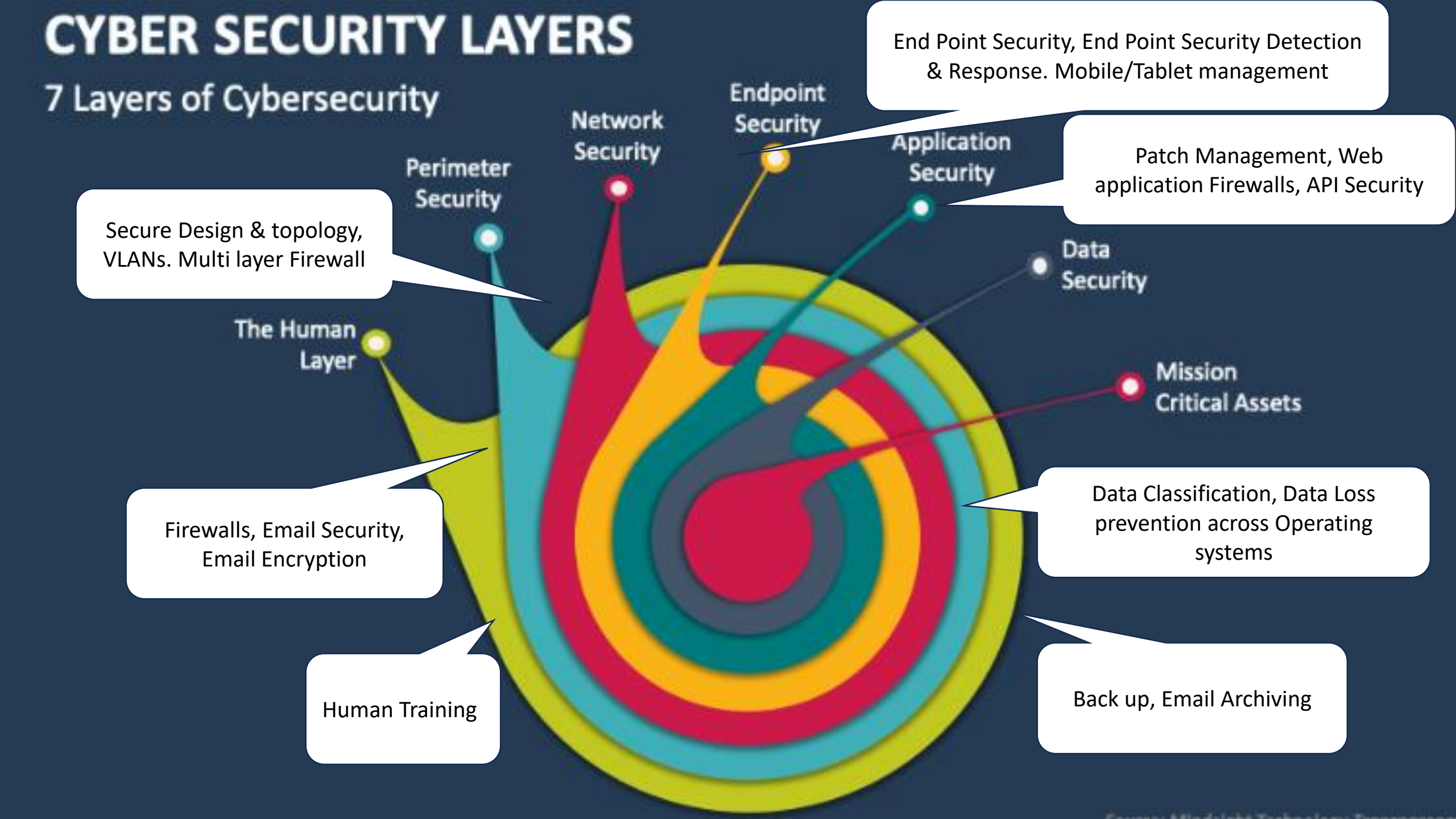


Introducing
Cyber Security Portfolio

CYBER SECURITY LAYERS

7 Layers of Cybersecurity



End Point Security, End Point Security Detection & Response. Mobile/Tablet management

