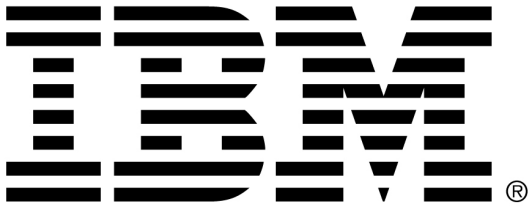

infosecurity
EUROPE
Security Workshops



Securing The ICS Environment

Cliff Wilson - ITS Security Services

30/04/14

infosecurity EUROPE

Cyber threats to industrial control systems are growing daily...

Inappropriate control valve access

Alarm disabling

Distribution disruption and damage

Signal tampering

Ingress to core or back end systems

The energy sector (oil, gas, electric) was the target of over 55% of cyber attacks in 2013

Source: ICS-CERT 2013 report

The threats and exploits are real and becoming more publicised

May 2013: Hacking group Anonymous announces its intention to launch security attacks against the oil & gas sector.

Saudi Aramco Struck By Shamoon Attack

Malware attack infected approximately 30,000 workstations at the world's largest oil producer.

Information Week, Aug 2012

RasGas Hit By Computer Virus

RasGas, the world's second-biggest LNG exporter, found its corporate networks and computers over-run by a hostile virus.

Reuters, Aug 2012

Telvent IT Breach Led to OT IP Theft

Attacker penetrated firewalls and security systems, implanted malicious software, and stole project files for systems that remotely control portions of the electric grid.

ZDNet, Sep 2012

Night Dragon Oil & Gas Targeted Campaign

State-sponsored attacker stole gigabytes of highly sensitive material, information on oil and gas field operations, financial transactions, and bidding data from at least five major energy companies.

Council on Foreign Relations, July 2013

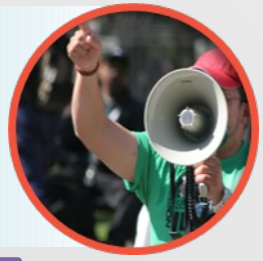
According to the Ponemon Institute, 76 percent of the energy sector admits to recent security breaches

Motivations and sophistication are rapidly evolving

National Security, Economic Espionage

Nation-state actors, APTs
Stuxnet, Aurora, APT-1

Notoriety, Activism, Defamation



Hacktivists
Lulzsec, Anonymous

Monetary Gain

Organized crime
Zeus, ZeroAccess, Blackhole Exploit Pack

Nuisance, Curiosity, Revenge

Insiders, Spammers, Script-kiddies
Nigerian 419 Scams, Code Red
Bought-In tools

Top reasons WHY compromises occur in the IS/IT World

End users/endpoints

1. Double-clicking "on anything"
2. Disabling endpoint security settings
3. Using vulnerable, legacy software and hardware
4. Failin
5. Failin
6. Failin
7. Conn insecu
8. Using creati
9. Using busine
10. Givin

Infrastructure

1. Connecting systems/virtual images to the Internet before hardening them
2. Connecting test systems to the Internet with default accounts/passwords
3. Failing to update or patch

BUT – FOR ICS (OT), it's a different picture…

- **Attacks are more focused**
- **Attackers are much better prepared and more skilled**
- **Attacks typically take longer to execute**
- **The motive is often damage to production or extortion**
- **Defences are typically very weak or non-existent**

And, of course, the results can be significantly more serious

80-90%

can be easily avoided!

incoming or outgoing.

10. Failing to segment network and/or adequately monitor/block malicious traffic with IDS/IPS

Critical defences are not always “up to scratch”

Forbes.com

Hackable Backbone

The first time Scott Lunsford of IBM offered to hack into a nuclear power station, he was told it would be impossible. There was no way, the plant's owners claimed, that their critical components could be accessed from the Internet. Lunsford, a researcher for IBM's Security Systems, found otherwise.
"It turned out to be one of the easiest penetration tests I'd ever done," he says. "By the first day, we had penetrated the network. Within a week, we were controlling a nuclear power plant. I thought, 'Gosh. This is a big problem.'“

In retrospect, Lunsford says--and the Nuclear Regulatory Commission agrees--that government-mandated safeguards would have prevented him from triggering a nuclear meltdown. But he's fairly certain that by accessing controls through the company's network, he could have sabotaged the power supply to a large portion of the state. "It would have been as simple as closing a valve," he says.

http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack_print.html

The insurance industry seems to agree…

Underwriters at Lloyd's of London say they have seen a "huge increase" in demand for cover from energy firms.
But surveyor assessments of the cyber-defences in place concluded that protections were inadequate.

… Energy industry veterans said they were "not surprised" the companies were being refused cover.

