IBM Security for Energy and Utilities

BigData Analytics per la sicurezza delle Infrastrutture Critiche

Vincenzo Conti
IBM Security Sales Consultant

Energy and utility organizations are at the forefront of attacks

Utilities are among the most targeted verticals

- Organized cyber-crime, hacktivists, nation-states and exploit researchers

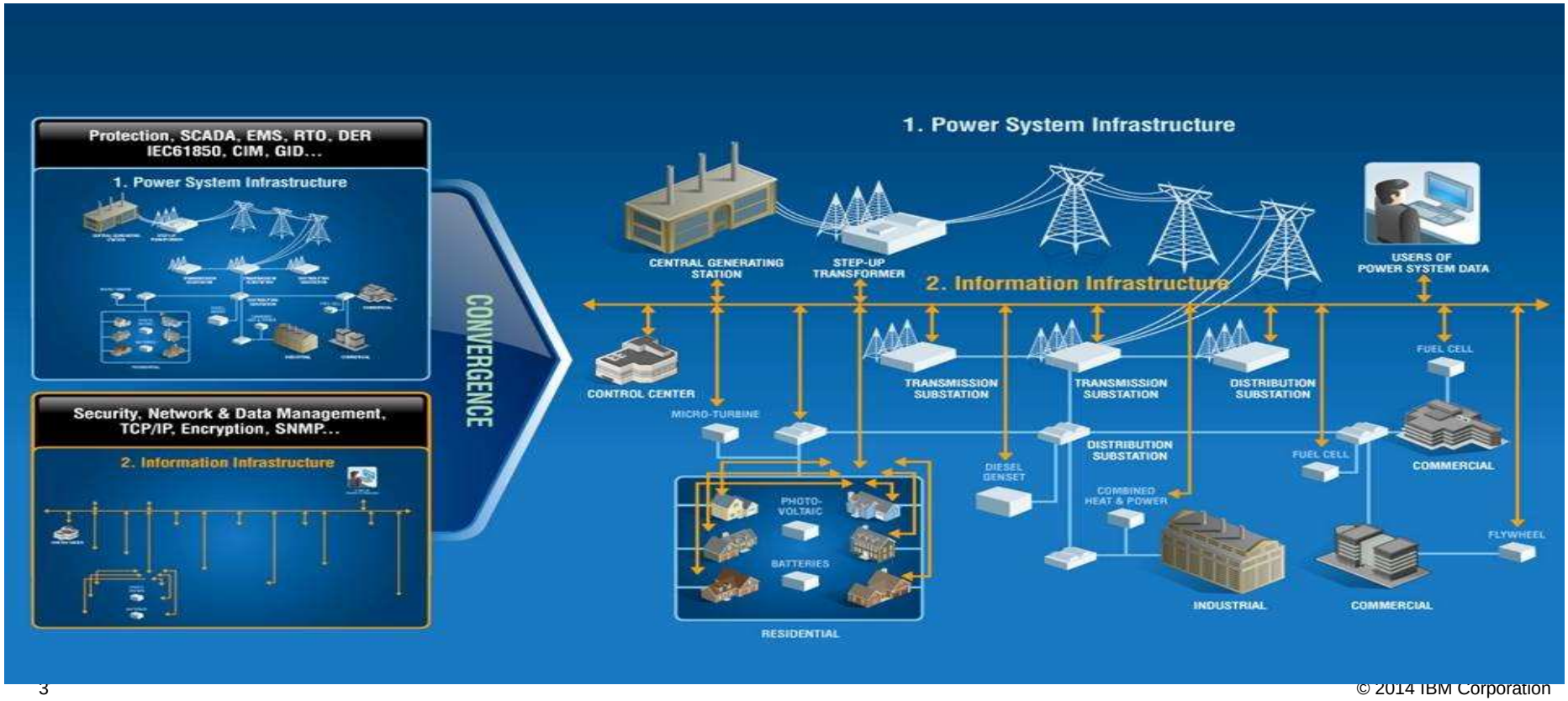
New vulnerabilities are being discovered

- Security testing through injecting invalid, unexpected or random data (fuzzing) have uncovered dozens of vulnerabilities in critical infrastructure systems
- Exploits can be implemented through physical access to networks or through techniques like brute-force password hacking Internet connected devices and phishing

Regulations provide guidance but do not protect against these recent exploits

- NERC CIP focus on IP communications, overlooking the real vulnerabilities that are present
- NIST CSF is process-based and voluntary
- ENISA Smart Grid Security Recommendations
- ENISA Protecting Industrial Control Systems

