nes

Networked
Energy
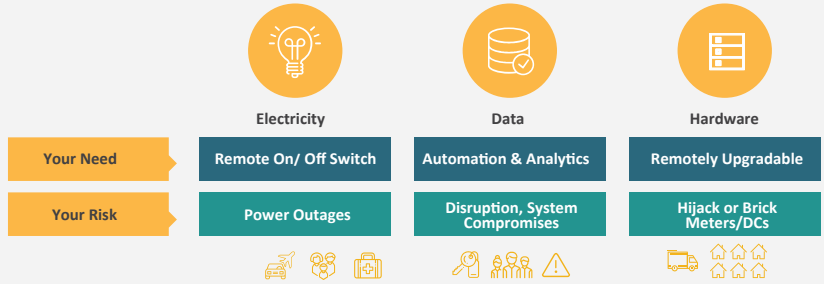Services

Grid Watch

Grid Watch allows you to augment your already robust OSGP smart meter security infrastructure by adding detection and response capabilities to your established protection layers. It allows you to identify changes in the threat-level, adapt your posture accordingly, spot a developing attack, identify points of penetration, quickly initiate responses to blunt the attack and start to offer credible deterrents to the cyber-criminal.
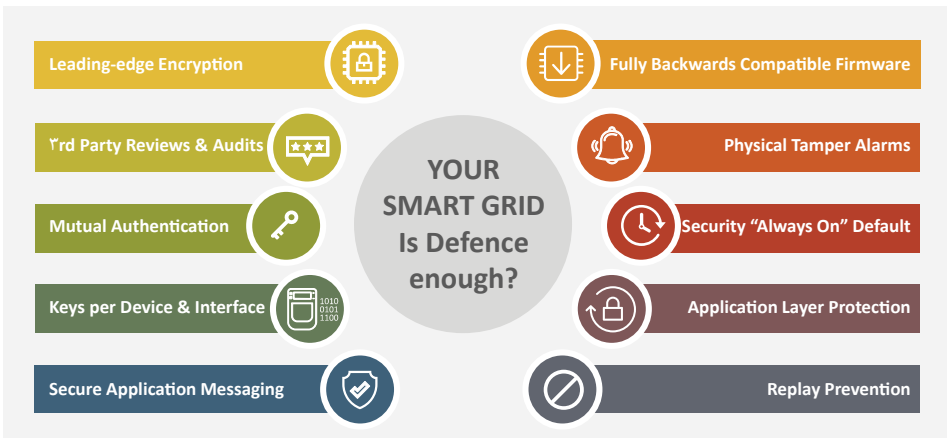
The Tempting Target

Your Smart Grid is your largest investment and a national asset upon which mission critical and life-saving services rely. Government, business and residents rely on the service it provides every second of the day. It provides you with your revenue and through it you have access to highly privileged and sensitive customer information.

The Threat Actors are highly motivated to attack you, and highly ingenious

	Electricity	Data	Hardware
Your Need	Remote On/ Off Switch	Automation & Analytics	Remotely Upgradable
Your Risk	Power Outages	Disruption, System Compromises	Hijack or Brick Meters/DCs

You have to plan as if they will succeed, eventually, one day

Is Defence Enough?