And…some stuff is just very hard to secure
- Wireless RF/ WiFi Attacks

- Increased use of wireless technologies
- Large security research focus
  - Common topic/stream at hacking conferences
- Packet Radio Software
  - New tools and software to attack & eavesdrop on any RF transmission
  - Community-based sharing of findings
- Easy access to tools and guides on long-range interception or wireless technologies
- Deep perimeters are no longer a defence

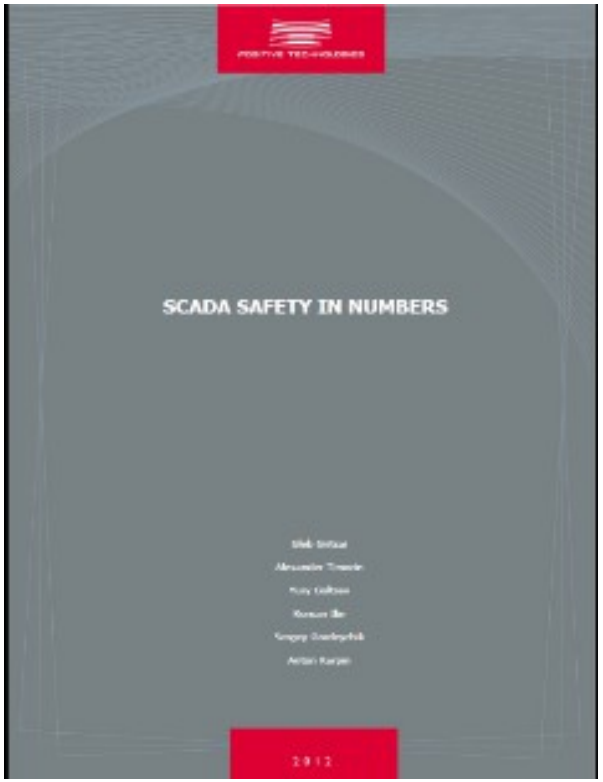
A 14.6 dBi Yagi antenna that can make a WiFi connection from 5Km away

Common IBM Security Assessment findings

- Weak protocols leave systems vulnerable
- Many ICS networks lack overall segmentation
- Many Security staff do not understand IP issues
- Over-reliance on “compliance”
- Most ICS networks lack antivirus protection
- Standard operating systems leave the device open to well known security vulnerabilities
- Most IP-based communications within the ICS network are not encrypted – to even a basic level
- Most ICS systems have limited-to-no logging enabled
- Patches are not, or cannot be installed on SCADA systems
- No host based security controls are configured on these devices
- Many organizations still rely heavily on physical security measures

Despite ongoing risk reduction efforts, the industry is still much more vulnerable than would be expected

- Since 2000, there has been a **10-fold increase** in the number of **successful** cyber attacks against SCADA systems at power generation, petroleum production and nuclear plants
- The number of detected vulnerabilities has increased by **20 times** since 2010
- **50%** of vulnerabilities allow **code to execute**
- There are **exploits for 35% of vulnerabilities** detected
- **41%** of vulnerabilities are **critical**. More than **40%** of systems available from the Internet **can be hacked by unprofessional users**
- **54%** and **39%** of systems available from the Internet in Europe and North America respectively are **vulnerable**



www.ptsecurity.com/download/SCADA_analytics_english.pdf

So…how bad could it get? – the “2012 Internet Census”

Fun Idea - Let’s Port Scan the Internet…

So, how big is the Internet? That depends on how you count.

420 Million pingable IPs + 36 Million more that had one or more ports open, making 450 Million that were definitely in use and reachable from the rest of the Internet

141 Million IPs were firewalled, so they could count as "in use". Together this would be 591 Million used IPs.

729 Million more IPs just had reverse DNS records. If you added those, it would make for a total of 1.3 Billion used IP addresses.

The other 2.3 Billion addresses showed no sign of usage

So, with one hundred thousand devices scanning at ten probes per second “we” would have a distributed port scanner (Botnet) to port scan the entire IPv4 Internet within one hour

A lot of devices and services we have seen during “our” research should NEVER connected to the public Internet at all. As a rule of thumb, if you believe that "nobody would connect that to the Internet, really - nobody", there are at least 1000 people who did. Whenever you think "that shouldn't be on the Internet but it’ll probably be found a few times“, it's there a few hundred thousand times. Like half a million printers, or a Million Webcams, or a whole generation of industrial control devices that have “root” as a root password...

Source - http://internetcensus2012.bitbucket.org

Auditing the ICS estate

- do you know exactly what you have – supposedly under YOUR control?

SHODAN (released by John Matherly in 2009) crawls the Internet looking for devices, many of which are programmed to answer. It has found cars, fetal heart monitors, office building heating-control systems, water treatment facilities, power plant controls, traffic lights and glucose meters etc

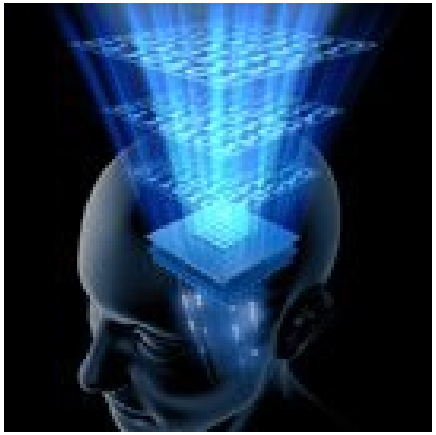
A free search will get you ten results. Approximately 10,000 users pony up a nominal one-time fee of up to $20 to get 10,000 results per search. A dozen institutional users, all of them cybersecurity firms, pay five figures annually for access to Matherly's entire database of 1.5 billion connected devices.

Source: September 23, 2013 issue of Forbes.

If you don't know – somebody else probably does!