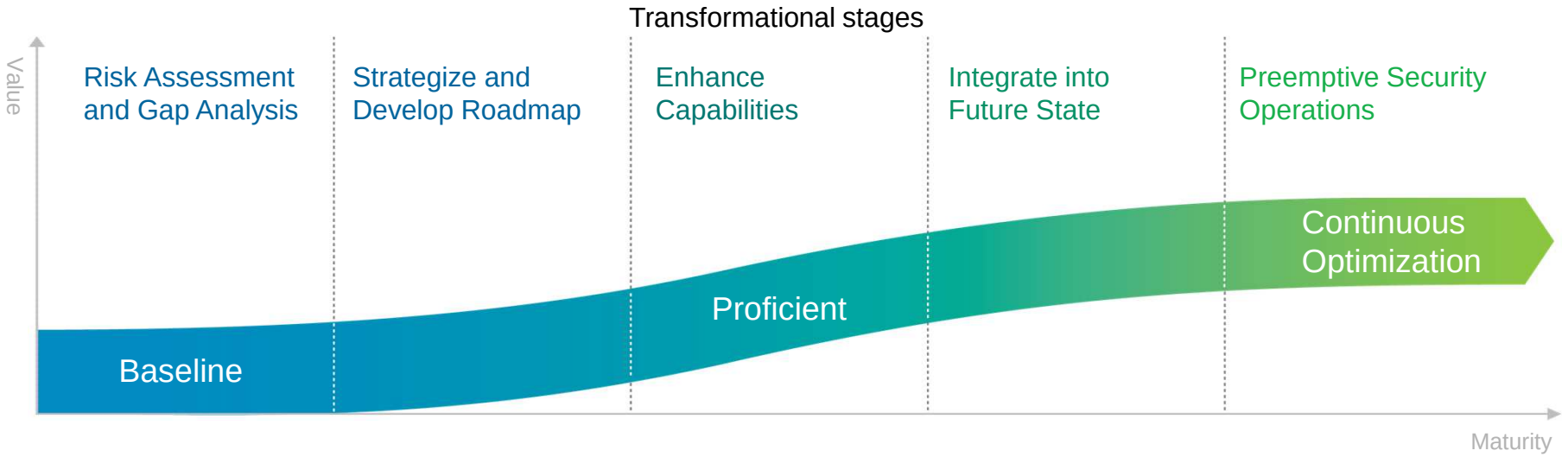
The instrumentation of electric power systems is driving IT and OT convergence, which makes security more complex



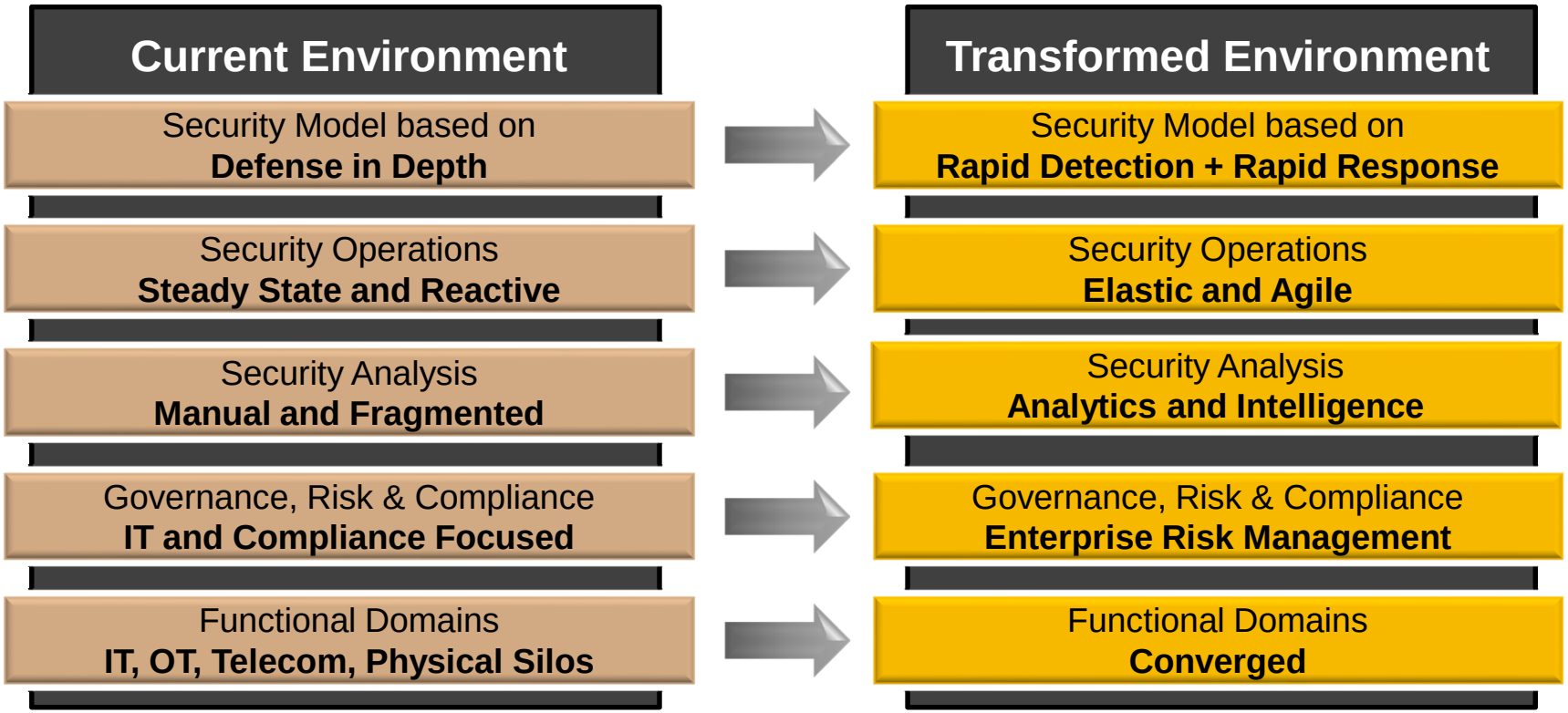
The smarter approach: security transformation based on your business strategy