Leading-edge Encryption

Fully Backwards Compatible Firmware

3'rd Party Reviews & Audits

Physical Tamper Alarms

Mutual Authentication

Security "Always On" Default

**YOUR SMART GRID
Is Defence enough?**

Keys per Device & Interface

Application Layer Protection

Secure Application Messaging

Replay Prevention
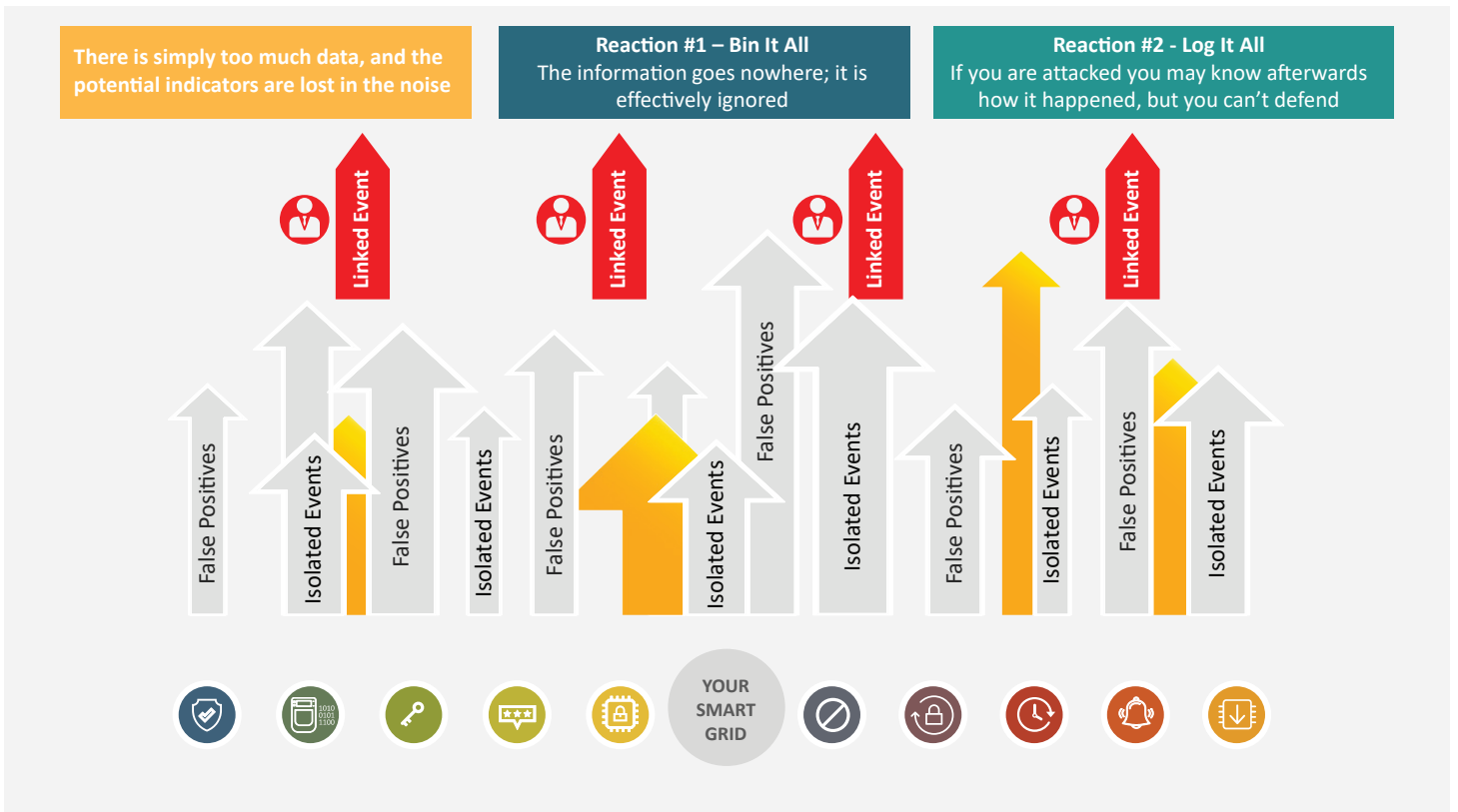
The Information and Communications Technology (ICT) industry has found, to its cost, that relying on defence against cyber criminals based on protection alone is insufficient. The key to modern cyber-security solutions is a combination of defence in depth and the assumption that eventually, protection will be breached. This means that only when detection and response is coupled with protection, is it possible offer a comprehensive defence.
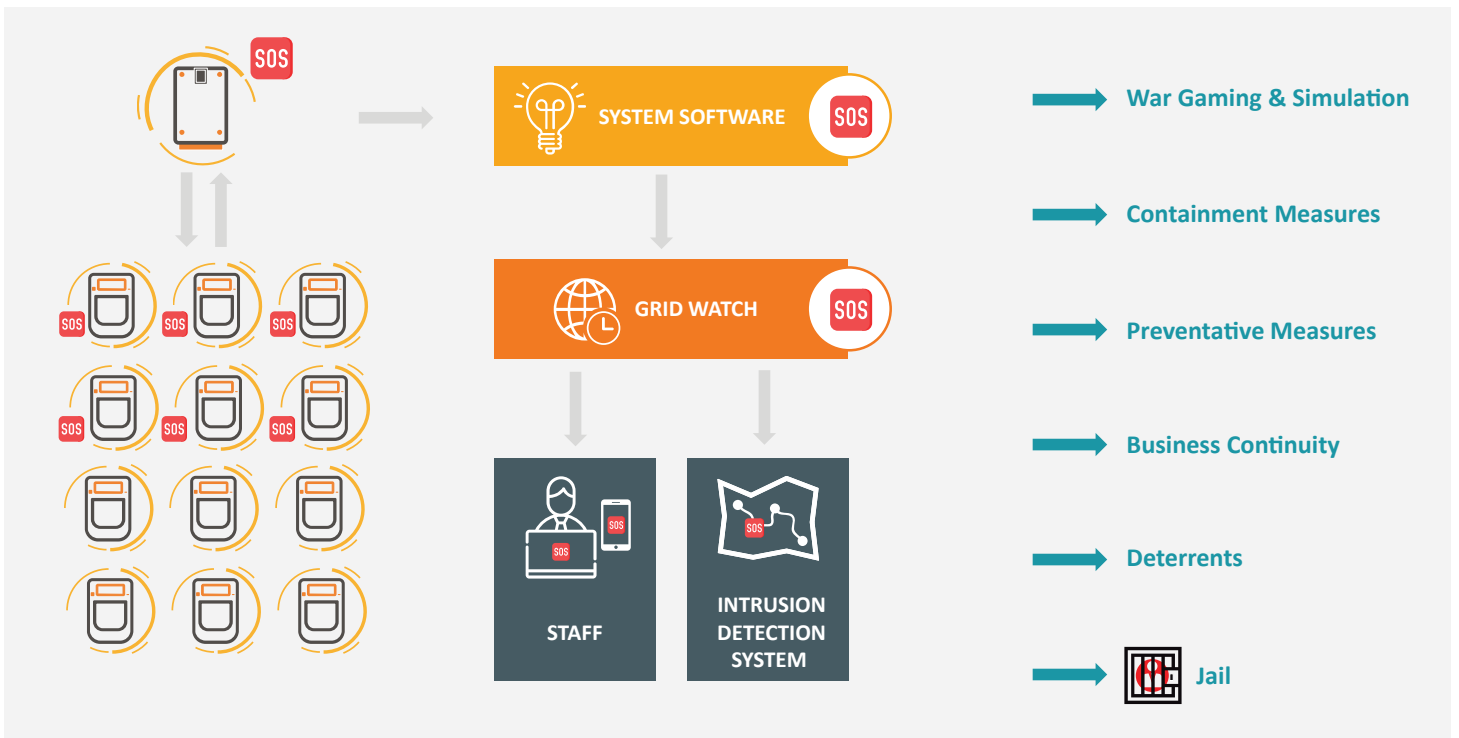
Is Visibility of Security Events Enough?