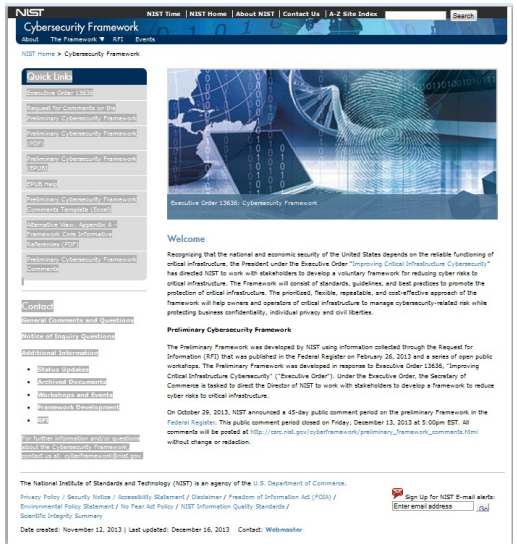
Addressing The Problem…

- **The NIST Cyber Security Framework**
- **ICS Security Assessments (incl. Penetration testing)**
- **Education and Awareness**
- **ICS Security Intelligence solutions based on existing technologies**



Go NIST Cyber Security Framework – Now!

In the US, the new NIST framework provides guidance to enterprises on securing their industrial control systems



- Drafted based on Executive Order 13636 to protect the nations critical infrastructure
- Provides a flexible framework for assessing an organization's critical infrastructure cyber protection
- Provides guidance on evaluating risk without being prescriptive
- Version 1.0 of the Cybersecurity Framework was published on Feb. 12th, 2014

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

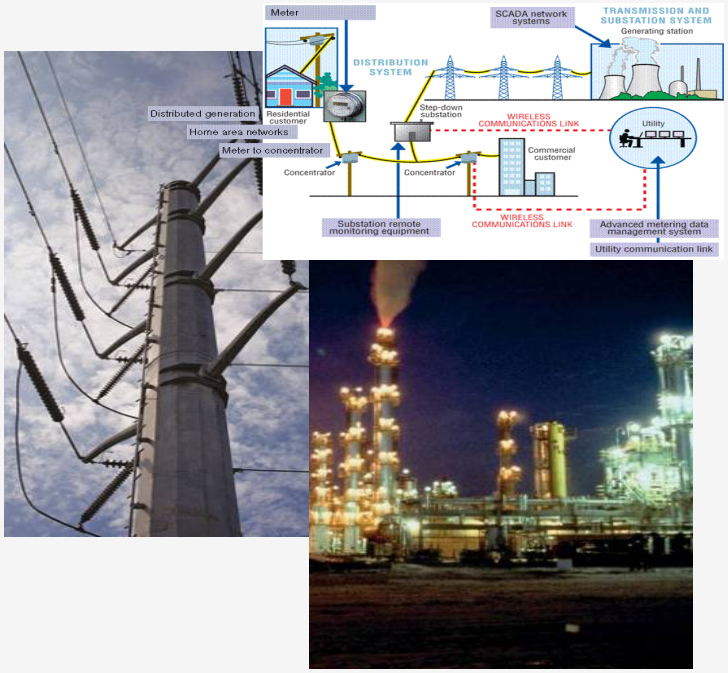
IBM is proud to have played a key role in the drafting and comment period – leveraging our extensive knowledge of cyber security and the specific threats involved

Industrial Controls Cybersecurity Consulting (IC3)

Consulting for the new NIST framework to help protect your operating infrastructure

Safeguarding your critical infrastructure assets

IBM NIST Cybersecurity Diagnostic

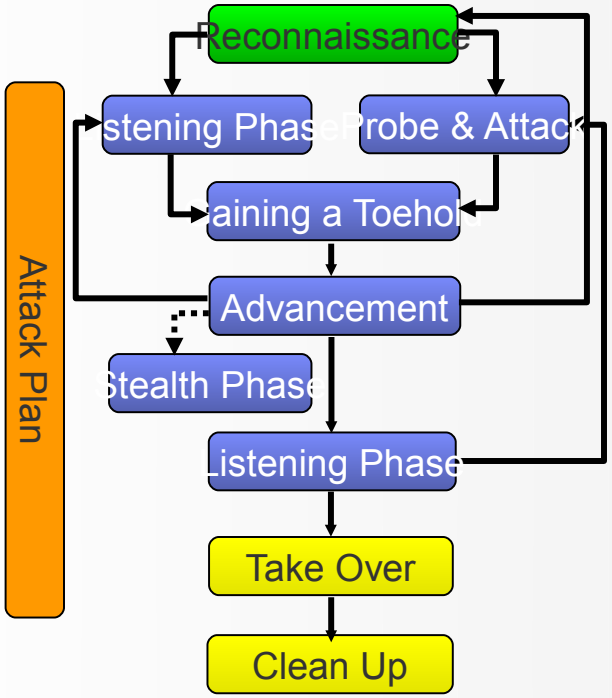


- **Provides a baseline assessment** of a client's security posture relative to the NIST CSF maturity model
- **Workshop oriented engagement** leverages tested methods and provides for interactive evaluation of security concerns
- **Provides education** on how the NIST CSF works, the intent and how to deploy it effectively
- **Risk-based analysis and recommendations** focused on key business processes
- **Self-Sustaining;** provides an ongoing operational self-analysis capability
- **Helps the CISO prioritize** the security investment in the company's critical infrastructure protection

