pap tecnos

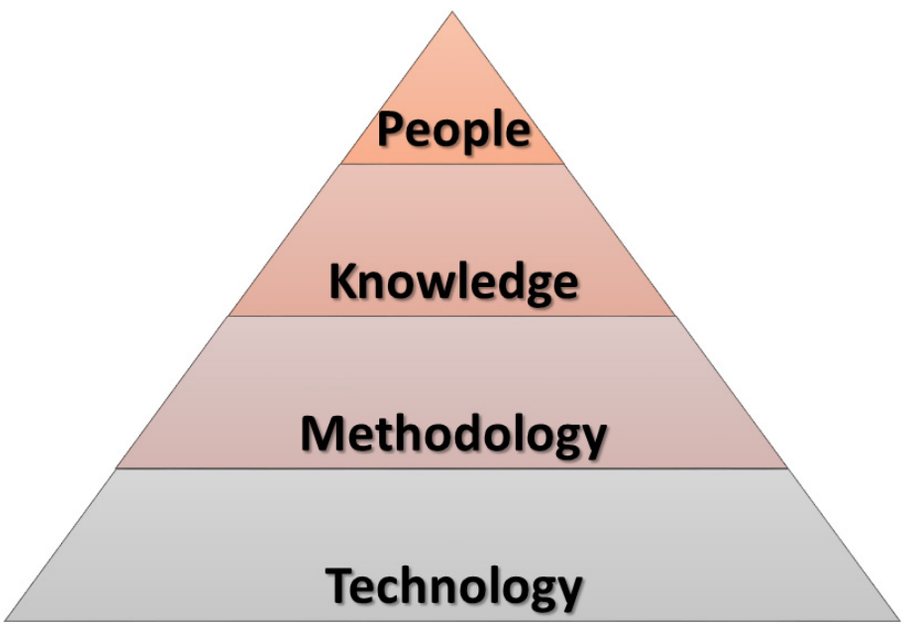
# Research Cyber Defense Center (RCDC)

A Holistic, End-to-End Solution based on PAP's Command Center & Defense Solution - Scales from a Small SOC to a National Level CERT

**From Security to Defense**

## Benefits

- **A state-of-the-art Cyber Defense Command Center**, designed and built by experts in National CERTs
- **Complete End-to-End Solution** that includes: a site survey; risk and vulnerability assessment; definition of cyber defense architecture; implementation of threat research process; incident management tools and processes; selection of cyber security defense tools; simulation capabilities; staff training and support.
- **Organizational Cyber Protection Solution** includes selection, installation, and configuration of best-of-breed cyber security products that precisely fit customer needs, providing maximum efficiency, security and cyber situation awareness.
- **Threat Research and Investigation Solution** that allows tiers 2&3 and cyber researchers a sophisticated platform for investigation processes, supported by a big data-based solution. All information is stored and converted to the STIX data model. Advanced analytic tools are provided for investigation and information sharing within and outside the organization.
- **Mitigation Capabilities** include a definition of processes to mitigate cyber risks, both post-detection and proactively, enabled by advanced incident management tools.
- **Time and Cost Savings** are enabled by management of cyber security through a well-defined process, tailored for each organization, that reduces the number of cyber events, and decreases response time per event, thus saving on costs.