Patch Management, Web application Firewalls, API Security

Secure Design & topology, VLANs. Multi layer Firewall

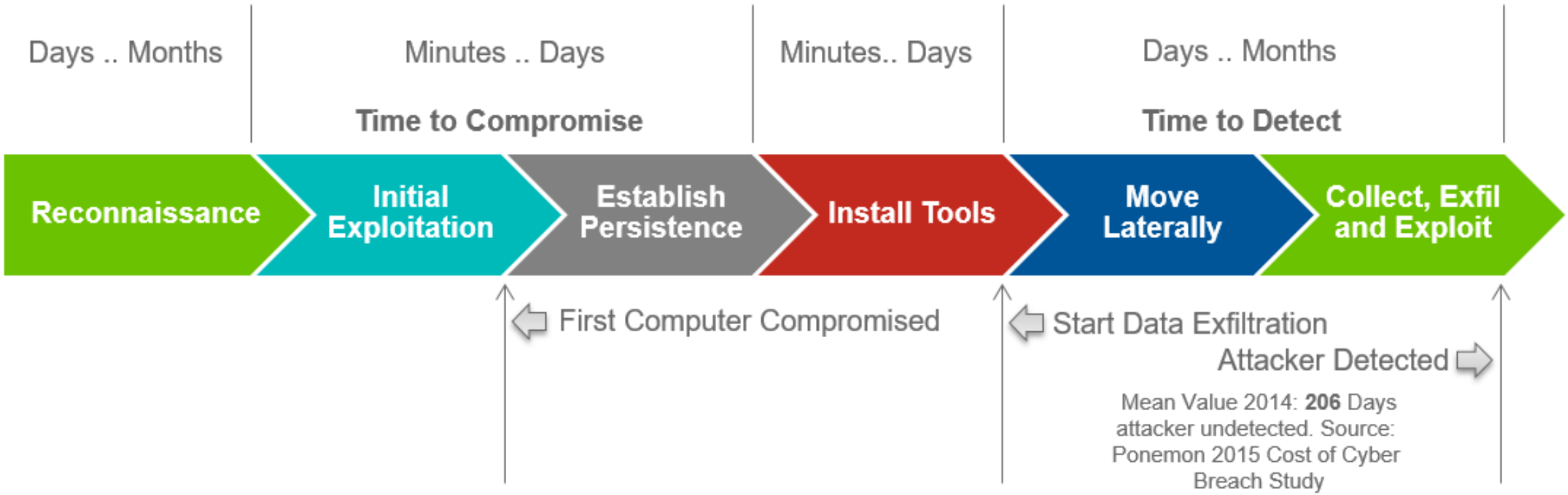
Firewalls, Email Security, Email Encryption