Business outcomes

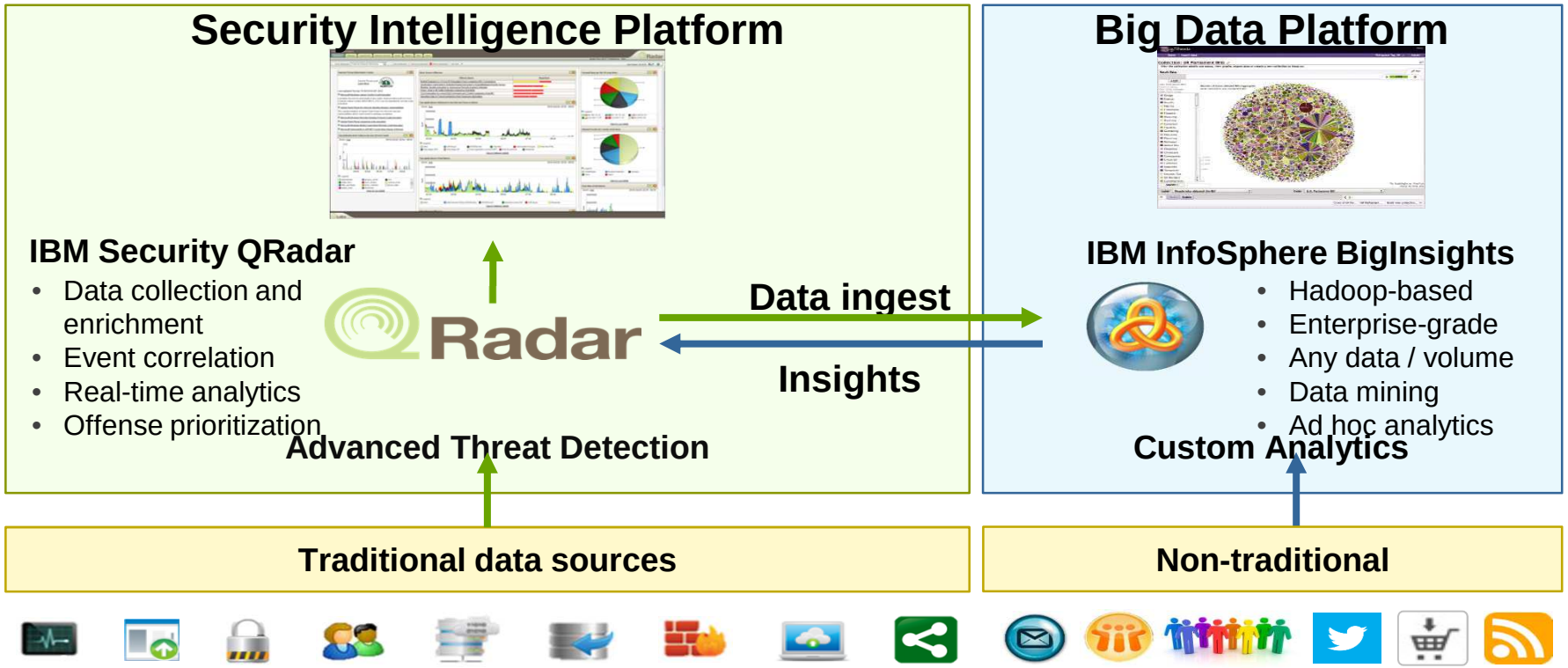
- Prioritized IT budget
- Utilize current architecture “no rip and replace”
- Operations optimized, eliminating unnecessary redundancies
- Incident response plan reduces downtime
- Enhanced situational awareness increases confidence of security and business decisions
- Reduce costs associated with breach



