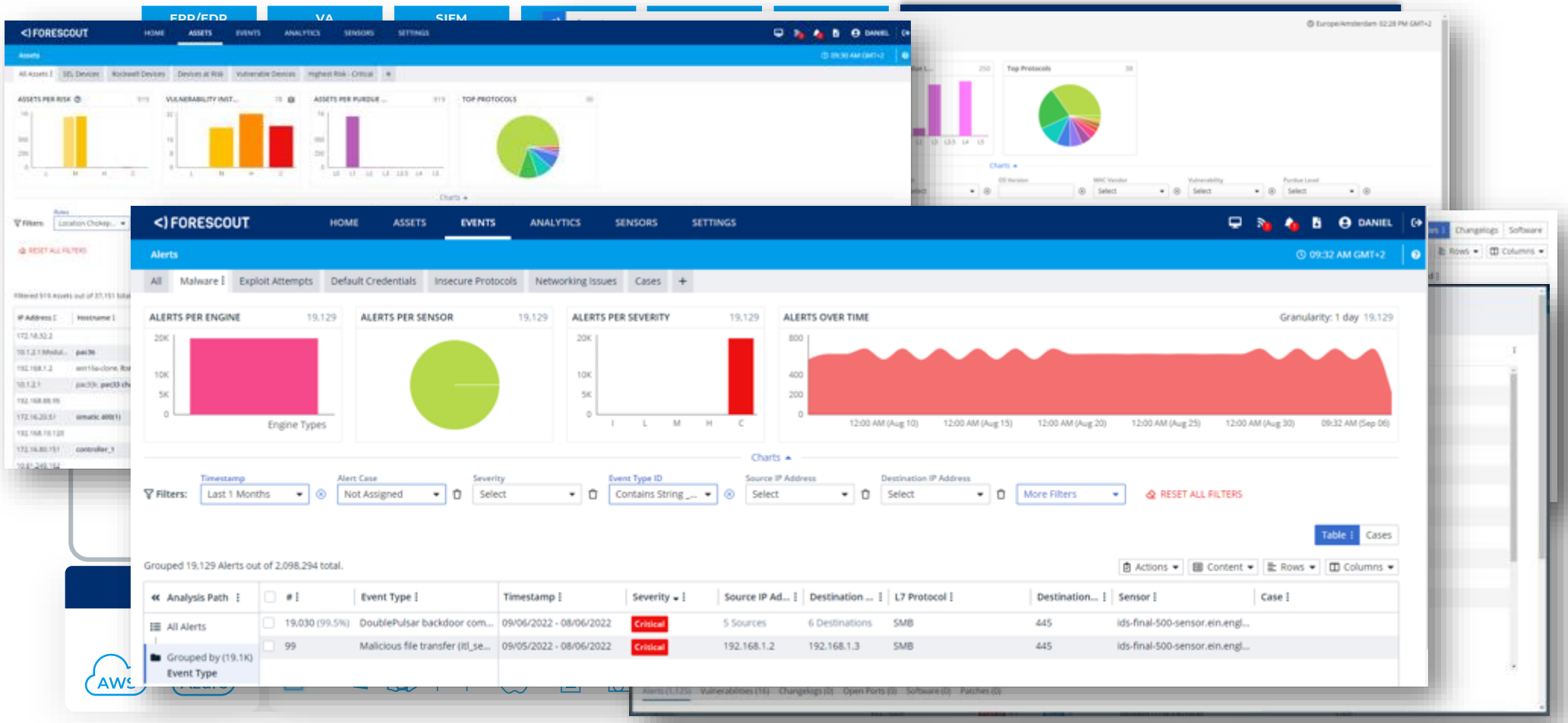
## Risk and Exposure Management REM

- Asset Discovery & Inventory
- Asset Compliance & Risk Mgmt
- Cyber Asset Attack Surface Mgmt

**Forescout Cloud 2.0 platform**

**Each offering has integration methods to network infrastructure, 3rd party services and applications, and to the other offerings**

# The Forescout Platform



# Why Forescout?

## Over 20 years of cybersecurity expertise...

- *Headquartered in Dallas, Texas*
- *Employees in over 30 countries*
- *Leader in complete IT –OT–IoT–IoMT visibility and threat research*

## Over 3000 customers globally...

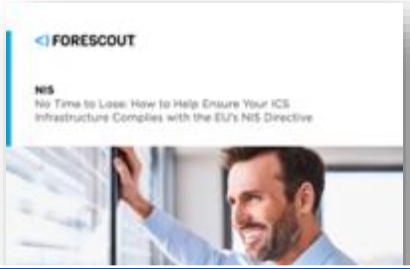
- *30% of Fortune 100, 20% of Global 2K*
- *Expertise across Financial, Insurance, Healthcare, Government, and Utilities industries*

## Trusted and Proven...

- *Millions of end points deployed in US DoD Comply-to-Connect Program*
- *Completed Project Memoria, the most extensive study of TCP/IP stacks that uncovered 97 new vulnerabilities impacting over 400 vendors*
- *Diverse customer case studies and recognized by numerous industry awards*


**Managing cyber risk through automation and data-powered insights.**

# Regulations & Standards for the Industry




| NERC-CIP | EU NIS / NIS 2 Directive | NIST Cybersecurity Framework | IEC 62443 |
|---|---|---|---|
| The **North American** Electric Reliability Corporation (NERC) is a private non-profit organisation responsible for developing a list of critical infrastructure protection standards (NERC-CIPs). The standards address critical infrastructures for **electricity production and transmission** and are among the most detailed and comprehensive cybersecurity standards of this kind. Utilities can face high fines if cyber security protection is not sufficient. | The European Union's Directive on the security of Network and Information Systems (NIS), establishes an advanced set of cyber security objectives for organizations supplying essential services in the EU. The NIS rules are transposed into national law by May 2018 and form the basis for the current EU cybersecurity regime. For essential service providers breaches of the Directive could generate significant fines in the millions of Euros. However, the definition of what constitutes an essential service, and how the NIS will be applied, is different in every EU country. | The U.S. Commerce Department's National Institute of Standards and Technology (NIST) has released version 1.1 of its Framework for Improving Critical Infrastructure Cybersecurity, more widely known as the Cybersecurity Framework. It is a voluntary framework and was developed with a focus on industries vital to national and economic security, e.g. energy and communications. It has since proven flexible enough to be adopted voluntarily by large and small companies and organizations across all industry sectors, as well as by federal, state and local governments. | IEC 62443, formerly known as ISA 99, is the worldwide de facto standard for security of industrial control system (ICS) networks. The standard was created by the International Society of Automation (ISA) and was taken over by the International Electrotechnical Commission (IEC), who is responsible for further developing it. IEC 62443 assists in the evaluation of existing and potential vulnerabilities within ICS and aids in applying the necessary mitigations. The overall goal of this standard is to reduce the risk of threats and failures within ICS networks. |
| Forescout e-book: https://www.forescout.com/simplify-nerc-cip-compliance-with-continuous-network-monitoring/ | Forescout e-book: https://www.forescout.com/company/resources/nis-directive-ensuring-ics-infrastructure-compliance | Forescout e-book: https://www.forescout.com/solutions/compliance/ebook-how-to-align-with-the-nist-cybersecurity-framework/ | Forescout e-book: https://www.forescout.com/company/resources/how-to-effectively-implement-isa-99iec-62443/ |



FORESCOUT

Thank you.