Human Training

Data Classification, Data Loss prevention across Operating systems

Back up, Email Archiving

The Six Phases of a Cyber Attack



Critical Infrastructure Assessment



Layers of Cyber Defense in IT

SIRI TECHNO FABS
www.siritech.net

Patch Management

Web Application Firewall

API Security

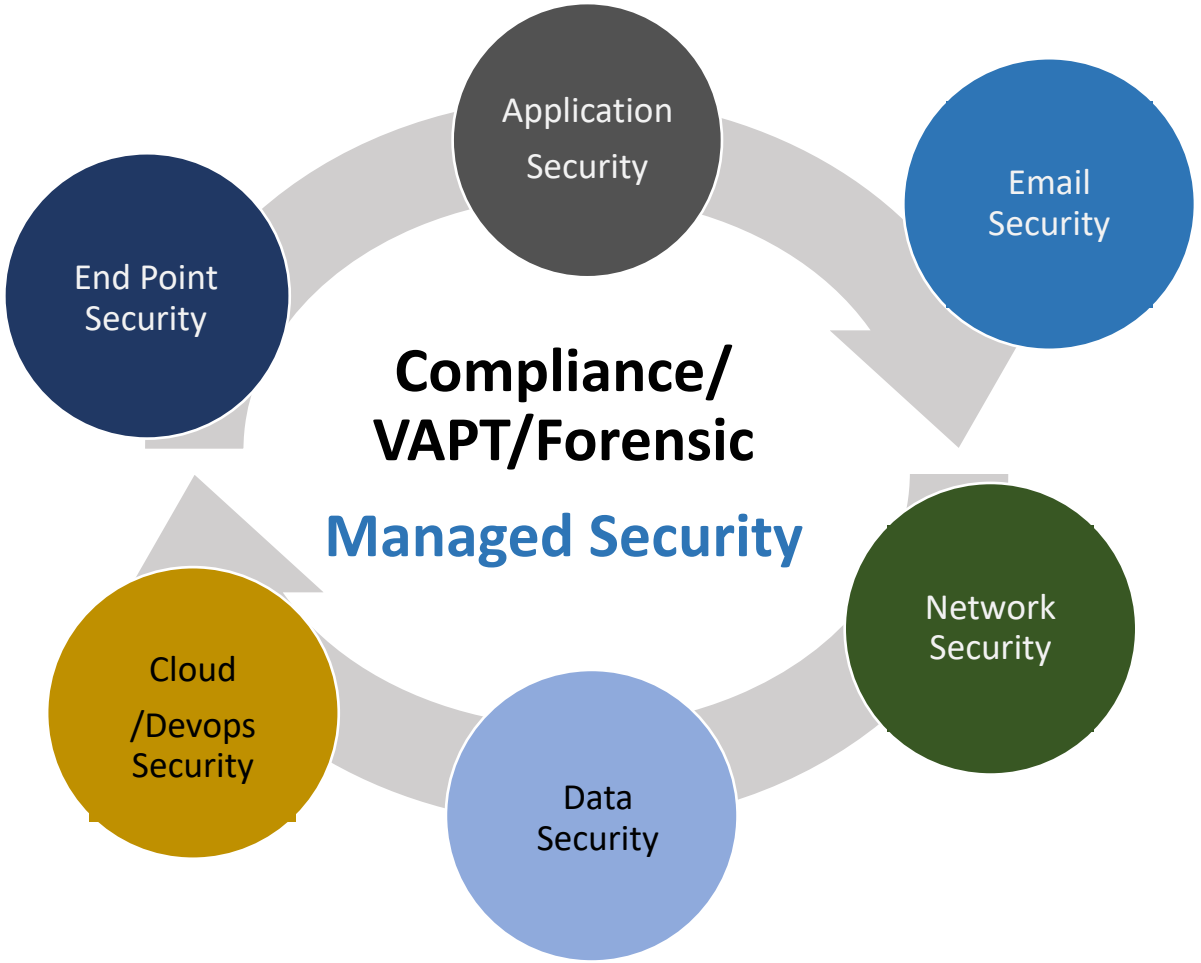
CS Asset Management

End Point Detection & Response

DLP & Encryption

Mobile Device Management/UEM

Identity & Access Management (IAM)



Email Security

Email Encryption

Email Security specially for Microsoft

Email archiving

Cloud Access Security Broker (CASB)

Cloud-native application protection platform (CNAPP)

NDR/NAC

Network DLP

Identity & Access Management

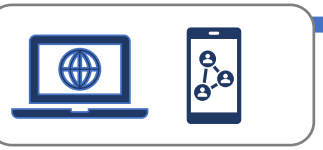
Privilege access Management(PAM)

Database Activity Monitoring

Data Classification

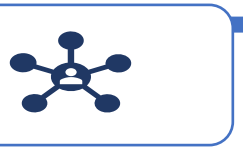
Data Loss Prevention

Defensive Security Mechanism



Endpoint Security

- Antivirus/EDR –
- Data Leak Protection (DLP)
- Email Security & Encryption
- Patch Management
- End Point Encryption
- Application Security
- Endpoint Monitoring & Risk Compliance
- Identity Access Management
- Mobile device Management
- Security awareness training



Network Security

- VAPT
- Network Access Control (NAC)
- Network DLP
- Network Detection and Response (NDR)
- Web Application Firewall (WAF)
- Logging & Reporting - SIEM Solution
- Security Operation Center
- DDoS, Encryption,
- Privilege Access Management
- Web Security



Cloud Security

- Cloud Access Security (CASB)
- Logical Segmentation
- Encryption and Hardening
- Logging & Reporting - SIEM Solution
- Cloud Monitoring

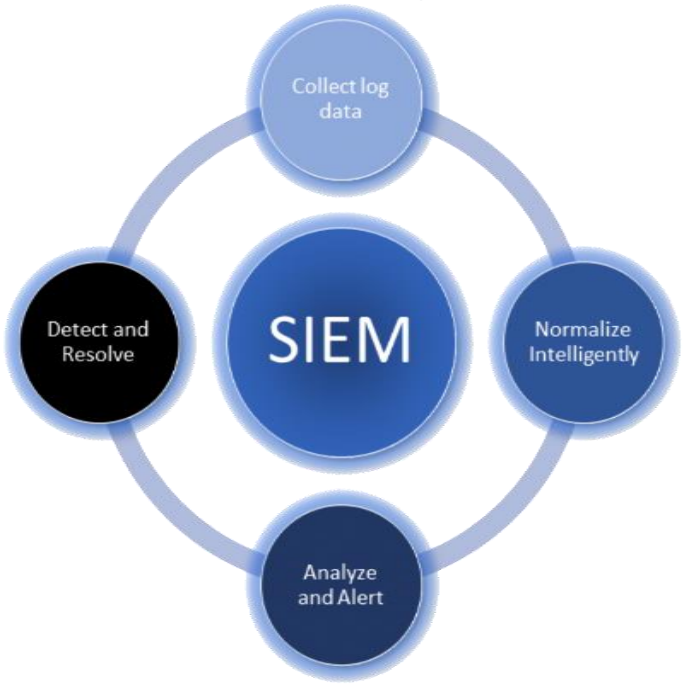
Consulting & Compliance-VAPT-Dark Web Monitoring

Security Operation centre (SOC)

