How to BUILD Next-Gen SOC

Chintan Gurjar

About Me

Born in India
1990

B.Tech
Computer
Engineering
2011

London
Master's
Cybersecurity
2013-14

Returned to
India
2014

Worked in
consulting firms
2014-2017

New Zealand
Worked for
Big4
2017

London
Worked in
product-based
firms
2020-Present

Companies I worked for:

INDUSFACE™

zebpay
bitcoin • blockchain • india

LUCIDEUS™
SECURING DIGITAL

Let's Nurture™

NOT SO SECURE

KPMG

TESCO

TikTok

Domains I worked in:

- Pentest/Red-teaming
- Threat Intelligence & Hunting
- A tiny bit of DevSecOps
- Vulnerability Management
- Audit and Risk Management

Total Experience

- 7 Years in Offensive Security
- 4 Years in Defensive Security

Certifications

OSCP | CEH | CTIA | MGT516 (SANS) | CCFA | CCFH | CBE

Outside of Work:

- Mentoring & Coaching
- Blogging/Webinars
- Paragliding
- Cricket, Badminton, Table Tennis
- Reading management books

Contact Me:

chintangurjar@outlook.com

@iamthefrogy

Chintan Gurjar

SCR – Situation, Complication, Resolution

Situation

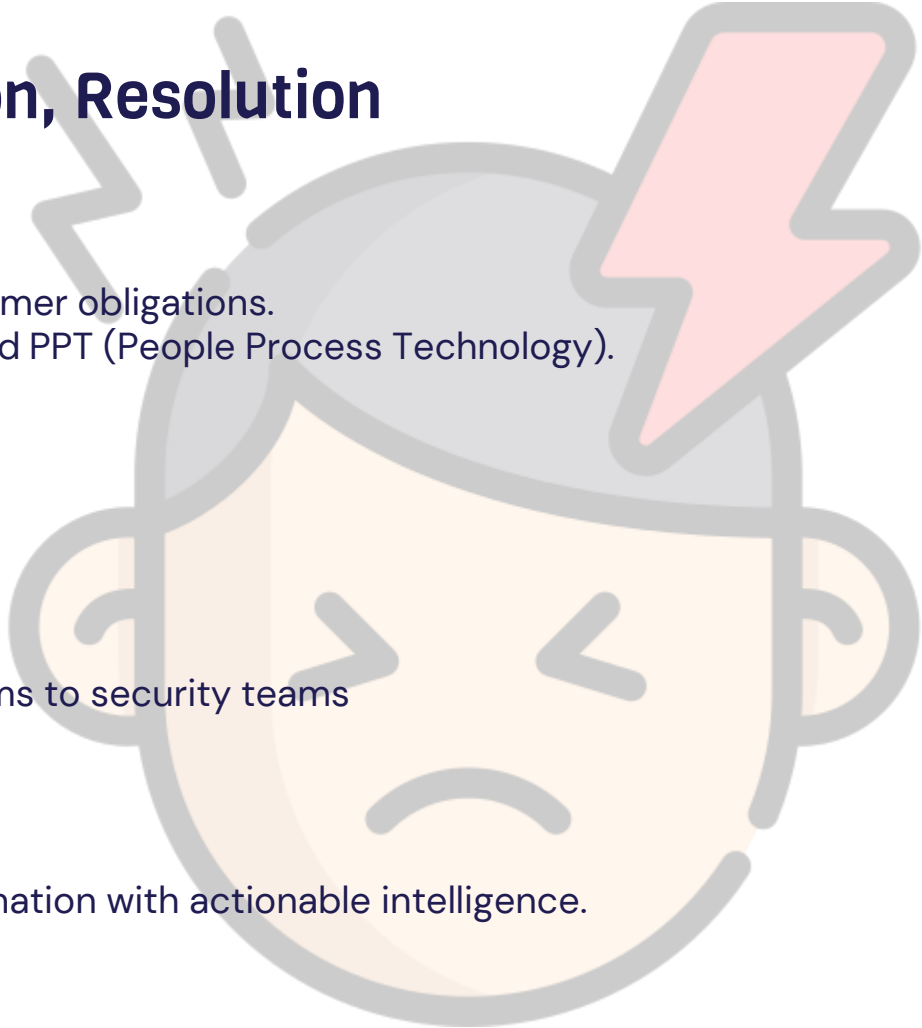
- Juggling business, compliance, and consumer obligations.
- SOC has become resource intensive. Need PPT (People Process Technology).