ICS Penetration Testing

Initiations & Reconnaissance → Vulnerability → **Penetration** → Reports

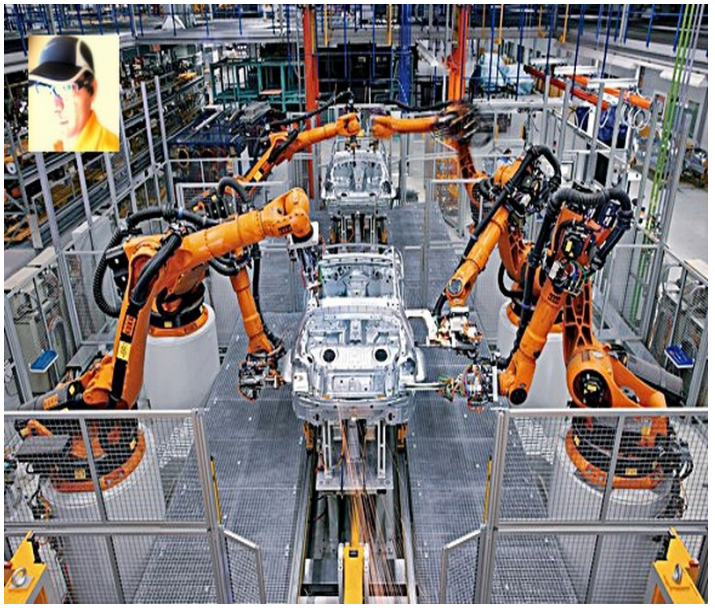
Penetration Test: following the IBM Ethical Hacking Methodology and inputs from X-Force researches, the penetration test will be executed systematically



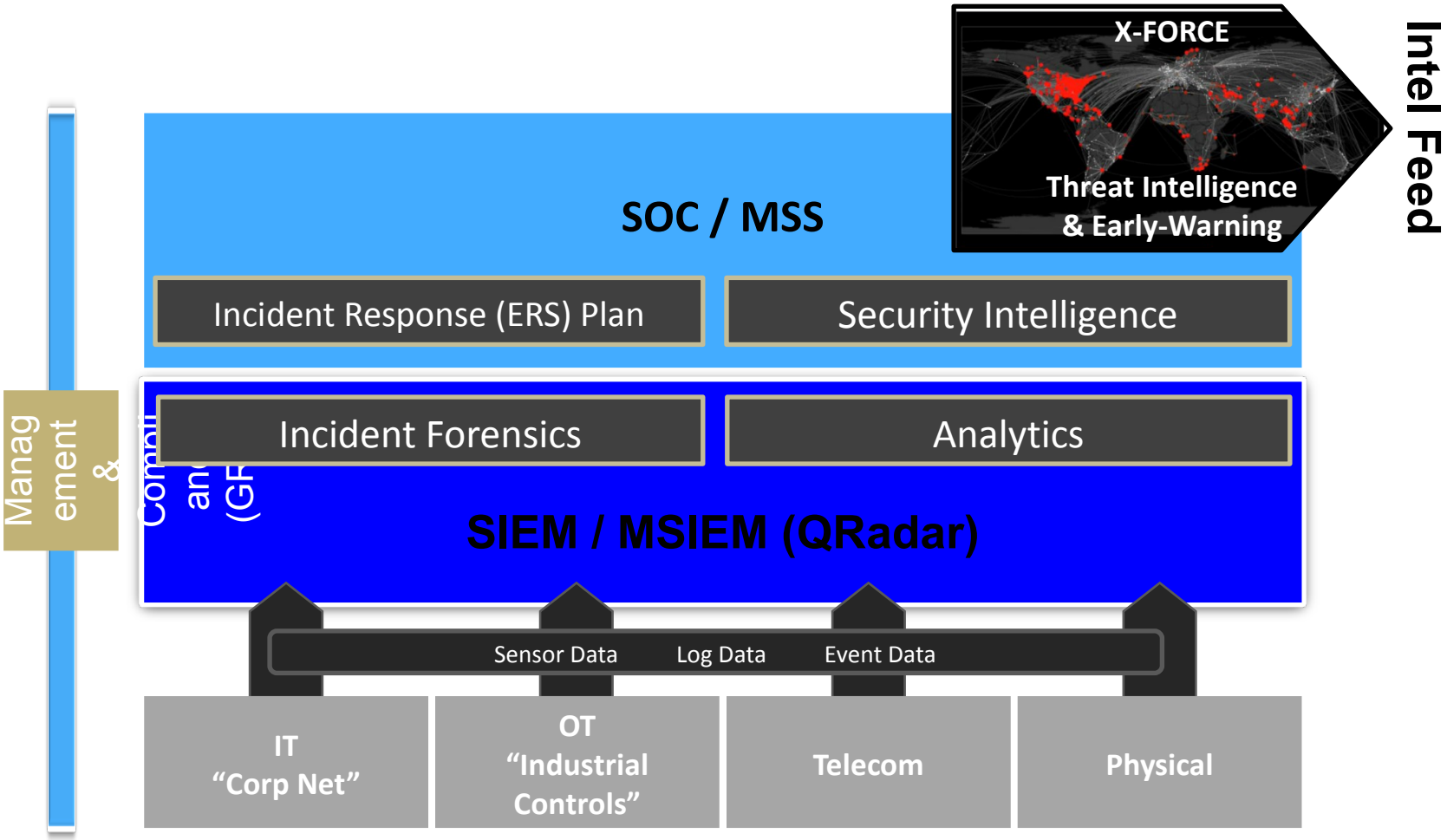
- Similar to the hacker behavior
- Through a systematical testing plan
- Leverage the commercial, open source and Proprietary tools developed by X-Force and the professional service team
- Reference the OWASP and OSSTMM Testing Guide

Organisations must also examine some fundamental shortcomings - NIST is only the starting point.