Security Incident & Event Management

SIRI TECHNO FABS
www.siritech.net

Threat Intelligence → Visibility with reporting → Uncover anomalous behavior → Better Reporting → Protect your critical data



- Log Collection, Analysis, Forensics & Retention
- Event Correlation
- IT Compliance
- Application Log Monitoring
- Object Access Auditing
- Real-time Alerting
- User Activity monitoring
- Dashboards
- Reporting
- File Integrity Monitoring
- System and Device Log Monitoring

Accelerate Threat Detection and Response

Reduce operational complexity

Maximize analyst time and talent

Network threat analytics

Cyber attack visibility and Fewer potential security breaches

Security Operations Centre (SOC)

SIRI TECHNO FABS
www.siritech.net

Challenges

- Can I have real time visibility of attacks ?
- Is there any insider threats ?
- Can I do cyber forensics ?
- Is there any automatic timeline ?
- How do I integrate threat intelligence ?
- How do I determine complex threats ?
- Is there any event co relation ?
- How do I monitor them ?
- What is the reporting mechanism ?

How do we manage Logs across so many systems ?



- 24*7 Real-Time Security Monitoring and Incident Response
- Visualize and Understand Malicious or Anomalous Activity
- Analyze, Prioritize, and Respond to Threats in Rapid Time
- Safeguard your Data, People, and Processes
- Contain Threats via Incident Playbooks and SOAR Platform
- Detect Complex Threats with Advanced Correlation and Machine Learning
- Intrusion Detection
- Vulnerability Assessment
- Threat Advisory Services
- Threat Intelligence
- Infrastructure Security Monitoring
- Meeting Compliance Requirement

Brand Protection & Dark Web Scanning

SIRI TECHNO FABS
www.siritech.net

Challenges

How to make sure continuous Brand Protection & Digital Risk Monitoring of the enterprise footprint with flexible configuration and scales to your environmental growth across a variety of digital channels?

Brand Protection! Digital Risk Protection!

Determine regulatory compliance scopes for the Indian Digital Personal Data Protection (DPDP) Act, 2023, General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and other data privacy laws

Comprehensive Coverage

- Brand Protection
- Digital Risk Protection
- Dark Web and e-Crime Monitoring (DWM)
- Cyber Threat Intelligence (CTI)
- Social Media Monitoring

Data Loss prevention

Continuous Brand Protection & Digital Risk Monitoring of the enterprise footprint

- Dark Web and Underground Resources
- Social Media Networks
- Mobile Marketplaces
- Domain Zones Repositories (Top TLDs)
- E-Mail and Spam Traffic
- Mobile Messengers (IMs)
- Surface WEB (phishing demains, etc.)
- Graphical Content (Logo, Images, etc.)

Sample SOC Use cases

SIRI TECHNO FABS
www.siritech.net

Excessive Windows Login Failures	Host compromise Phishing based Infiltration attack	DB Authentication Failure	Windows abnormal Shutdown	Remote access login - success & failure	Critical service stopped on Windows Servers	Malicious/Suspicious attachments identified
Excessive Firewall Denies	Geo Location anomaly For VPN / SSO logins Followed by MFA anomaly	Login attempts with the same account from different source desktops	Data Leakage Identified through large file send via mail	Interactive use of service account	Detection of use of default product vendor accounts	Targeted Attacks
Firewall Drop	Service Account misuse	Removable media detected	Top 10 Email Receivers/Senders	Active Directory Attempt to restart AV service or process, AV modules from Infected machine.	Database Schema Creation/Modification	High Email Bandwidth utilization by individual users
IPS alert	User Login Success and Firewall Deny	Server shutdown	Top 10 users sending mails to external domains	Any DB / Oracle- Update or Insert Commands	Detection of system time changes (Boot time)	POS malware
Login Failures	Abuse of access privileges	Users Created /Deleted within short period	Windows Service Stop-Restart	Any DB / Oracle user Created/Deleted	Windows Security Log is full	High number of rejected mails from single “from” address

