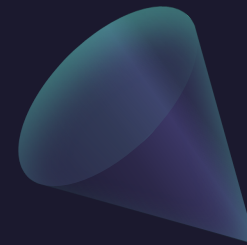
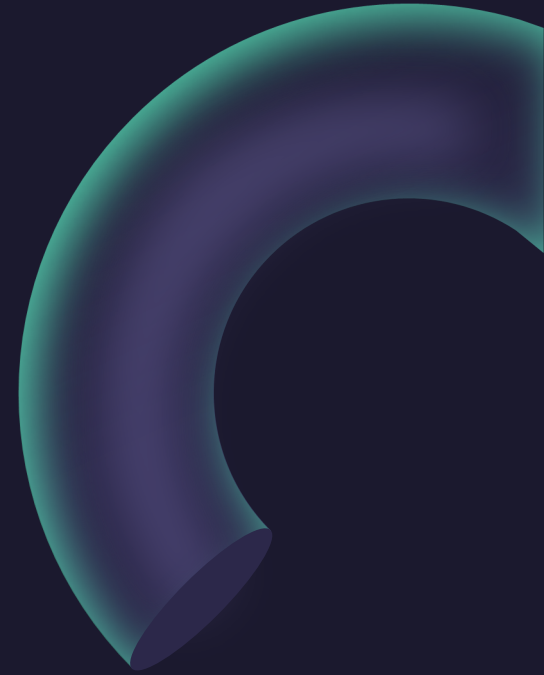


Cybersecurity.

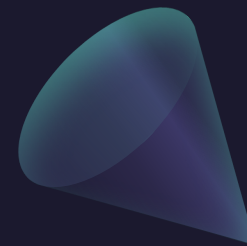
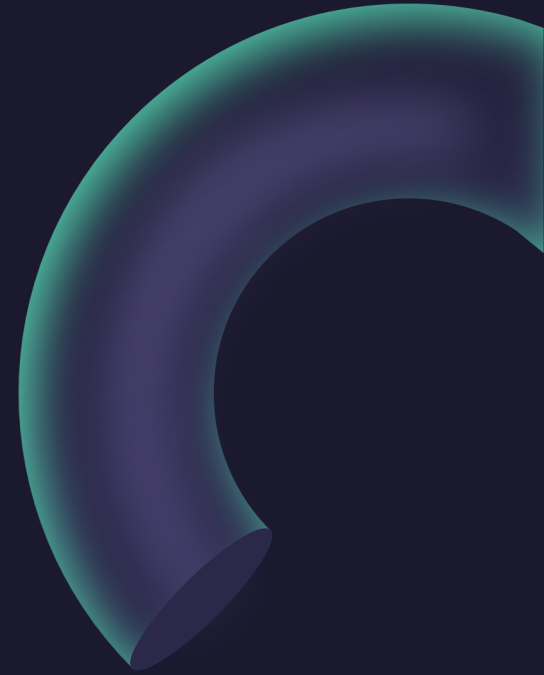
Security services

- Security operation center(SOC)
- Network operation center(NOC)
- Endpoint Detection and Response(EDR)
- Vulnerability Assessment and Penetration Testing(VAPT)
- IT Security Audit Services
- Email Security
- Web Security
- Security compliance consulting services(PCI, SOX, GLBA, HIPAA, FISMA, ISO 27001..etc)
- Data Activity Monitoring(DAM)
- Web application firewall(WAF)



SOC-Consulting Services

- Creating security architecture design from scratch needed for the entire IT environment
- Creating a roadmap and successfully implementing entire security architecture
- After implementing, if needed will provide 24/7 full-on SOC support to maintain security spectrum
- SOC team will monitor entire environment 24*7 to prevent security attacks and provide timely security reports and audits
- Maintain security standards to meet the compliance regulations like HIPAA, PCI DSS...etc.
- Secure entire environment comprised of user, server, database and applications from undiscovered attack, data theft , social engineering using various up to-date security technologies and prevent operational crash or stoppage, smooth running of day-today business.