Complication

- Huge of amount of data sources
- No correlation
- Lack of standardization
- Poor visibility
- Lack of communication among other teams to security teams
- Cost cutting

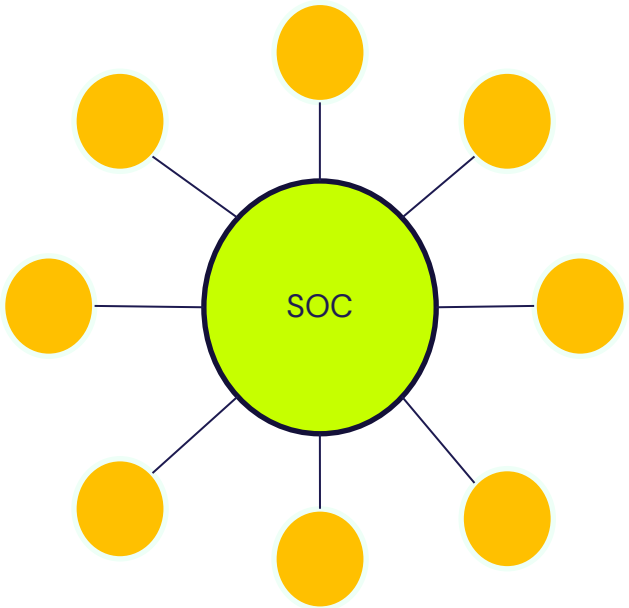
Resolution

- Convert security events and threat information with actionable intelligence.