Sample Cloud SOC Use cases

SIRI TECHNO FABS
www.siritech.net

Authentication IAM, PAM, User Directories	EC: AWS Cloud - An AWS API Has Been Invoked From Kali	EC: AWS Cloud - Detected a Massive Creation of EC2 Instances	AWS Cloud: S3 Bucket has been created	AWS Cloud: S3 Bucket accessed by Non-Standard User	AWS Cloud: Multiple Console Login Failures from Same Source IP	AWS Cloud: An EC2 Instance Has Been Created In A Non-Standard VPC or without VPC
AWS Cloud: Detected A Successful Login To AWS Console From Different Geographies	EC: AWS Cloud - Detected An Email with An Attachment From a Spam Sender	EC: AWS Cloud - Microsoft Word Launched a Command Shell	AWS Cloud: Network ACL Changes	AWS Cloud: An EC2 Instance Has Been Created with Large Specifications	AWS Cloud: An EC2 Instance Has Been Created From A Non-Standard Amazon Machine Image (AMI)	AWS Cloud: Detected A Change To AWS Trail Logging Configurations
AWS Cloud: Multiple Failed API Requests From The Same Username	BB: AWS Cloud: API Request Has Been Denied	AWS Cloud: Password Policy Updated	AWS Cloud: Multiple Console Login Failures From Different Source IPs	AWS Cloud: Cloud activity by root user	AWS Cloud: Routing Table Changes	AWS Cloud: A Signing Certificate Has Been Removed
AWS Cloud: User who has no admin rights accesses an Admin Role	AWS Cloud: User Profile Updated	AWS Cloud: Multiple Failed API Requests From Same Source IP	AWS Cloud: Multiple Failed API Requests From Different Source IPs	AWS Cloud: VPC Configuration Changes	AWS Cloud: S3 Bucket has been deleted	AWS Cloud: S3 Bucket Policy changes
AWS Cloud: Logs Have Been Deleted / Disabled or Stopped	AWS Cloud: Group has been Created or Deleted	AWS Cloud: User added to a Group with Admin Role Capability	AWS Cloud: Network Gateway Changes	AWS Cloud: Critical EC2 Instance Has Been Stopped OR Terminated	AWS Cloud: Security Group Configuration changes	AWS Cloud: Key Pair Management configuration changes

Secure Access Service Edge (SASE) Solutions

SIRI TECHNO FABS
www.siritech.net

Challenges

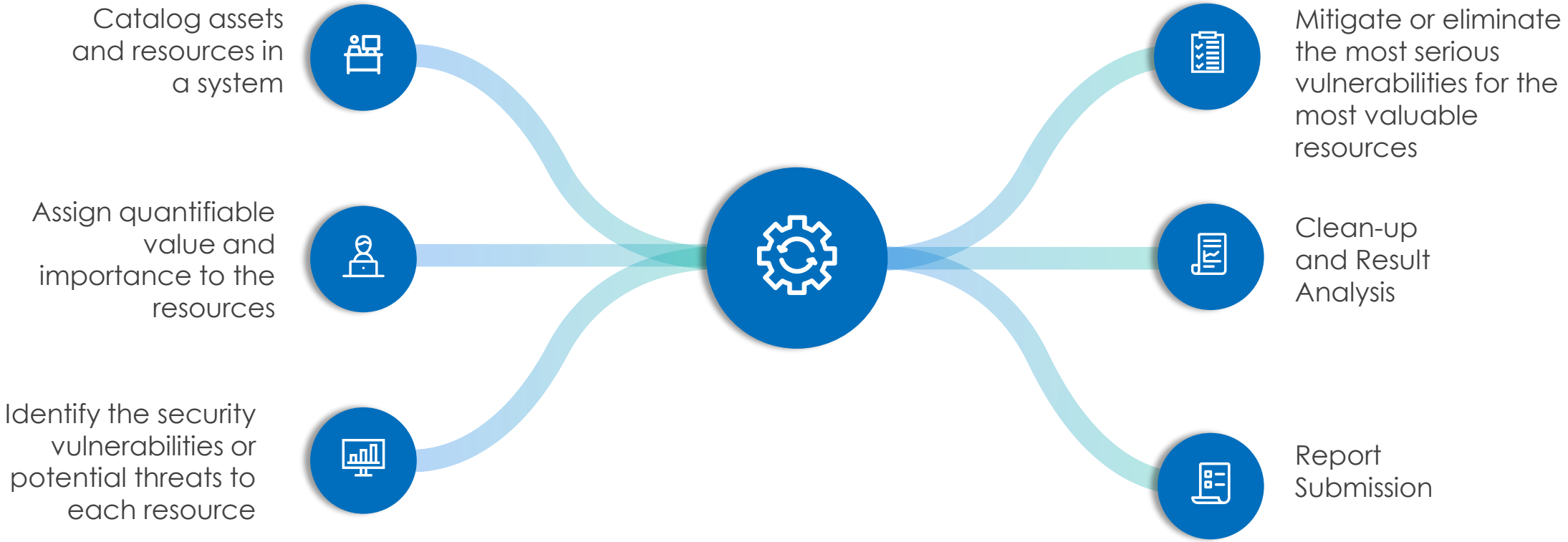
- Latency and Performance Issues
- Inconsistent Security Policies & Remote and Hybrid Workforce Security
- Securing Multi-Cloud Environments, Data Protection and Compliance
- Mitigating Advanced Cyber Threats & Scalability and Cost Efficiency
- Complex Network and Security Management



