

Research Cyber Defense Center (RCDC)

A holistic end to end solution based on PAP's Command Center From security to defense

Research Cyber Defense Center builds over PAP's extensive experience designing, developing, building and implementing National CERT programs and protecting National level projects.

Research Cyber Defense Center is a state-of-the-art cyber defense command center solution, with a holistic approach covering all aspects of cyber security of the organization. The solution can be granularly customized for each customer's specific characteristics and requirements.

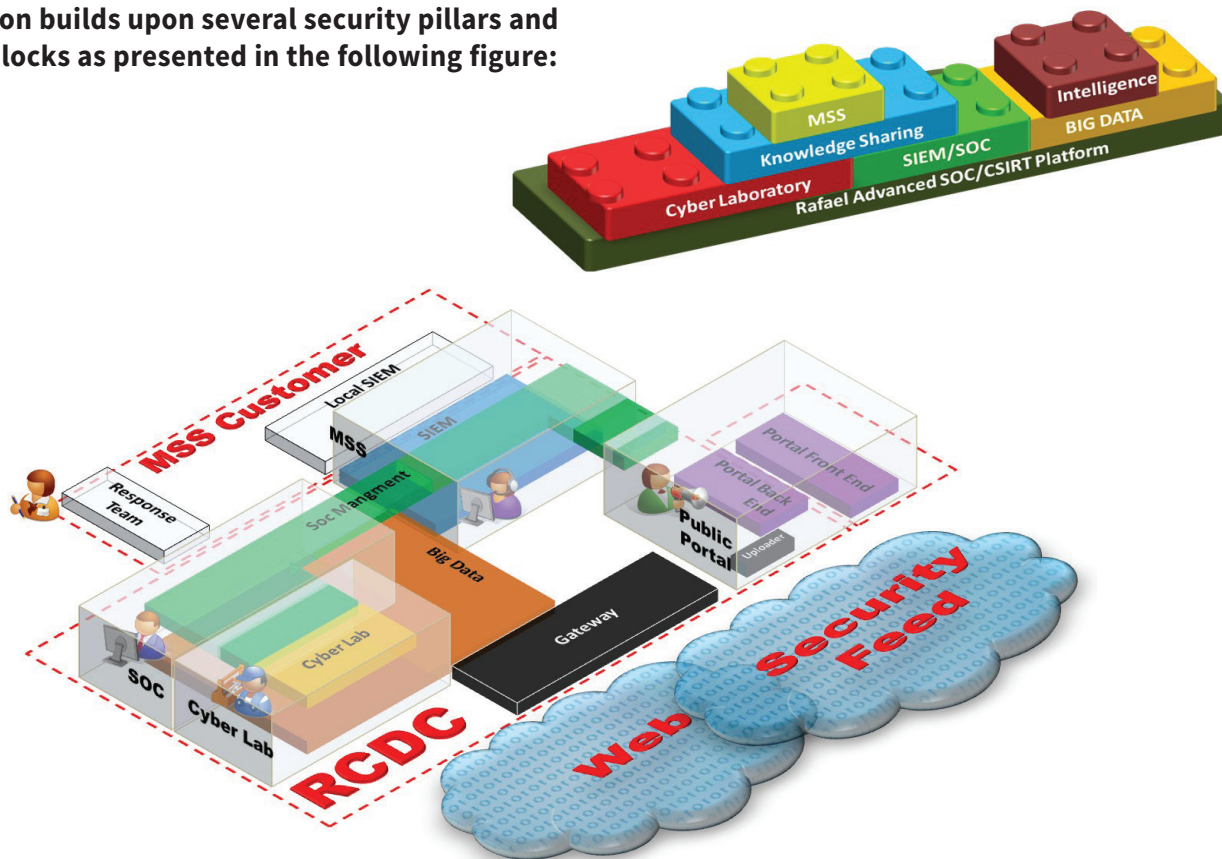
This solution is designed to secure an entire organization's IT network, including all of the incoming and outgoing communications, and computing systems. Any organization type and size can implement this solution, including governments, agencies, corporations, utility companies, critical infrastructures 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, along with Cyber Information Sharing and reporting. This enables cyber analysts and officers to offer fast response and mitigation against cyber attacks.

Benefits

- PAP's cutting edge solution - is a state-of-the-art Cyber Defense Command Center solution from a reputable company, who designed and built National CERTs.
- Complete end-to-end solution – the solution is delivered to the customer as an end-to-end turnkey project, where PAP owns all project phases end-to-end.
- Organizational Cyber Protection solution – PAP has the experience and capability to select, install and configure the market's best of breed cyber security products that fits the exact customer needs.
- Mitigation Capabilities – RCDC mitigates cyber risks, post-detection and proactively.
- Time and Cost Savings – There are no sunk costs on previous investments, with a prioritization and governance plan tailored specifically to each organization's needs.

The solution builds upon several security pillars and building blocks as presented in the following figure:



Main Features

The main building blocks included in PAP's solution are:

- 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 premise or as a Managed Security Service (MSS)
- Big Data Repository and tools – repository which holds internal and externally collected data and processes 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 - enable stakeholders to have full visibility into the organization's cyber posture.
- Public Portal and Information sharing interfaces – for 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 is home to state-of-the-art technologies. We employ the best scientists, engineers and cyber experts, who design and build innovative solutions which are ahead of today's cyber security challenges. The combination of technology and process is a core differentiator of our solution. Rather than simply providing product solutions, we tailor products into customer specific custom processes, which creates a unique solution per customer.