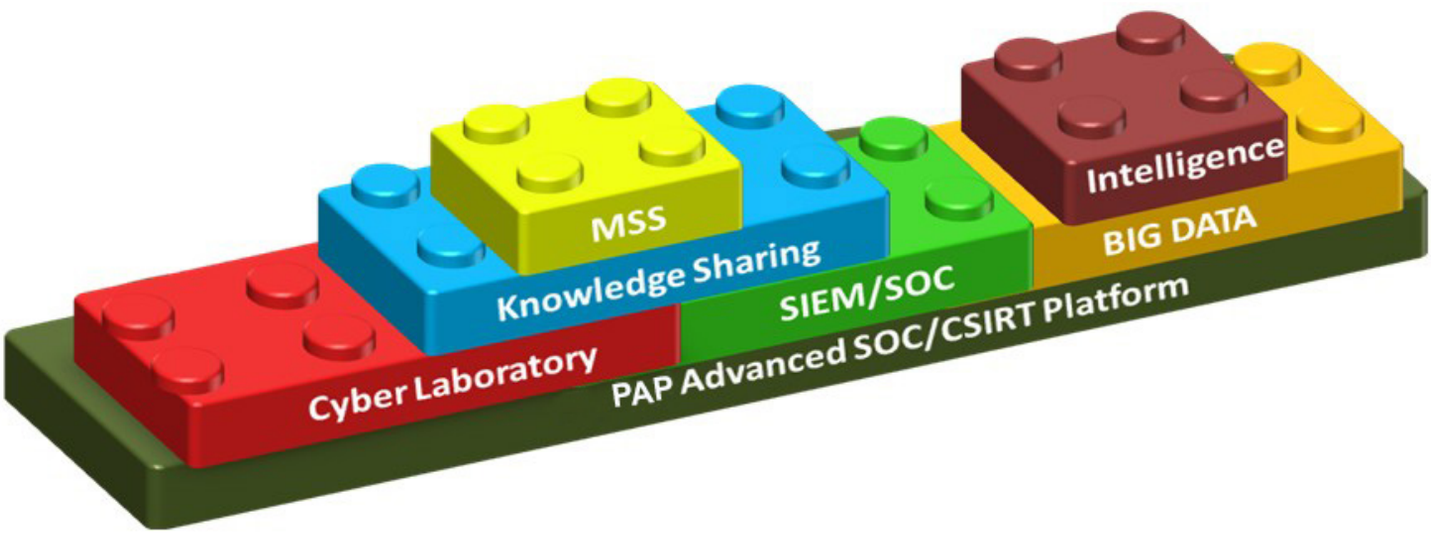


Research Cyber Defense Center is a fully-customized, state-of-the-art cyber defense command center solution, based on a holistic approach covering all aspects of cyber security.  It is built on PAP's extensive experience designing, developing, building and implementing National CERT programs and protecting National level projects.

The solution secures an organization's entire IT network, including all incoming and outgoing communications and computing systems.  It can be implemented by any organization of any type or size, including governments, agencies, corporations, utility companies, critical infrastructures and other facilities.

The solution offers 24*7 cyber incident management, monitoring and analysis of traffic and events; alerting; cyber data aggregation, correlation and investigation; and cyber information-sharing and reporting. This enables fast response and mitigation of cyberattacks.

The solution is built on the following security pillars and building blocks:

