Kelima SEC
consult • design • deliver

*Kelima is a boutique ICT consulting company and KelimaSec is our cyber security division.*

*Our aim is to offer affordable premium quality security consulting to create outstanding business value. We deliver a diverse range of security consulting, design, assessment, and penetration testing services.*

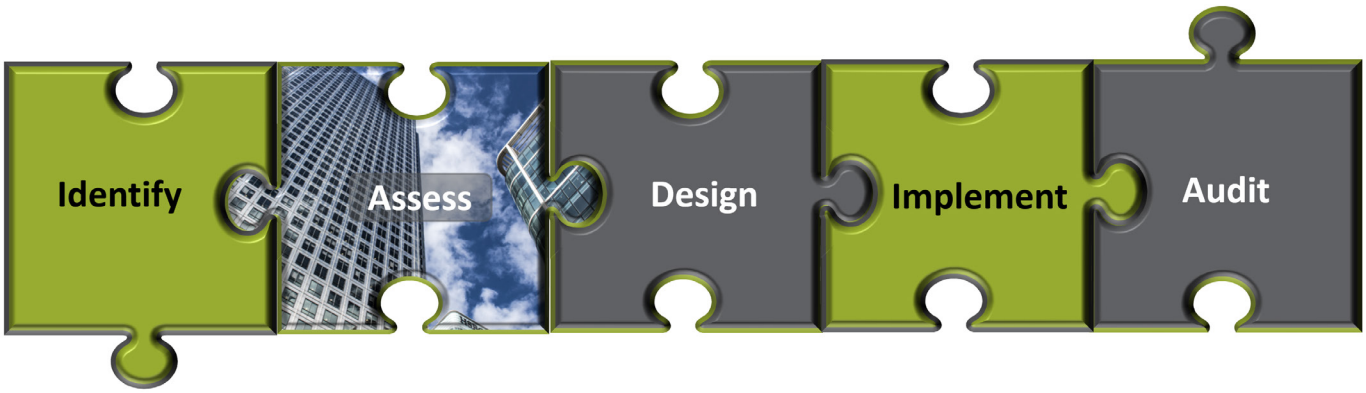
## Our Service

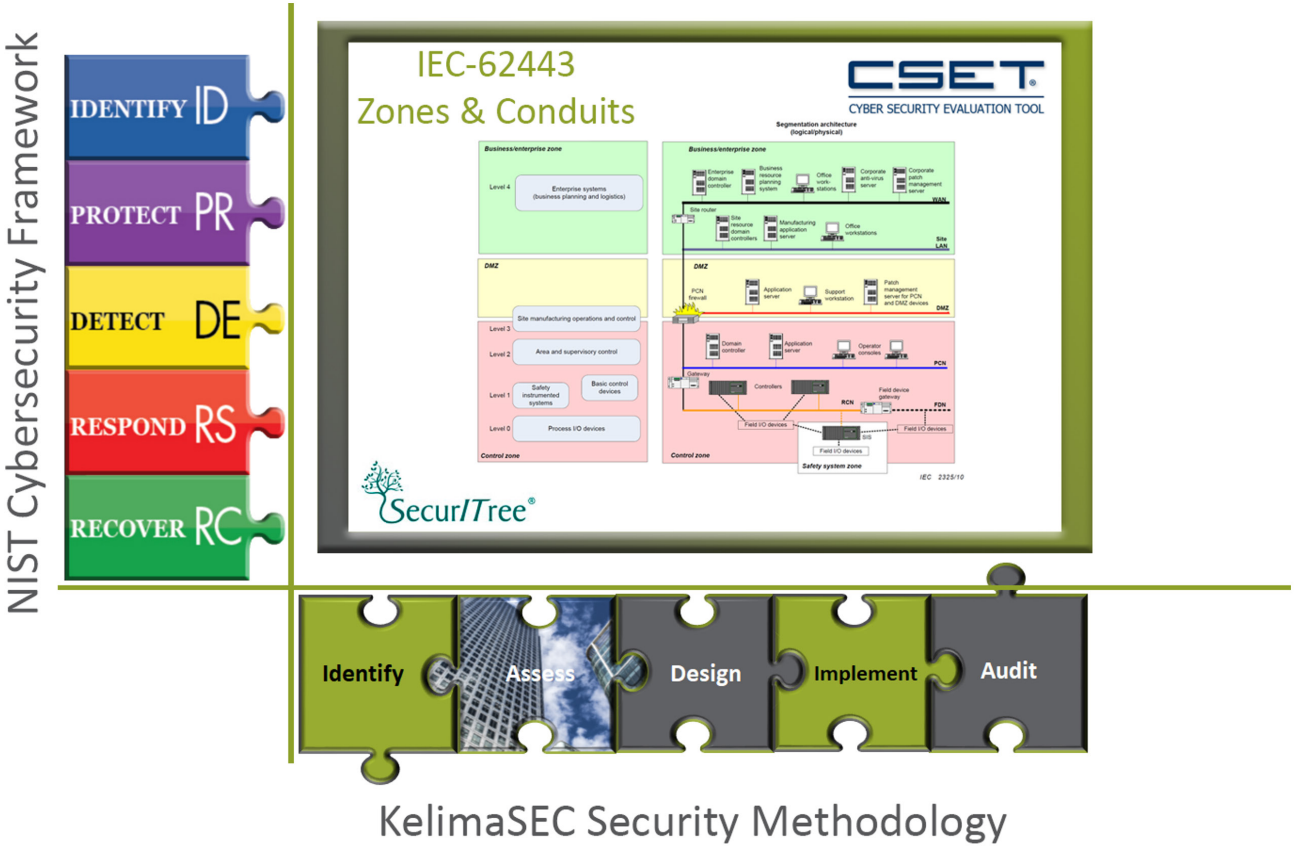
***We focus on providing real-world value to our clients. Our security skills cover the spectrum from C-Level enterprise architecture and risk through to deep technical software and hardware penetration testing. These skills have been honed against high security envrionments within Government and Utility sectors, and practiced through the lens of both client and service provider.***