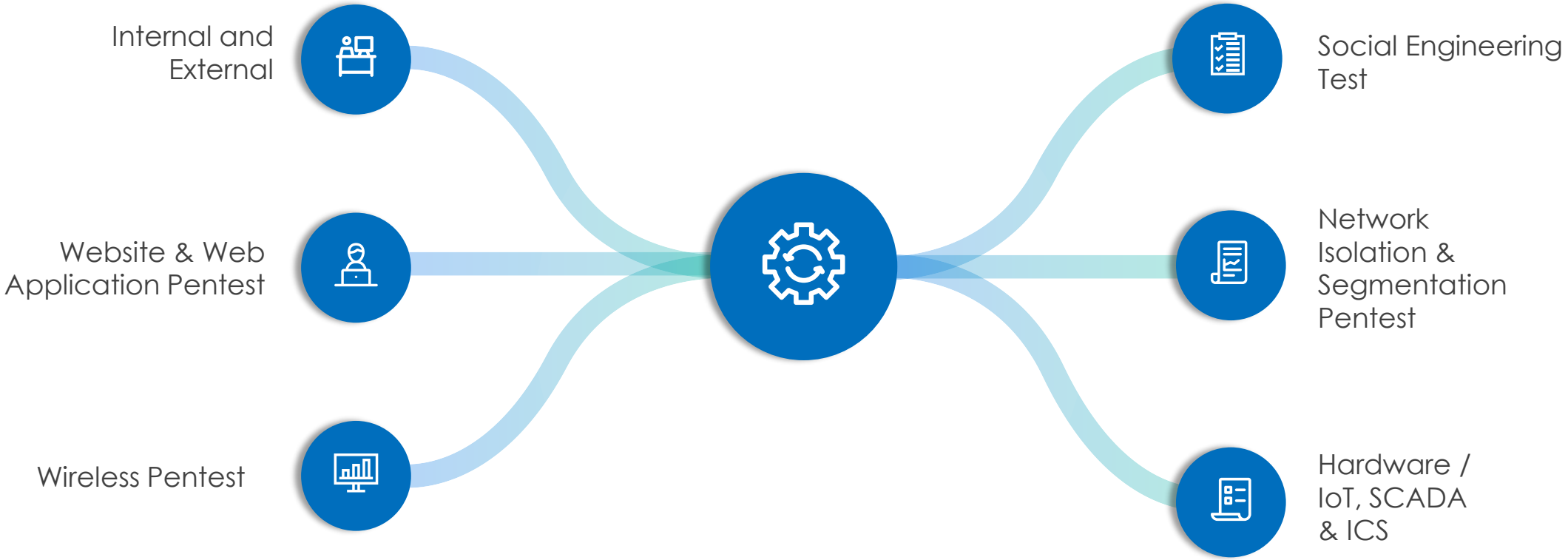
SASE delivers multiple converged-network and security-as-a-service capabilities, combining software-defined wide-area network (SD-WAN) with Security Service Edge (SSE) components such as secure web gateway (SWG), cloud access security broker (CASB), network firewalling and zero trust network access (ZTNA).

- Reduce network cost and complexity
- Improve overall security posture
- Boost network resilience and business agility
- Complete VPN replacement

Vulnerability assessment



Penetration Testing



Data Classification & Data Loss Prevention

SIRI TECHNO FABS
www.siritech.net

Challenges

Identify internal confidential data like customer proof of identity (Aadhar/PAN/Credit Cards Etc.) numbers for protection

Ensure there is no leakage of any critical data all critical data is

Determine regulatory compliance scopes for the Indian Digital Personal Data Protection (DPDP) Act, 2023, General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and other data privacy laws

Data Classification

Data classification is the process of organizing data into categories that make it easy to retrieve, sort and store for future use.
A well-planned data classification system makes essential data easy to find and retrieve. This can be of particular importance for risk management, legal discovery and regulatory compliance.
Written procedures and guidelines for data classification policies should define what categories and criteria the organization will use to classify data

Data Loss prevention

Ensure that there is no critical data leakage across any operating systems be it Windows/Mac/Linux

- Cross platform support (Windows/Mac/Linux)
- Feature parity across operating systems
- Zero day support for Windows and Mac
- Light weight
- Unparallel device control capabilities
- Ease of deployment and use
- Recognized by industry professionals