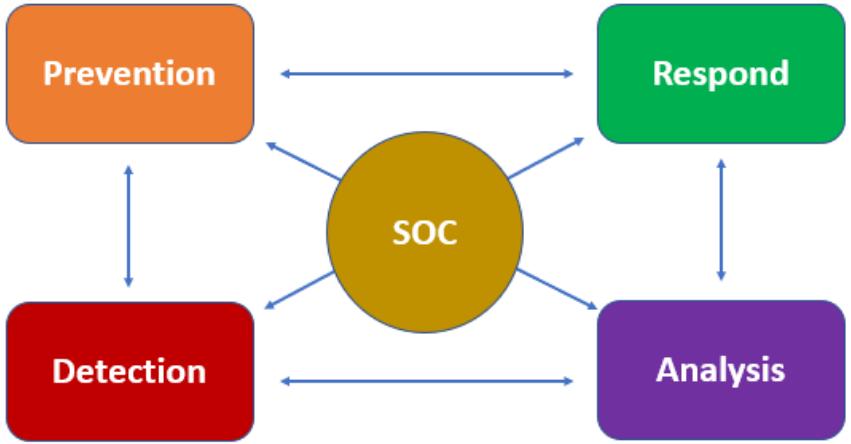


Traditional SOC vs. Next-Gen SOC

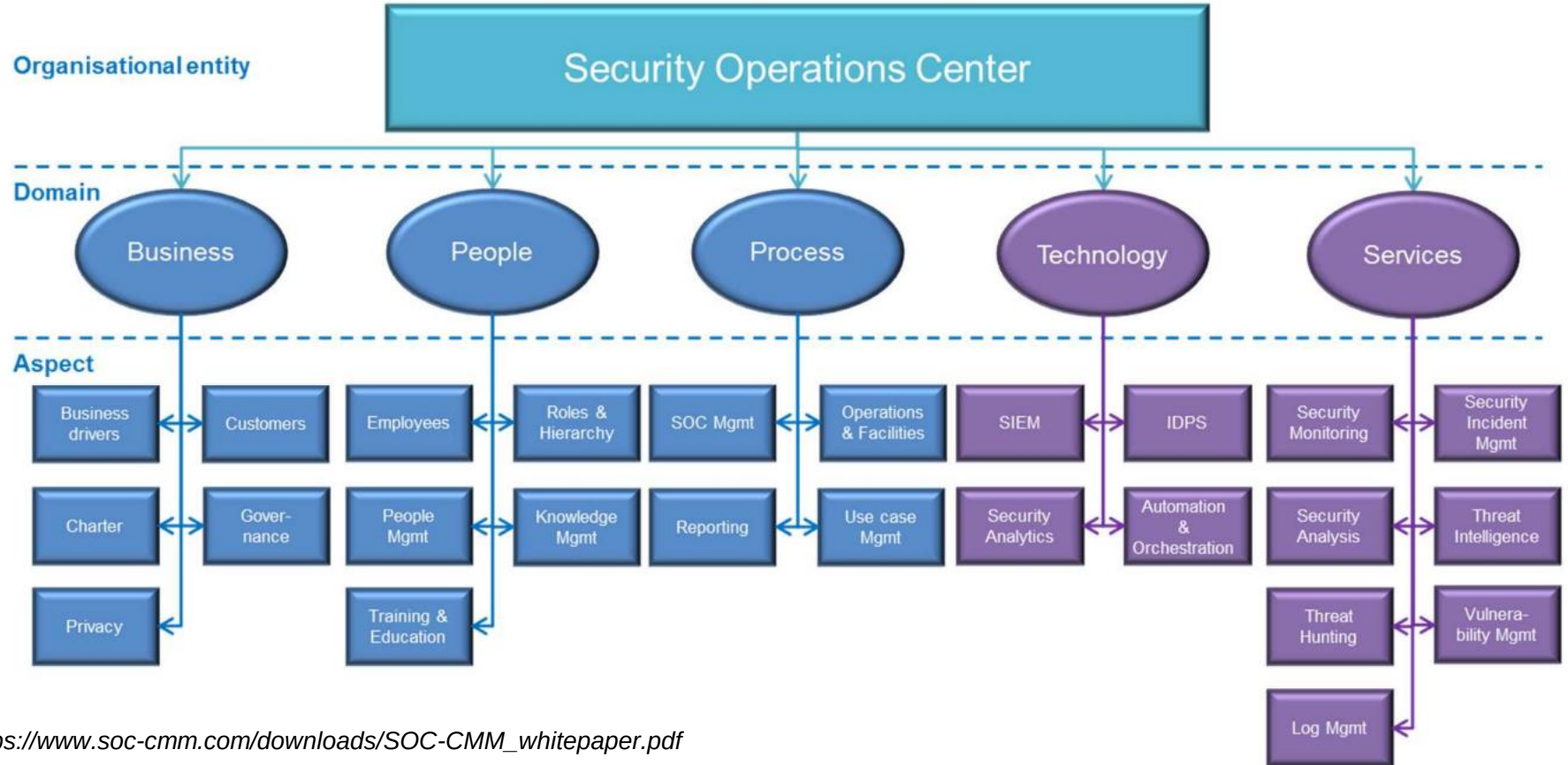
Traditional SOC



Next-gen Collaborated SOC



Next-Gen SOC Organizational Entity



https://www.soc-cmm.com/downloads/SOC-CMM_whitepaper.pdf

BENEFITS OF NEXT-GEN SOC (INTETEGRATED SOC)

Tactical Benifts

- Find threats earlier in the cyber kill chain
- Focus efforts on real threats than traditional daily events and alerts
- Dynamic correlation to rule logic improvisation by working with SIEM and other team

Operational Benefits

- Intelligence-driven processes
- Improved effectiveness of SIEM, NGFWs, IPS, IDS, and SWGs.

Strategic Benefits

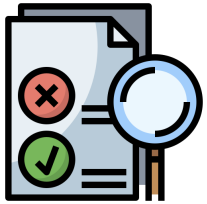
- Executives can understand relevant threats and appropriately allocate resources where necessary.
- Improved internal and external communication with top executives and board members

Metrics are key to action

Process of defining quality metrics:

- Know your audience well (Strategic, Operational, Tactical)
- Be S.M.A.R.T (Specific, Measurable, Achievable, Relevant, and Time-Bound)
- Document metrics
- Discuss with the client
- Sign off
- Implement

Phases of SOC implementation



Phase 1

Assess the current maturity state

Phase 2

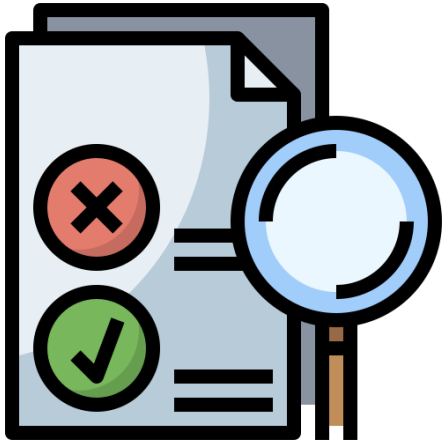
Design your target SOC state

Phase 3

Develop an implementation roadmap

Phase 4

Comprehensive reporting



Phase 1

Assess the current maturity state

Overview – Assess The Current Maturity State

Objectives

- Make your client understand the benefits for re-assessing and refining SOC
- Assess your current prevention processes and competencies, and it's completeness
- Assess your current detection processes and competencies and their completeness
- Assess your current analysis processes and competencies and their completeness
- Assess your current response processes and competencies and it's completeness

Results

After completion of this phase, you will know the current maturity state of your SOC and will have an idea what of where the re-defining process needs to be started.

