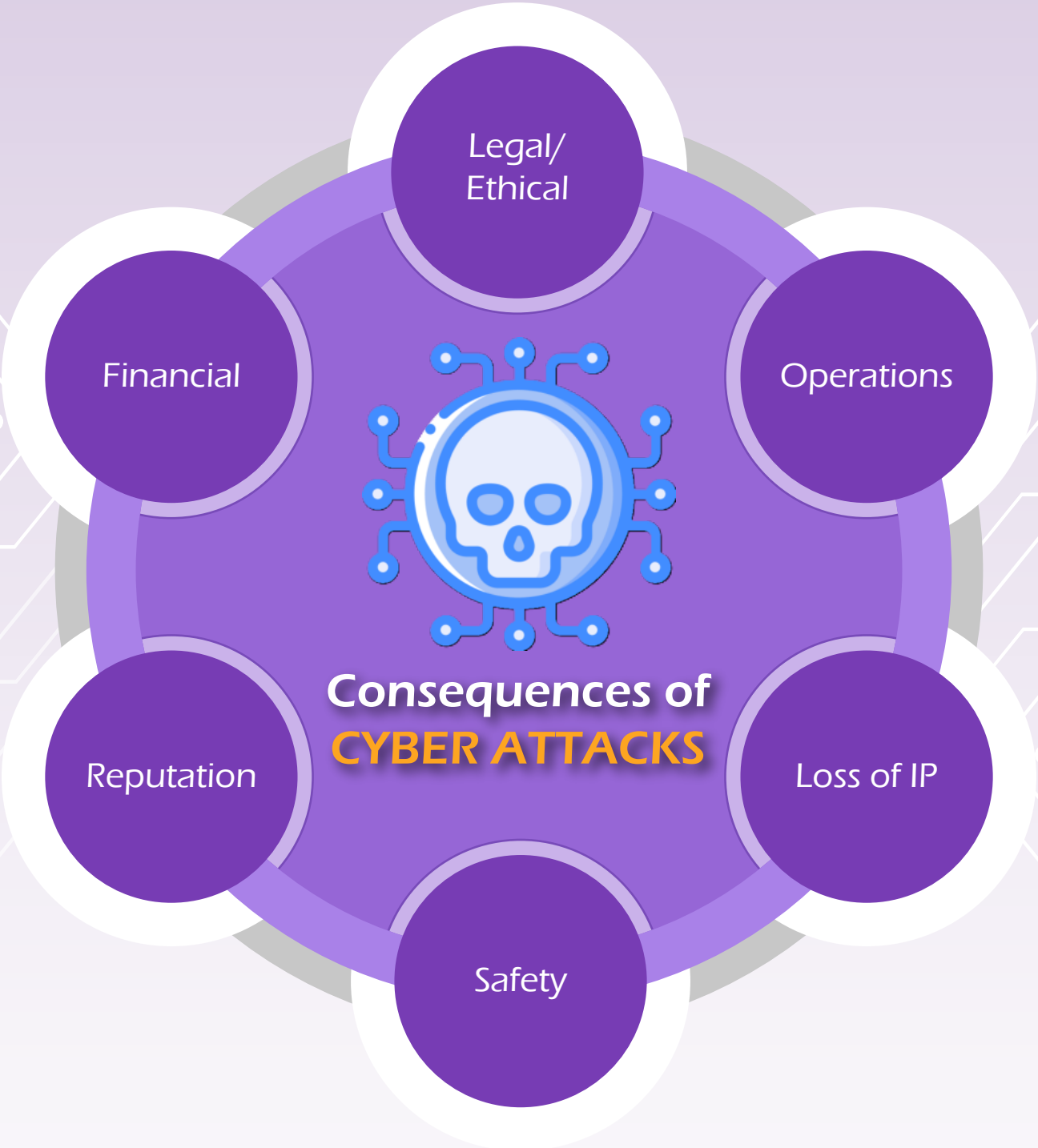
Enterprise Threat, Incident & Compliance Management Services

info@johnkeellsit.com +94.11.2318319 www.johnkeellsit.com

JOHN KEELLS
disruptive minds


Legal/
Ethical
Financial
Operations
Consequences of
CYBER ATTACKS
Reputation
Loss of IP
Safety