Safeguarding Emails

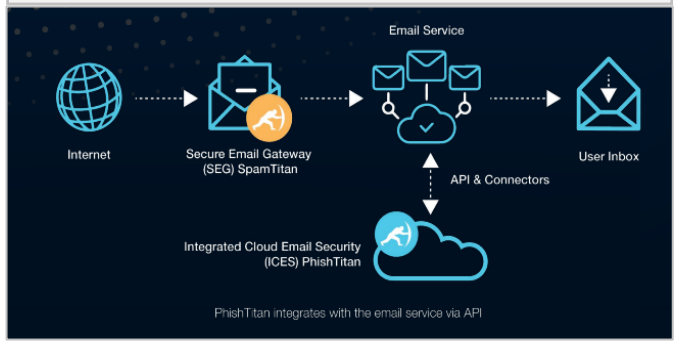
Phish Titan

SpamTitan rejects 99.99% of malicious mail with front line tests before reaching customer mail servers. This multi-vectored approach scans emails to block phishing threats using Realtime Blackhole list (RBL), Recipient verification , Sender Policy Framework (SFP), Domains Key identified mail (DKIM)

1 Secured Email Gateway

SPAM Titan + Phish Titan

- Malware blocked at point of entry
- Double Antivirus plus Sandboxing
- Malware/Aniti-SPAM/Malicious Email Blocking
- AI, ML & LLM based Phishing protection
- BEC Protection
- Advanced Threat Protection
- Post Delivery Remediation



2 Integrated Email Security

Encrypt Titan

It secures messages & stops accidental/deliberate data leaks. messages . It is delivered via conditional TLS and/or secure web portal. It enables users to encrypt email messages by wither using keyword or content filters that have been configured on SPAM Titan or by using Encrypt outlook plug in.



3 Encrypting Emails

SIRI TECHNO FABS
www.siritech.net

Cyber Knowledge Assessment, Risk & Compliance Reporting (SAFE Titan)

Privileged Access Management (PAM)

SIRI TECHNO FABS
www.siritech.net

Challenges

How do I Control and monitoring privileged user access to your most critical data and systems

How do I Control and monitoring privileged user access to your most critical data and systems

How can we streamline the authorization and monitoring of privileged users

How do I Control and monitoring privileged user access to your most critical data and systems

Accidental or deliberate misuse of privileged access ?



Secure, control and monitor access to critical information and resources

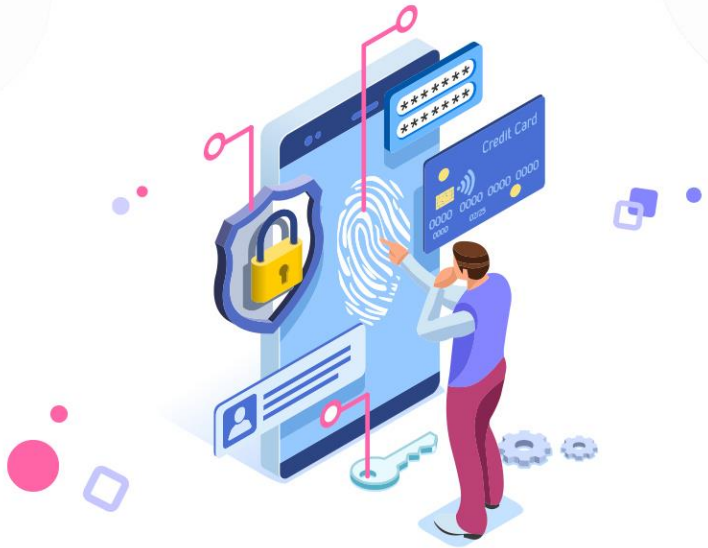
- Identify Critical Resources and Access Points
- Discover and Onboard All Privileged Accounts
- Segment Systems and Assets
- Separate Privileges and Duties
- Robust Reporting and Logging System
- Behavioral Analysis

Identity Access Management (IAM)

SIRI TECHNO FABS
www.siritech.net

Challenges

- User Password Fatigue
- Siloed User Directories for Each Application
- Provide Consistent Access to On-Prem and Cloud Applications
- Different Administration Models for Different Applications
- Scaling hurdles and performance drag
- Scaling hurdles and performance drag
- Compliance Visibility: Who Has Access to What?



Define and manage user identities and access permissions

- Manage User Identities
- Provisioning and de-provisioning Users
- Authenticating Users
- Authorizing Users
- Reporting
- Single Sign-On
- Multi-Factor Authentication
- Governance for Access Management

Network Access Control

Challenges

- Network Segmentation
- Incident response
- How do I manage my Assets
- How do I have Device compliance visibility ?



Restrict unauthorized users and devices from gaining access to a corporate or private network

- Improved Security
- Policy Life-cycle Management
- Profiling and Visibility
- Guest Networking Access
- Security Posture Check
- Incidence Response

Database Activity Monitoring

SIRI TECHNO FABS
www.siritech.net

Challenges

Identify and report on fraudulent

Illegal or other undesirable behavior

How do I monitor database Activity?

How do I make sure integrity of Databases?