Benefits

Activity will enable you to:

- Understand difference traditional vs next-gen SOC
- Know where you stand
- Optimize security operation through next-gen processes

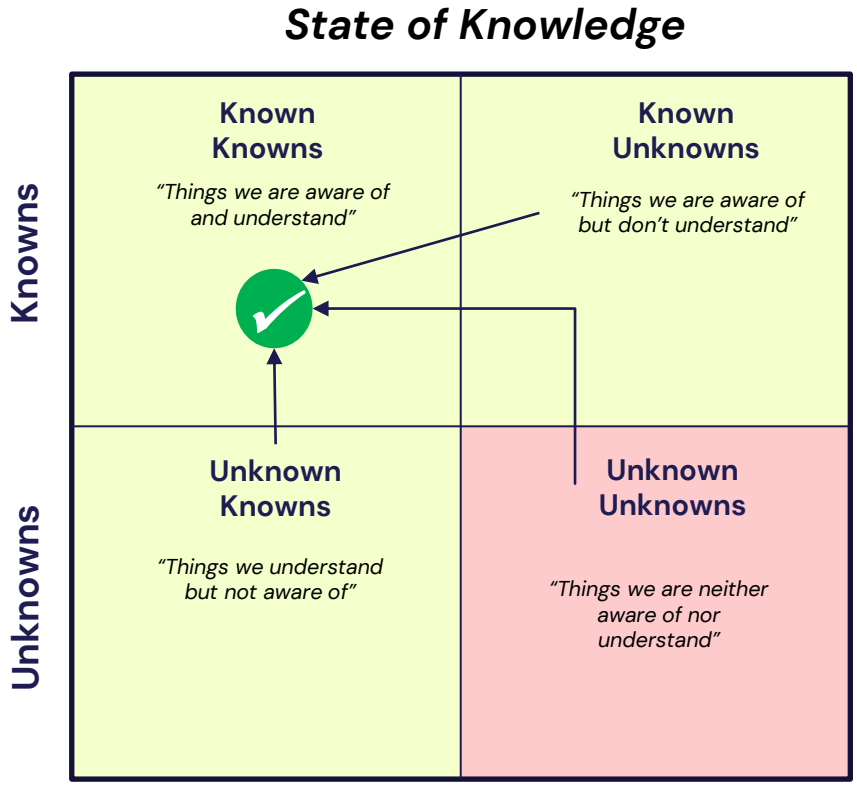
Discuss why build Security Operation Center

Discuss why running SOC? Objectives, strategic vision etc.?

Process:

1. Discuss scope, goal, responsibilities, etc.
2. Put everything on the whiteboard.
3. Organize notes and remove duplicates.
4. Finalize benefits, goals, and objectives of SOC.

What do you know about your organizations' security state



Process:

1. Assess what the client knows about their SOC in terms of all these 4 criteria
2. Ask each stakeholder to define PPT (People, Process, Technology)
3. Think of an additional PPT you would have included to mature the state of SOC
4. Discuss why to include or why to exclude
5. Prioritize based on the organization's need, cost, etc.
6. Identify what to outsource/insource.

SOC Levels by domains covered

Foundational	Operational	Strategic
• Device monitoring • Intrusion management • Log collection and retention • Reporting & escalation • Vendor management • Audit compliance • Firewall • AV/EDR • SIEM • VA • Patch management • Ticketing	• **Entire Foundational +** • Event analysis and incident triage • Hardening • Static malware analysis • Change management • Cloud security • Encryption management • IAM	• **Entire Foundational + Operational +** • SIEM with defined use-cases • Threat intelligence • Digital forensics • Network flow analysis • Dynamic malware analysis • Visualization and dashboards • Threat hunting • Use case management