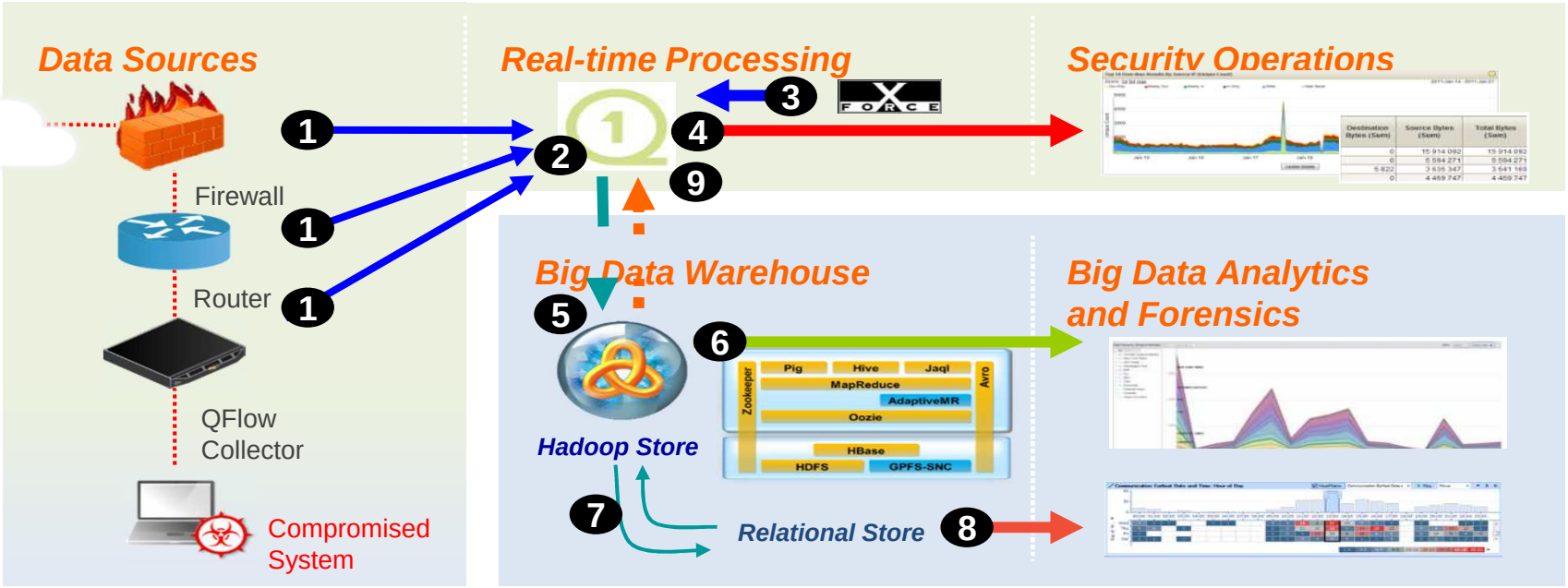
A view of a transformed security environment



How? By integrating QRadar with IBM's Hadoop-based offering



Use case – Detection of an internal compromised system



Requirements

```
Source: Netflow
Sample Size: >100GB /src
Query time: <30sec
Analytics: Time interval
```

IBM Approach

1. Netflow extracted, sent to QRadar
2. Bi-directional flow processing
3. Correlation against external threats
4. Real-time flow analysis to the SOC
5. Enriched flows sent to BigInsights
6. Custom BigSheets queries / analytics
7. Post-processed data storage
8. i2 time-based visuals / analytics
9. Update of QRadar real-time rule sets

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security

www.ibm.com/energy