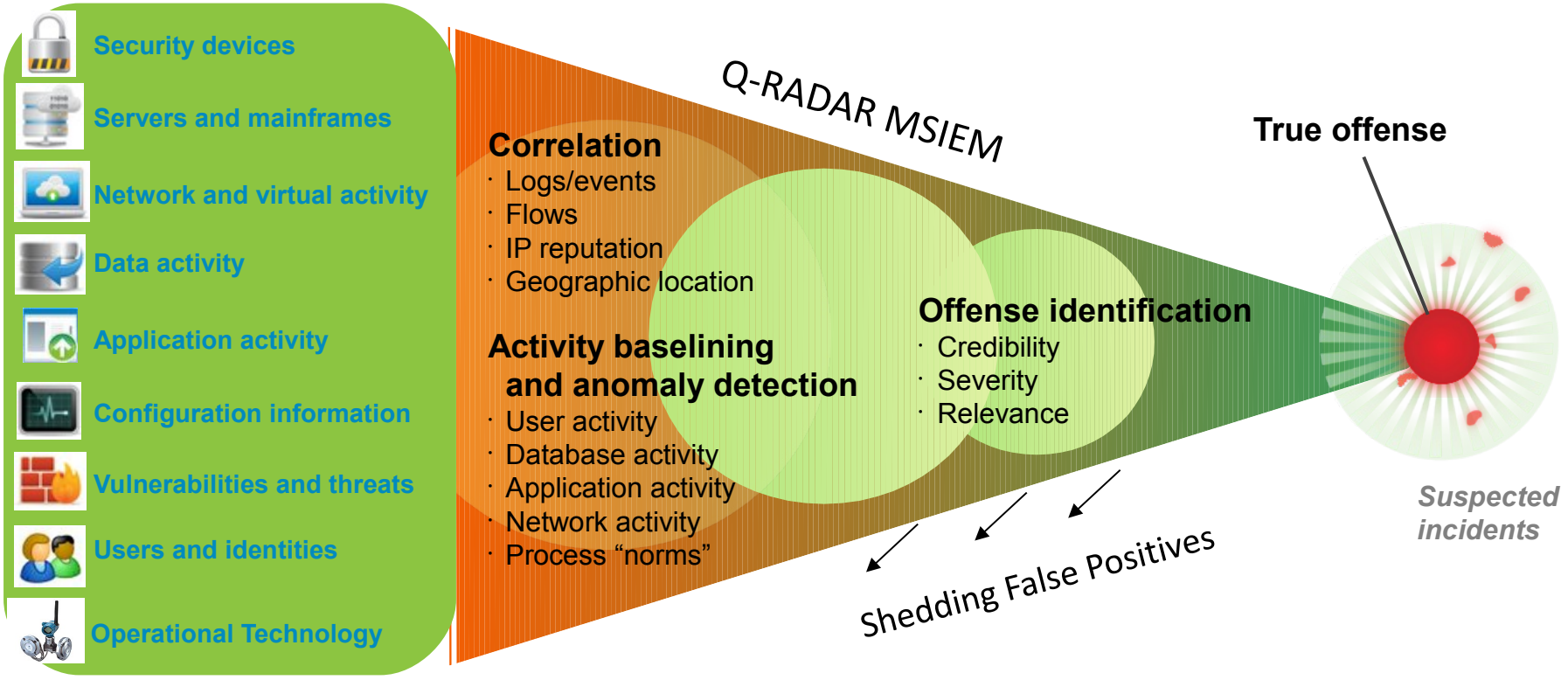
- Failure to adapt
  - Security models frozen in time, dating back to 2004 or earlier
  - Unable to secure the mixed bag of new and legacy equipment / devices
  - Unprepared to address the new interconnectedness (the Internet of Things) and new challenges - like BYOD
  - The “Grey Hair” problem (insurance company term) – Education needed
- Over-reliance on compliance
  - Secure does not mean complaint
  - Compliant does not mean secure
- Failure to govern effectively
  - Sluggish to address convergence of IT and OT
  - OT not feeding Enterprise-GRC
  - IT, OT, Physical and Telecom still operating as islands



Implement a set of security intelligence-led “rapid detection and response” capabilities - Strength in depth is no longer adequate protection



Enterprise Security Intelligence - Integrating across the IT and OT silos



Key Themes

Increased Data Sources

Data from 450+ security collectors and Integration with X-Force intelligence and other external feeds to use in analysis for determining relevant vulnerabilities and potential threats

Integrated Vulnerability Management

Comprehensive understanding of the configuration and exposure of systems in the environment, enabling contextual analysis to determine vulnerabilities against particular threats