Encrypt files, databases and applications, address data security and privacy regulations, and control encryption keys for cloud-based data

- Protect data across environments
- Address compliance requirements
- Reduce administrative effort
- Management of user access policies

Patch Management

SIRI TECHNO FABS
www.siritech.net

Challenges

How do I reduce my cyber risks ?

How do I fix vulnerabilities of my software, Operating systems & applications ?



Identify unexpected patch failures and maintain the functionality and security of all your critical systems and applications

- Deploy patches on time
- Pre-test complex updates
- Policy-driven patch management
- Patch Knowledge
- Patch Scheduling
- Extensive expertise

Compliances – ISO 27001

Challenges

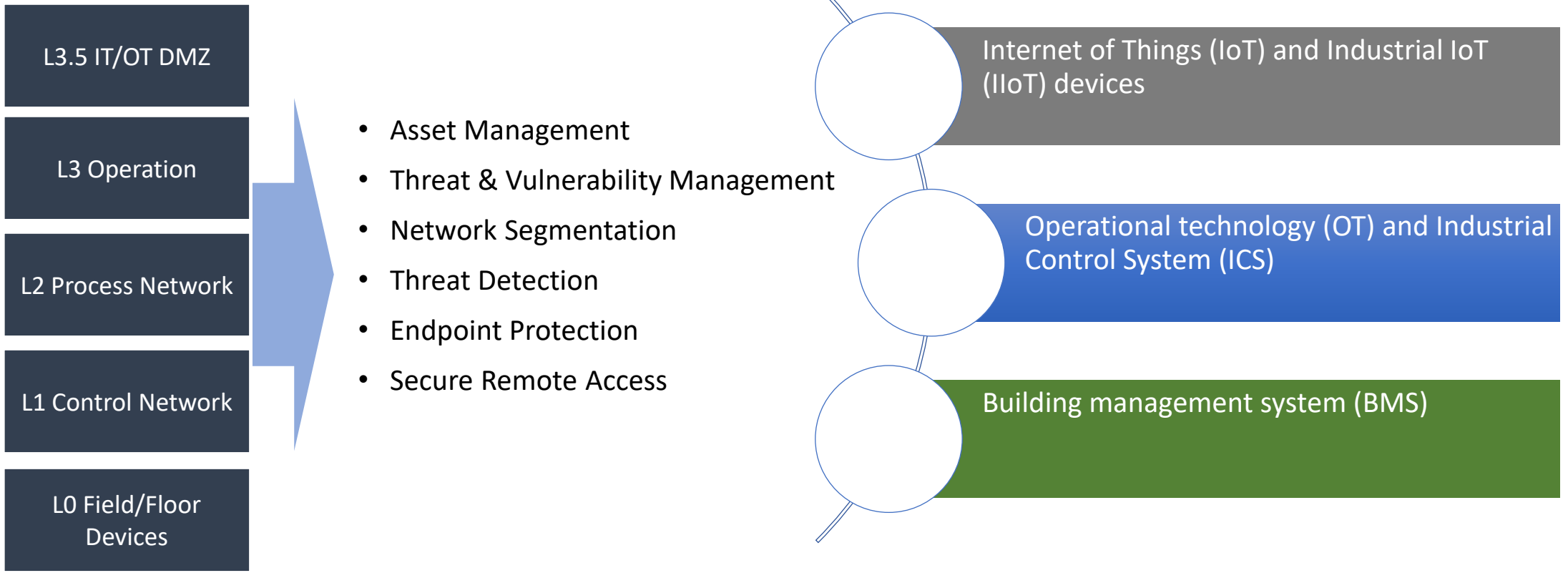
How do we demonstrate good security practices, which can improve relationships with clients and give you a competitive advantage?

How to identify, manage and reduce the severity of regular threats to information?

a. Protect Confidentiality: ISO 27001 helps safeguard confidential information, including customer data, intellectual property, and business secrets.
b. Ensure Integrity: The standard ensures the integrity of information by preventing unauthorized modification, and ensuring its accuracy and reliability.
c. Maintain Availability: ISO 27001 aids in ensuring that information and IT systems are available when needed, minimizing downtime and ensuring business continuity.
d. Manage Risks: ISO 27001 provides a systematic approach to identify, assess, and manage information security risks, enabling organizations to make informed decisions and allocate resources effectively.
e. Enhance Trust and Reputation: Achieving ISO 27001 certification demonstrates an organization's commitment to information security, enhancing customer trust and reputation.

Operational Technology Cyber Security Controls

OT/ICS Technology



Some of our SMB customer's

STF SIRI TECHNO FABS
www.siritech.net

Mfg.



















IT/ITES.















Service













Health







BFSI









Our Partial Clientele























































Our Partial Clientele





Siri Technofabs
#643 68CRS K.S. LYT
Bangalore 560078
Karnataka, India
+91 8105644411
support@siritech.net
www.siritech.net