OUR APPROACH

More than just SIEM

Our holistic approach to fulfill your cyber security requirements comes from a unique UTP (Unified Threat Platform) that modernizes compliance management. It extends to your entire digital framework - inclusive of identities, endpoints, network, data, applications, and infrastructure. Our Zero Trust architecture serves as a comprehensive end-to-end strategy, providing integration across all elements in the SIEM solution.

1 Discovery and Adaptation (Workshops/Consultation)

- Engagement
- Advisory consultation
- Requirements gathering

2 360 Security Assessment

- Security workshops
- Gap analysis

3 Maturity Model

- Architect/Innovate
- WBS plan
- Integration
- Budgeting
- Interoperability
- Quick wins and long-term plans
- Blueprint and report

4 Adopt (Execution)

- Deployment
- Configuration
- Best Practices
- Process improvements

5 Govern

- Business commitment
- Management baseline
- Advance operation
- Design principle/policy
- Threat intelligence
- Visibility and analytics
- SOAR and deployment

6 Manage

- Threat intelligence
- Visibility and analytics
- SOAR and deployment

OUR SOLUTION

COLLECT
Integrating the threat intelligence feed

CORELATE & ANALYTICS
Integrating the threat intelligence feed

VISUALIZE
Event data visualization and compliance monitoring & management

AUTOMATE & ORCHESTRATE
Automated workflow remediation in response to incidents with the use of automation rules and playbooks

AI AND ML
Use statistical and machine learning-based techniques to identify patterns between event information and behaviour trends

HUNT FOR THREATS
Proactively hunt for undetected threats using threat hunting queries and notebooks.

RETAIN
Policy configuration as per the business requirements.

OUR SOLUTIONS

Unified Threat Protection

Foundation

- Workload health monitoring
- Secure connectivity
- Score and recommendations
- Resource monitoring, resource logs and diagnostics
- Safe attachments and safe links
- Anti-phishing policies
- Collaborative tools protection
- Real-time reports
- Report message add-In
- Advanced protection for internal mail
- Attack surface reduction
- Next-generation protection
- Secure connect to workload

Advanced

- Compliance management
- Vulnerability assessment and exploit protection
- Hardening cloud resources
- Insights and customs alerts
- System integrity assurance
- Manage patch and vulnerability with periodical assessments
- Immediate and automatic vulnerability patching
- Protection of web applications
- Cloud apps discovery
- Network monitoring and threat protection
- Identify applications with cloud discovery
- Provide capabilities from automated responses
- Endpoint detection and response capabilities

*Includes Foundation solution

Enterprise

- Firewall management
- Application protection
- Network threat detection
- Session controls for applications
- Sanction and unsanctioned applications
- Information protection and shadow IT
- File monitoring
- Awareness and simulation campaigns
- Search device and event data
- Create custom incidents
- Evaluation labs

* Includes Foundation and Advanced solution

Compliance Management

Foundation

- MS native log sources configuration
- Data retention within SIEM
- Default analytic rules configuration
- Default dashboards configuration
- User entity behaviour configuration

Advanced

- Third party log sources integration
- Custom data retention configuration
- Custom analytics rules configuration
- Custom dashboards configuration
- Automation rules configuration
- Default playbooks configuration
- Default hunting rules configuration

*Includes Foundation solution

Enterprise

- Threat intelligence data feed integration
- Customized playbooks configuration
- Customized hunting rules configuration
- Anomaly rules configuration
- Jupyter notebooks configuration
- Watchlists configuration

*Includes Foundation and Advanced solution