Enhanced Identity Context

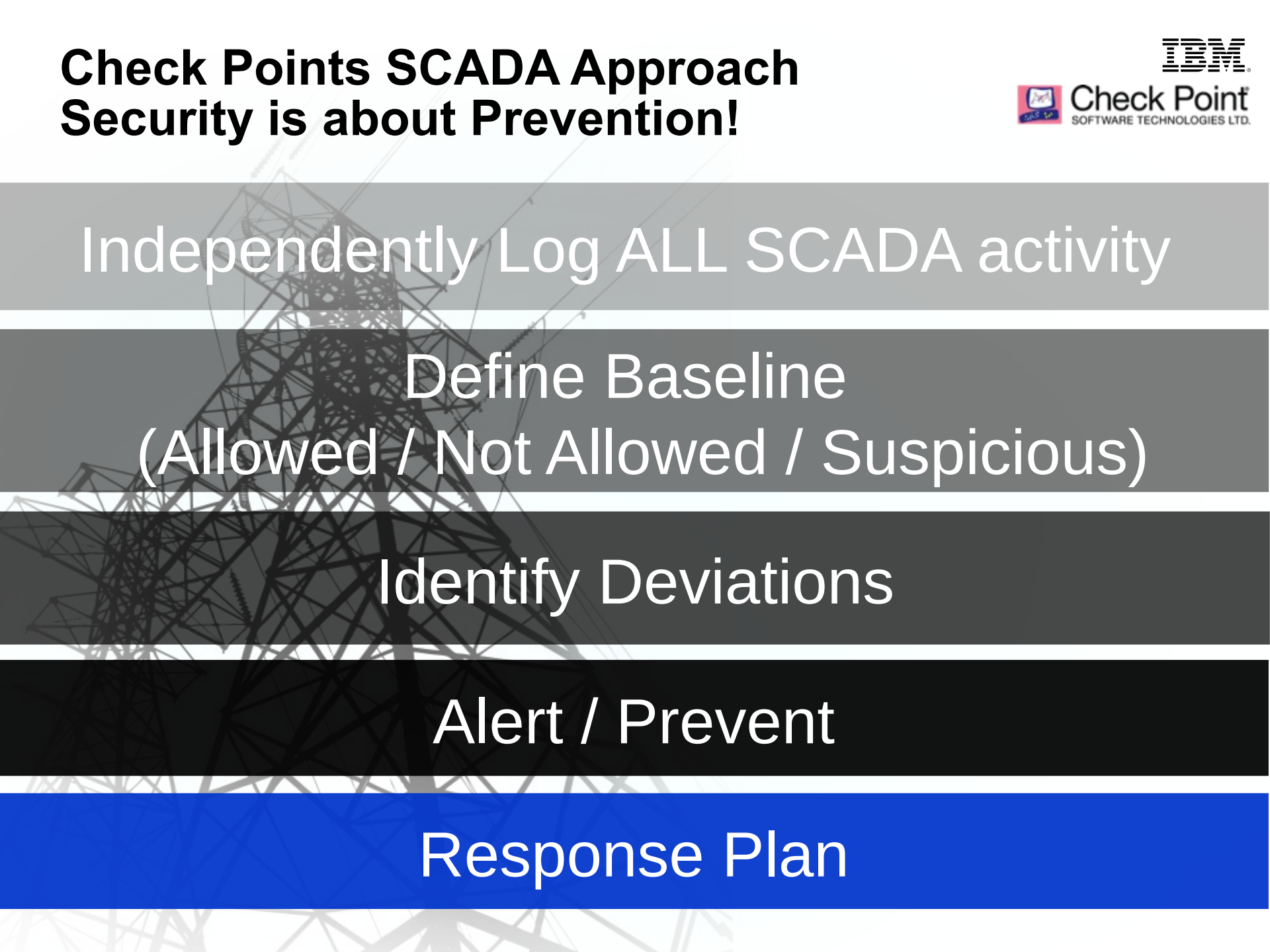
Integrated understanding of users, their roles, level of privilege, geographical location and their typical behaviors to enable enterprises to identify abnormal activity that might indicate insider threat

An example of an ICS Security Solution built using existing Appliances and Security Intelligence products

Check Points SCADA Approach
Security is about Prevention!

IBM

Check Point
SOFTWARE TECHNOLOGIES LTD.



Independently Log ALL SCADA activity

Define Baseline
(Allowed / Not Allowed / Suspicious)

