

DEEP INFOSEC / PUBLIC GUIDE

Deep InfoSec — Company & Capabilities

An introduction to the group’s security engineering, proprietary platforms, assurance, industrial programmes and sovereign infrastructure services.

Engineering, security and operating capability — brought together around the outcome your organisation needs.

deepinfosec.com • sales.general@deepinfosec.com

What this means for your organisation

Understand the full portfolio, delivery method and the practical difference between consulting, product evaluation and multi-site implementation.

Security consulting

Effective security consulting has to end in a system that works, not only in a maturity score. Our architects examine identity, networks, cloud, software supply chains and operational responsibilities together. They help teams set priorities, make changes safely, document the new operating model and retain a clear record of accepted residual risk.

DeepShield

A security team should be able to understand what a device is doing on its network and why an intervention is proposed. DeepShield combines network observation, attack-pattern detection, policy-controlled response and event timelines. We start by defining protected assets, traffic paths, safe intervention boundaries and escalation responsibilities. The result is a protection design that operators can assess without losing sight of availability or business impact.

Deep Advisor

Deep Advisor turns dispersed scanner, identity, cloud and endpoint findings into a connected view of exploitable attack paths. Instead of treating every alert as an equally urgent problem, teams can see which combinations reach critical systems, which controls interrupt those paths, and which intervention changes risk most meaningfully. Reports link findings to owners, decisions and supporting evidence for engineers and executives.

Energy & minerals

Energy programmes deliver value only when measurement improves the operation of the network. We connect metering, power quality, asset health, maintenance and investment decisions in a single practical design. A first diagnostic identifies where visibility is weak; a pilot tests the instruments and dashboards; expansion then follows measured value, equipment compatibility and the ability of local teams to maintain the system.

Managed data centres

A managed data-centre service must remain reliable when applications change, links fail and teams rotate. We design hosting, segmentation, access, backup, recovery and operational reporting around the criticality of each workload. Infrastructure supplied for managed services is ISO-certified within the applicable provider scope, while customer ownership, data residency and exit arrangements are built into the architecture.

Workstreams and outputs

Security consulting

Advisory, embedded specialists, implementation sprint or managed improvement programme; integrate Deep Advisor and DeepShield where appropriate.

- CISO and security strategy: target operating models, security governance, board reporting, budgets, policies and a sequenced risk-reduction programme.
- Cloud, identity and DevSecOps: architecture reviews, IAM/SCIM reconciliation, privileged access, Kubernetes, pipelines, application and API security.

What you receive: Security maturity and exposure assessment tied to business services

DeepShield

Appliance or sensor integration; Observe, controlled enforcement and orchestration options depend on approved hardware, topology and scope.

- Network observation: collect approved traffic, DNS, flow and security telemetry from defined links or sensors, correlate suspicious activity and build an event timeline.
- Threat detection: combine signatures, policy, reputation and behavioral indicators to surface phishing, command-and-control, abnormal egress and connected-device anomalies.

What you receive: Protected-asset and network integration map

Deep Advisor

Software platform plus specialist risk engineering; connectors, hosting, data residency and automation permissions are scoped per engagement. AI can assist prioritization without replacing human authorization.

- Unified security evidence: connect approved vulnerability, cloud, Kubernetes, identity, CI/CD and incident sources without replacing existing operational tools.
- Attack-path reasoning: relate exposures, exploitable sequences, compensating controls and critical business services; distinguish observed evidence from modeled assumptions.

What you receive: Source integration and coverage matrix

A practical engagement, from first scope to handover

01 Define the decision

We agree what must change, which systems matter, what the organisation already owns and what constitutes an acceptable outcome.

02 Evaluate on the right perimeter

A scoped assessment or pilot gives engineering teams sufficient information to choose a realistic deployment and acceptance plan.

03 Deliver with evidence

The team delivers designs, implemented controls or services, records decisions, tests outcomes and explains operating responsibilities.

04 Transfer operational capability

Documentation, knowledge transfer, maintenance pathways and follow-up are part of a sustainable programme.

Talk directly to the specialist team

Explore the full offering at deepinfosec.com and select the specialty matching your objectives. Public introductions are freely available; confidential technical and commercial dossiers follow a controlled customer process.

deepinfosec.com · sales.general@deepinfosec.com