Even if you are aware of security events, you can be missing important indicators of attack, simply because they are lost in the background of low-level threat indicators and false positives. Common responses are to log everything or log nothing. In either case, you are unable to spot the key indicators which would allow you to adopt a modified security posture in response to a threat or to react to block an attack or limit a penetration.

Linked Event

False Positives · Isolated Events · False Positives · Isolated Events · False Positives · Isolated Events · False Positives · Isolated Events · False Positives · Isolated Events · False Positives · Isolated Events

YOUR SMART GRID

Grid Watch, Threat Detection for the Smart Grid

Grid Watch applies tried and tested security approaches for intrusion detection, as implemented in your ICT IDS platforms, to your smart meters. It intelligently interprets security event information from your OSGP AMI. At its foundation are the security event indications which are provided by every OSGP secured smart meter deployment in the world. It applies sophisticated correlation and pattern matching rules, based on the topology of your network, developed and extended by our own security specialists, to highlight concerted and sustained threat and attack. The result is a highly refined set of threat and attack indicators that you can rely on and respond to. Grid Watch is designed to integrate into your existing Security Information Event Management (SIEM) tooling, and so contribute to your wider corporate IT security standards. Grid Watch also provides report outputs so you can gain in-depth and historic information about the threat-landscape and identify long-term changes which you may otherwise miss.

SOS

SYSTEM SOFTWARE — SOS

GRID WATCH — SOS

STAFF

INTRUSION DETECTION SYSTEM

War Gaming & Simulation

Containment Measures

Preventative Measures

Business Continuity

Deterrents

Jail

Grid Watch integrates seamlessly with your OSGP AMI deployment, without impacting performance or functionality and can be extended to integrate to your wider Smart Grid deployments.