Identify Deviations

Alert / Prevent

Response Plan

SCADA Firewall and Application Control

IBM

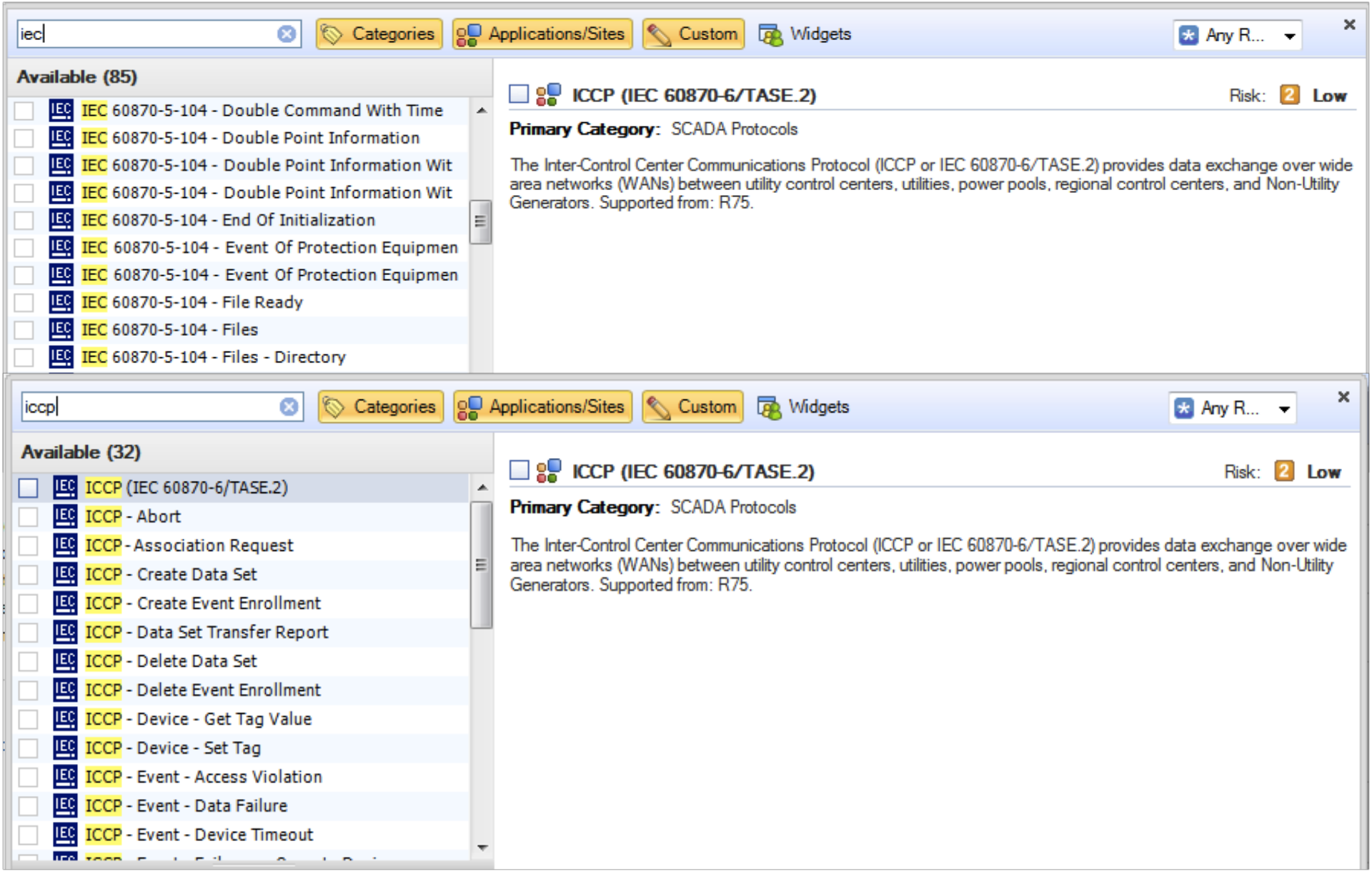
Check Point SOFTWARE TECHNOLOGIES LTD.

Protocol-specific controls with directional awareness

Policy granularity at the command level: e.g., read/write/get

Name	Source	Destination	Applications/Sites	Action
Block High Risk apps	Any	Any	High Risk	Block Blocked
Control servers	Control_servers	PLCs	Modbus Protocol-write single register Modbus Protocol-write multiple coils Modbus Protocol-write file record Modbus Protocol-write single coil	Allow
Monitor servers	Monitor_servers	PLCs	Modbus Protocol-read input register Modbus Protocol-read coils Modbus Protocol-read file record	Allow
Block SCADA traffic	Any	Internal PLCs	SCADA Protocols	Block

Granular SCADA Commands (Examples)



SCADA Protocols Support

- IEC 60870-5-104
- ICCP (IEC 60870-6)
- OPC
- DNP3
- MMS
- Modbus
- BACNet
- ELCOM-90 *
- Profinet *
- Profibus *