SIEM

- It's a security management system that combines security information management (SIM) and security event management (SEM). SIEM tools collect data from various sources including log data, security alerts, and events, and centralize it into a platform for real-time analysis.
- This solution collect and aggregate logs in a central location, separate from the host that created them. As a result, in the event of a compromise or hardware failure or internal threat, your logs are still intact and in tamper-free state.
- This helps advanced visibility both on-premises and cloud, maintain log history , produce regular security reports for auditors and meet compliance regulations such as HIPAA, CMMC, NIST, FFIEC, PCI DSS, etc.



Benefits

Real-time threat recognition and response

Centralized security management and reduce visibility gaps

Ease compliance auditing and reporting

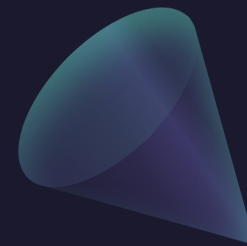
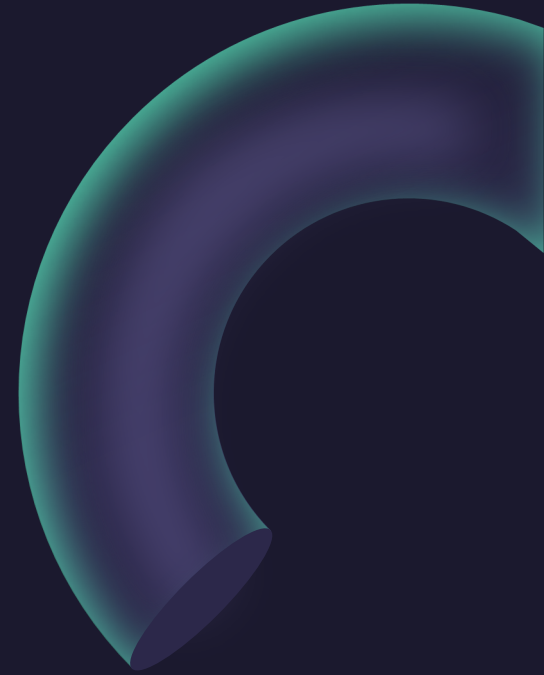
A central view of users, applications, servers and devices

Reduce manual tasks with automation and improve analyst experience



SOAR

- SOAR stands for security orchestration, automation, and response which incorporates automated responses to security events created by security analyst
- Modern-day security strategies demand faster and hassle-free security-centric automation, SOAR don't demand coding capabilities rather eases analyst to create automated workflow just by enabling playbook.
- The EDR sends an alert to the SOAR, which triggers the SOAR to execute a predefined playbook. It validates the alert with data from integrated threat intelligence feeds and other security tools. Then, the SOAR executes automated responses, such as triggering a network detection and response (NDR) tool to quarantine the endpoint or prompting antivirus software to find and detonate malware.
- With the SOAR platform, organizations can reduce the manual burden and operational cost as it enables the centralized integration of a variety of tools required for reporting, playbook creation, alert handling, analyst training, and several other aspects.






TESTING

- Application security review and testing
- Application security training and source code security
- Application source code reviews
- Card data discovery
- External vulnerability (asv) scans
- Firewall security review services
- Internal vulnerability scanning services
- Internal vulnerability scanning services
- Security event logging and monitoring services
- Application and network level penetration testing

DATA ACTIVITY MONITORING



- Database Security solutions secure sensitive data stored in databases. DAM technologies provides full visibility into data usage, vulnerabilities, and access rights. It enables security, audit, and risk professionals to improve data security and meet compliance mandates.
 - All database activity, including administrator activity and select query transactions, will be monitored, and audited independently.
 - Alert or block database attacks and abnormal access requests, in real time
 - DAM technologies employ real-time security technology to independently track and examine “database users” actions without depending on DBMS audits or logs. In a nutshell, keeps track of and audits what users do with their access or how and by whom data is accessed, including the administrator.
- 

Thank you