Security Operations Capabilities

Assess

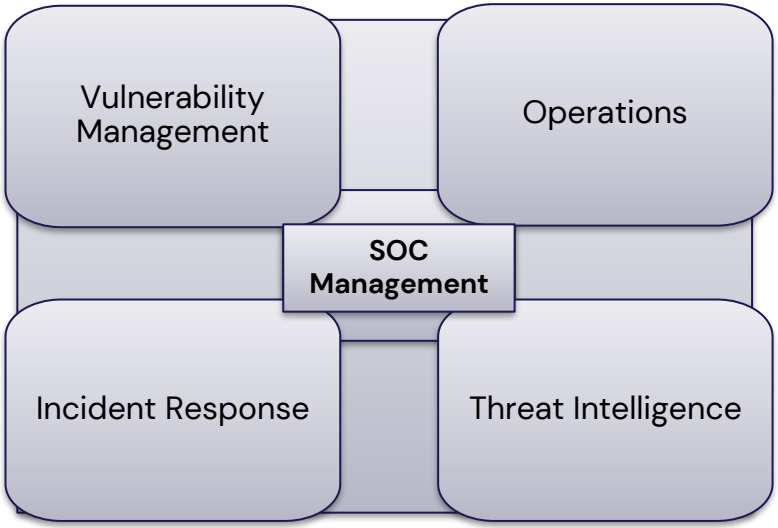
SOC Levels by maturity of elements

Foundational	Operational	Strategic
• Network and system architecture diagrams • Asset inventory and classification • Access control policies and procedures • Vulnerability management processes • Patch management processes • Configuration management processes • Security monitoring tools and processes • Security training and awareness programs • Data classification and protection policies • Disaster recovery and business continuity plans	• Real-time monitoring and analysis of security events • Detection and analysis of security threats and vulnerabilities • Incident response and remediation • Continuous improvement of security posture through lessons learned and analysis of security events • Security testing and assessment processes • Threat intelligence gathering and analysis • Vulnerability management and remediation • Patch management • Security incident management and response • Compliance management	• Development of long-term security strategies and roadmaps • Alignment of security initiatives with business goals and objectives • Collaboration with other teams, such as the incident response team, to ensure a coordinated and effective approach to security • Management of security budgets and resources • Regular reporting and communication of security posture to executive leadership and stakeholders • Risk assessment and management processes • Security architecture design and review • Vendor and third-party risk management • Cybersecurity strategy development and review • Collaboration with industry partners and law enforcement agencies on cybersecurity issues.

Clear comunication is the key

SOC is the single pane of glass which definitely requires a transparent and clear communication strategy.

Problem = Disjoint teams and no communication
Solution = Collaboration through transparent communication



Communication Best Practices

1. Security operations should not be handled haphazardly; a consistent and transparent communication should be maintained.
2. Create an open and accessible channel of communication within the threat collaboration space.
3. Set up a central web/knowledge portal that is easily accessible throughout the threat collaboration space where you can store cookbooks, SOPs, guides, policies, metrics, tools, etc.
4. Organize regular meetings with key personnel from various working teams (VM, SIEM, TH, CTI, Appsec, Security Architecture) to discuss issues, share objectives, and communicate operational procedures related to their individual roles.

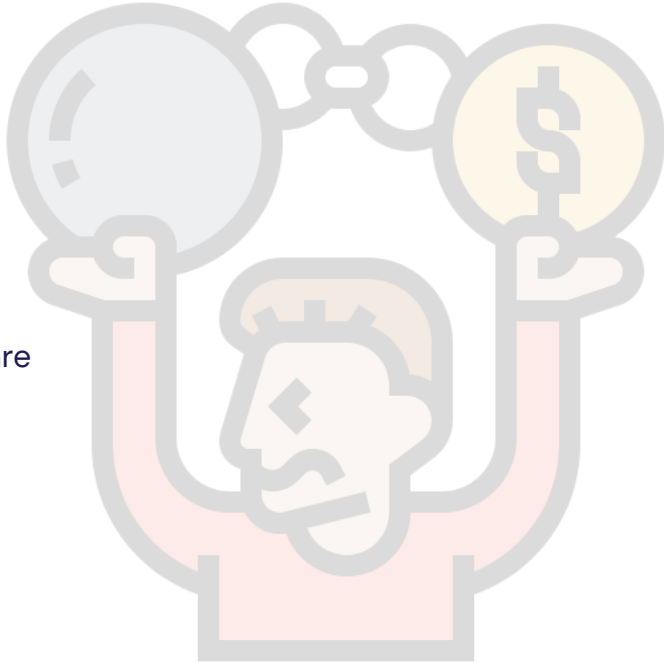
Benefits of internal collaboration

1. Improved communication
2. One organization one goal
3. Improved revenue growth
4. Improved knowledge sharing
5. Increase productivity
6. Increase problem solving ability
7. Increase operational efficiency

