SOC Services
Locuz’ IT Security Lifecycle services combine people, processes and technologies to provide secure access to business applications, over any network and from any device.

Our security operations help with 24/7 Security and threat intelligence management for enterprises. Our Security experts help prevent breaches, mitigate risk and ensure regulatory compliance.
The world today is comprised of two types of organizations: those who have been breached, and those who do not yet know that they’ve been breached. The difference between these types of organizations is related to how soon the company can detect a breach and how effectively they can respond. Detecting and protecting information systems from today’s advanced, constant threats requires a comprehensive understanding of how different information security silos relate to each other. By deploying IT security analytics solution, you can detect the attacks as fast as possible, they can block or stop such attacks and provide in detail information to re-build an attack.

With a focus on responding to, and containing threats, it is possible to define a Security Operation Center in simple terms: the technology and processes used to detect breaches and coordinate the appropriate response. An effective Security Operation Center provides the information necessary for organizations to efficiently detect threats and subsequently contain them. While eliminating the threats we face is an impossible goal, reducing the time it takes to respond and contain them is certainly achievable.

Locuz Security Operations Center provides you with an analysis on possibilities of security risks to your network, firewalls, servers and applications. Outsource your security operations, and we can help you with 24x7 staffed monitoring and management services. Our experts help you manage your risk, reduce costs, and ensure regulatory compliance.

One of the Leading General Insurance Companies in India, trusts us for continuously monitoring & managing their Security Incidents & Events. We enable them to detect, respond and prevent threats which has considerably enhanced their Security Posture while gaining operational visibility, investigative capabilities and achieve compliance to meet IRDA Regulations.
SOC - Framework

This framework delivers advanced threat analysis, comprehensive information security reporting, and an intelligent security search. By utilizing a broad range of information — logs and other events generated by hosts, devices, applications and databases, network flow data, known vulnerabilities, and more, it provides deep visibility and analytics to address the most demanding security and compliance requirements.

Key Benefits

- Implement and measure critical Security controls
- Reduce information security complexity
- Assist with compliance needs around PCI-DSS, HIPAA etc.
- Gain advanced security intelligence
- Discover and eliminate today’s advanced threats
- Continuous monitoring of security events
- Lower the total cost of ownership (TCO) for information security
The Key functional components of SOC

Tools & Technology

- Security Analytics Platform
- Proactive Monitoring – Automated Monitoring, Monitored object reporting, Integrated to Business Processes and 24x7 Monitoring
- Alert and Notification – Security Incident Incident Reporting, Alerts Categorized based on Risk Level and Notifications to Business Process Owners
- Events Correlation – Contextual Correlation of events, Situational Awareness and Mapped to Business Processes

Risk Management

- Incident Management – Investigation and Analysis, Evidence Gathering, Escalation Management and Forensics
- Behavioral Analysis – Detection, Anomaly Detection and Network Behavioral Analysis
- Reporting – Periodic Incident / Event Reporting, Trend Analysis Reporting, Feedback and Review Mechanism

Automation

- Compliance and Audit – Compliance Templates, Compliance Enforcement, Compliance Violation Reporting and Review of Compliance Policies periodically
- Change Management – Change Management processes, Automated Approval Processes and Change Control Validation
- Configuration Management – Configuration Management Database, Configuration Logs, Archivials, Mapped to Change Control and Configuration Rollback

Risk Ranking – Risk Management Framework, Categories Alerts, Notifications and Compliance based on Risk level and Risk Review
- Vulnerability Management – Periodic Vulnerability Assessment and Audit, Alert and Notify the Business Process Owners for action to close the Vulnerabilities and Validate Remedial Action Completion
Spectrum of Service Deliverables

**Monitoring & Log Analysis**
- Device and App/DB Monitoring
- Real time Event Analysis, Correlation and Alerting
- Creation and adding custom correlation rules
- Remedial Action
- Risk & Threat Management and Prevent recurrences

**Emergency Response**
- Team comprising of Cyber Security Experts, Security Specialists & CEH
- Investigation, response & mitigation of all Critical or Severity 1 Incidents
- Connect with law enforcement agencies

**VA / PT / App Security Testing**
- Determine what security vulnerabilities exist and plan mitigation/vfx
- Tracking the new vulnerabilities from various resources such as CERT
- OS/DB Hardening
- Grey Box Testing
- Black Box Testing

**Security Intelligence**
- Track and advise new global security threats and vulnerabilities
- Impact & Risk Analysis of New Vulnerabilities and Threats
- Security Analytics
- Intelligent Security Search
- Build sophisticated machine learning models

**Forensic**
- Real-time Forensics Operationalized
- Flexible, Scalable Security Investigations
- Fraud investigation
- Effective remedial solution of intricacies related to Forensic Investigation of crime of any type

**ISMS / ISO / Compliance**
- Carry out ISMS/ISO extension activities such as, Gap Analysis, Risk Assessment & Treatment, Policy and Procedure Formation, & Awareness
- Internal Security Audits
- Compliance Automation & Reporting
- Prepare Reports
- Security Awareness trainings

**SOC Operations**
- Define Critical & Key SLA’s
- Creation of CAB and effectively manage Change Requests
- Process Checklists and run books
- Develop & recommend improvement plans
- Monthly Review and daily/weekly / monthly reports
Meet the Team

- **Risk Mgmt Committee**
  - ITIL Certified
  - Manages resources to include personnel, budget, shift scheduling and technology strategy to meet SLAs;
  - Communicates with management
  - Serves as organizational point person for business-critical incidents
  - provides overall direction for the SOC and input to the overall security strategy.