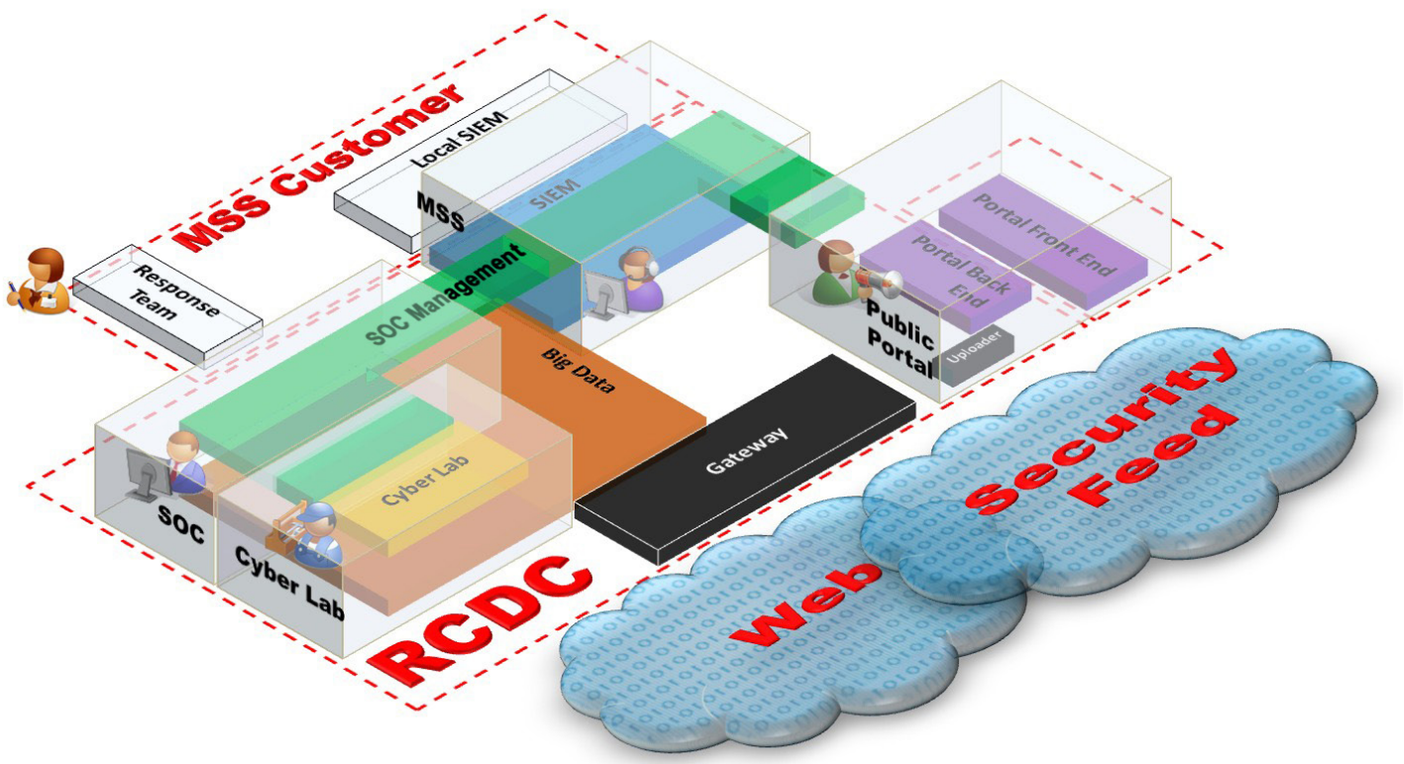



As part of the process, PAP designs a tailored solution for each customer, based on needs and goals. This may include all or part of the Research Cyber Dome Center building blocks. The solution can be implemented from scratch, or can take into account pre-existing systems and processes, and add additional solution layers on top of them to create a complete solution.

## Features

### Main Building Blocks

- **Cyber Protection Solution** – Tools to secure the organization's IT network and systems.
- **Internal & External Cyber Management** – SOC and SIEM tools for managing cyber events either on-site or as a Managed Security Service (MSS).
- **Big Data Repository and Tools** – Repository holding internal and externally collected data, and processing it for intelligence purposes.
- **Incident Response** – Tools for managing incident research and providing remediation.
- **Cyber Lab for Analyzing and Handling Incidents** – Tools and systems for cyber data analysis.
- **External Feeds and Data Sources** – Access to external threat research feeds.
- **External Cyber Management** – Tools and capabilities to manage security of external sites.
- **Cyber Posture** – Full visibility into the organization's cyber posture.
- **Public Portal and Information-Sharing Interfaces** – Enables cyber info-sharing with the public.
- **Operational Procedures and Training** – Customer-tailored procedures and staff training.
- **Operational Management** – Ticket and task management, to control the RCDC operation.
- **IT & Control Room Infrastructure** – Delivery of IT equipment and facilities construction to host RCDC.




PAP provides state-of-the-art technologies, designed and built by its team of top scientists, engineers and cyber experts to counter today's evolving cyber security challenges. The combination of technology and process is a core differentiator of our solution. Rather than simply providing products, we tailor unique customer-specific solutions.

pap tecnos
calle San José Artesano, 8, 28108 Alcobendas (Madrid) - Spain
Tel: + 34 91 6623236 E-mail: rbrown@paptecnos.net