## Why Kelima?

**Our delivery philosophy is to be honest about what's possible and what's not. One size does not fit all.**

Our experience designing and implementing solutions, and conducting risk assessments and penetration tests, allows us to see security from both the attacker's and defender's perspective. This drives our pragmatic approach. We work closely with our customers to ensure the proposed solution can provide tangible business benefit; and won't proceed if it can't.






KelimaSEC Security Methodology

## Our Core Strengths

- Honest advice. Trusted thought leadership.
- Infrastructure security design and implementation, specialising in Government and Critical Infrastructure providers.
- Assessment of business and technical risk using industry standard or custom risk managment frameworks. KelimaSec utilises 'attack tree' analysis to provide an objective view of the risks, and the mitigating controls that provide the most business value.
- Penetration testing services against application, network, and hardware infrastructure, including smart meters and emerging IoT systems.
- Design, implementation, integration and migration to cloud-based solutions.

| Identify | Assess | Design | Implement | Audit |
|---|---|---|---|---|
| • Development of security policies, standards and procedures<br>• Tailored to the specific requipments of Government and Critical Infrastructure providers | • Business and technical risk assessments<br>• Attack Tree analysis to identify controls that provide real business value<br>• Integration of a risk-based approach into business processes | • Cloud, virtual, and physical security integration<br>• Identity, access, and monitoring solutions<br>• Designed to meet PSPF, NIST, NERC, PCI-DSS and related standards and guidelines | • Waterfall or Agile<br>• On-prem, cloud, or hybrid models<br>• Based on risk analysis for pragmatic tactical and long-term business gain | • Vulnerability and penetration testing services<br>• ISO/IEC 27001 and NIST Cybersecurity Framework assessments<br>• Pre and Post audit assessments and guidance |

*Over the last 10 years, our team's had experience and involvement in a range of security engagements. Some recent examples include:*

## Smart Meter Programs

- Lead security consultancy and thought leadership for Victorian smart meter implementation projects for utility organisations. These projects involved the design and implementation of core security services to support the deployment of meters throughout Victoria.
- As well as design, we conducted detailed hardware penetration testing, to component level, of the smart meters, communications cards, and supporting infrastructure.

## IT / OT Security Strategies

- The design and delivery of strategies for the secure integration of IT and OT systems for a number of Australian water and electricity utilities.
- A business-driven risk-based approach that focused on pragmatic and realistic outcomes.
- The use of industry standard guides and tools including IEC 62443, ISO/IEC 27001/2, the NIST Cybersecurity Framework, and DHS Cyber Security Evaluation Tool (CSET), to drive actionable and auditable change across the organisations.
- A business case and strategic direction for the secure integration of IT and OT functions, while improving the operational visibility and auditability for the business.

## Security Testing and Evaluation

- Penetration testing and evaluation of Home Automation and grid integration IoT devices and associated cloud-based management infrastructure.
- Penetration testing and risk assessment of enterprise-grade virtual hosting and orchestration solutions, including physical and virtual network infrastructure and management and monitoring systems.
- Penetration testing of internal and Internet-facing systems for critical infrastructure providers.
- Penetration testing of SCADA applications including Internet and mobile integration capabilities.