Additional protocols can be added per request

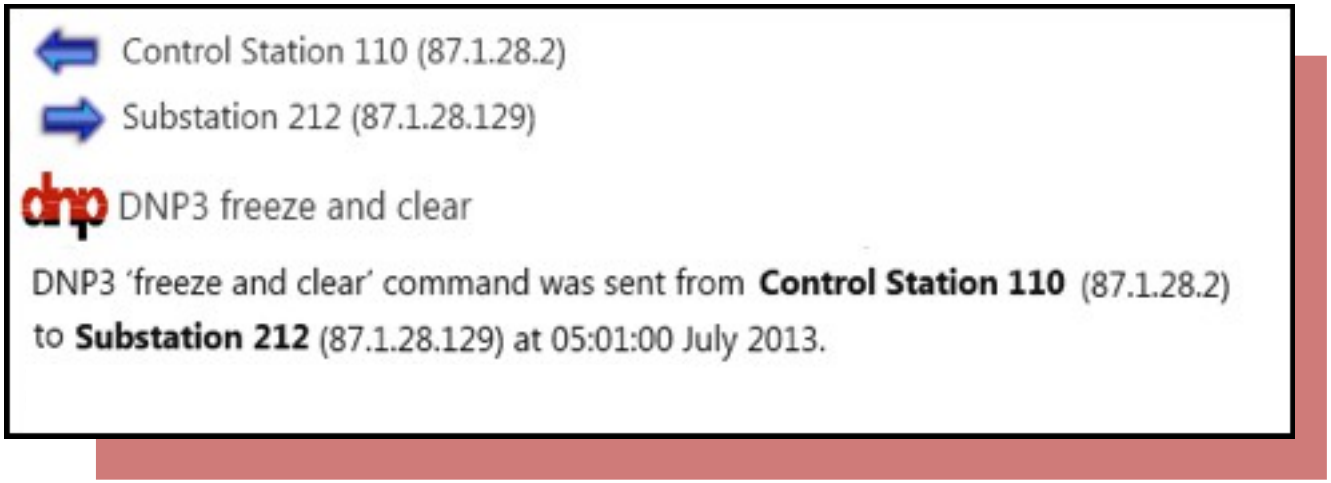
61000 System and 21400 Appliance

* In development

SCADA SmartEvent

Forensics are key for any investigation !

IBM Check Point SOFTWARE TECHNOLOGIES LTD.



History of all SCADA commands in the network

History of attempts to send excessive amount of commands

History of all network reconnaissance attempts

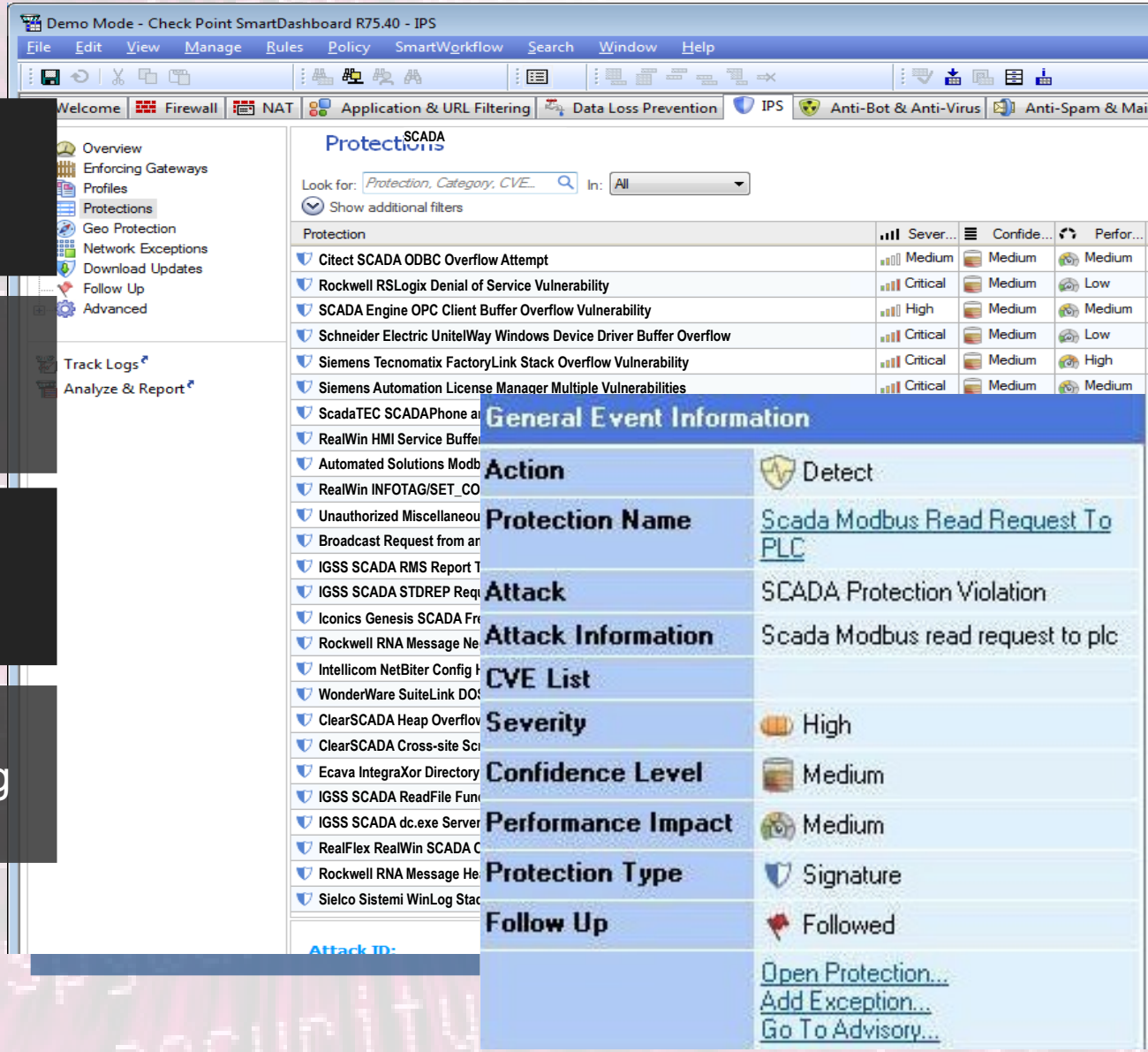
Complete Forensics down to packet captures

SCADA Intrusion Prevention

IBM

Check Point
SOFTWARE TECHNOLOGIES LTD.

- Integrated SCADA IPS signature set
- Built on industry leading IPS Software Blade
- Support for both ICS-specific and corporate IPS requirements
- Full packet capture and integrated event monitoring and analysis



Thank You
- Questions?