- **SOC Manager**
  - Subject matter Experts have vast knowledge and experience with network threats, their detection and mitigation, and in-depth experience
  - provides expert security assistance
  - Take immediate corrective action to restore services and attack mitigation
  - Handling Major (High Priority) Incidents and escalations

- **Threat Intelligence & Vulnerability Mgmt**
  - Subject matter Experts have vast knowledge and experience with network threats, their detection and mitigation, and in-depth experience
  - Expert of Security, OS, Network, Web technology, Database
  - Configure tools and security technologies
  - Implement security policies in technologies under SOC
  - Quick at Incident response
  - Interact and drive vendors, OEM, Government bodies
  - Handles Day to day operations of the Device Administrations
  - Configuration Management as per the change request policies
  - Device Configuration Backups

- **Emergency Response Team**
  - Expert of Security Technology and process
  - Understand attacks and threat matrix
  - Extremely good at reaching to root cause
  - Think out of box
  - Understand Virus, Trojans, backdoor, malicious code
  - Performs deep-dive incident analysis by correlating data from various sources
  - Determines if a critical system or data set has been impacted
  - Advises on remediation
  - Provides support for new analytic methods for detecting threats.

- **Incident Response & Forensics Team**
  - Continuously monitors the alert queue
  - Triages security alerts
  - Monitors health of security sensors and Network Elements
  - Collects data and context necessary to initiate Investigate and Analysis work.

- **Security Monitoring**
  - Impact and Risk Assessment of Incidents
  - Manages Risk, Compliance and Governance
  - Alignment of Risk Management with Business Needs
  - Qualified Risk Ranking

- **Security Management Team**
  - Network Scanning
  - Vulnerability Scanning
  - Situational Awareness
  - Security Consulting
  - Ethical Hacking
  - Gap Analysis
  - Develop intelligence from their past incidents and from information-sharing sources, such as a specialized threat intelligence vendor, industry partners, the cybercrimes division of law enforcement, information-sharing organizations

- **Meet the Team**
  - ITIL Certified
  - Manages resources to include personnel, budget, shift scheduling and technology strategy to meet SLAs;
  - Communicates with management
  - Serves as organizational point person for business-critical incidents
  - provides overall direction for the SOC and input to the overall security strategy.

- **Subject matter Experts**
  - have vast knowledge and experience with network threats, their detection and mitigation, and in-depth experience
  - provides expert security assistance
  - Take immediate corrective action to restore services and attack mitigation
  - Handling Major (High Priority) Incidents and escalations

- **Security Management Team**
  - Expert of Security Technology and process
  - Understand attacks and threat matrix
  - Extremely good at reaching to root cause
  - Think out of box
  - Understand Virus, Trojans, backdoor, malicious code
  - Performs deep-dive incident analysis by correlating data from various sources
  - Determines if a critical system or data set has been impacted
  - Advises on remediation
  - Provides support for new analytic methods for detecting threats.
Facts-at-a-glance

Certifications

Technology Alliances

Service Assurance

- Cert-In Empaneled Auditor in India
- Life cycle Approach - Security consulting/audit, deployment & managed services
- GRC assurance – 74% of compliance reported on one of our largest IAM deployments
- Field Tested methodologies - Standard and proven framework
- Domain Knowledge, Focus on Cloud Security & Mobility, Best in Class Resources
- Industry Experience – Large Security Services contracts with several Financial Services firms, Healthcare & Life Science firms and Federal Agencies
- The team supports and monitors over 10,000 devices and Apps/DB, both physical and virtual, deployed at customer premises and service provider facilities
- Flexible Engagement Models - On Premise, Cloud based (Shared) and Hybrid
Dashboards

Work flow (Event Management)
About Locuz

Locuz is an IT Infrastructure Solutions and Services company focused on helping enterprises transform their businesses thru innovative and optimal use of technology. Our strong team of specialists, help address the challenge of deploying & managing complex IT Infrastructure in the face of rapid technological change.

Apart from providing a wide range of advisory, implementation & managed IT services, Locuz has built innovative platforms in the area of Hybrid Cloud Orchestration, High Performance Computing & Software Asset Analytics. These products have been successfully deployed in leading enterprises and we are helping customers extract greater RoI from their IT Infrastructure assets & investments.