Identify and document Security Obligations

Process:

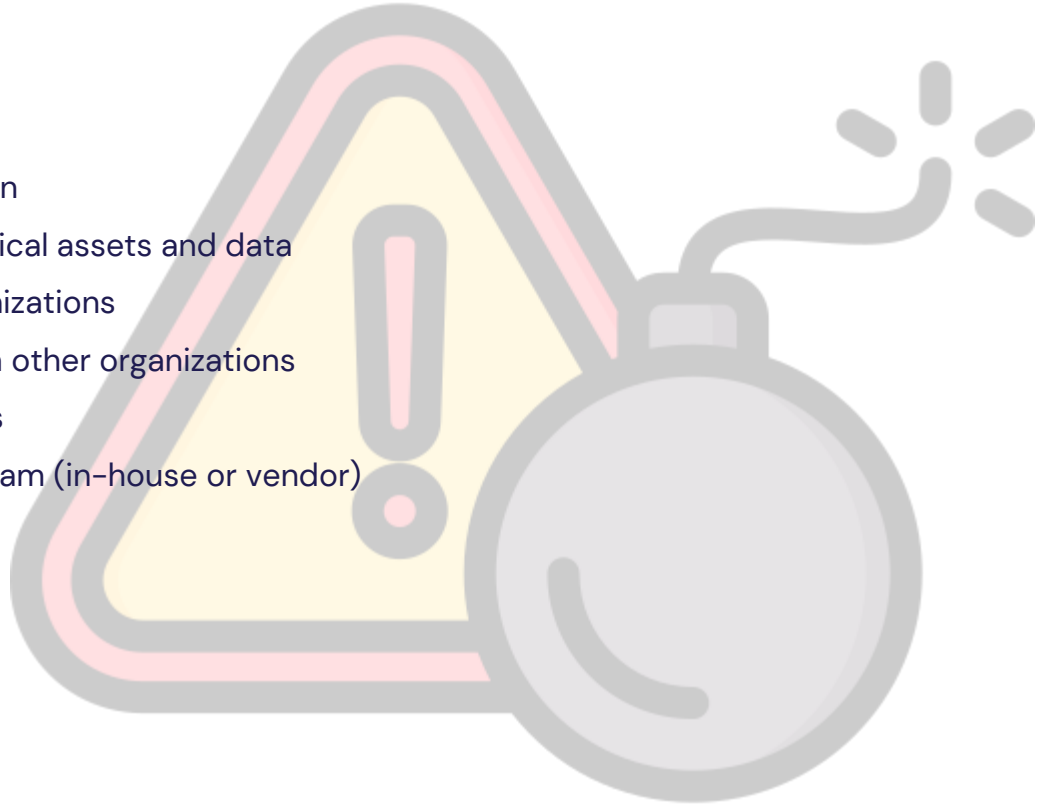
1. **Identify stakeholders**
2. **Brainstorm security obligations**
    1. Business obligations
    2. Customer obligations
    3. Regulatory obligations
    4. Other obligations
3. **Discuss**
    1. Identify what all business/customer/regulatory obligations are there.
    2. How will it affect SOC processes and priorities?
    3. How to solve them?
    4. Log them into requirements



Identify Threats to your Organization

Process:

1. Brainstorm threats Low to Critical
2. Identify critical assets in your organization
3. Identify crown jewel data in your organization
4. Discuss what can be the threats to your critical assets and data
    1. Consider past incidents of your organizations
    2. Consider incidents' case studies from other organizations
    3. Consider threat modelling techniques
    4. Consider talking threat intelligence team (in-house or vendor)



4 core elements of successful SOC division

People	**Team Management, retain and motivate resources**	Provide clear career path and in-house, external trainings along with CTFs, incentives and reward program
Process	**Standard Operating Procedures** **Daily operations, Workflow Management** **Success Measurement management**	Write and maintain policies, workflows, procedure documents, cookbooks, policies, table-top exercises. Implement and measure the key success criteria for the program using KPIs and OKR methods.
Technology	**Prevention** **Detection** **Analysis** **Response**	Enable all prevention, detection, technologies, implement processes for analysis and escalation with response capabilities. Provide visualization and dashboards.
Services	**What all services can you provide**	Based on your maturity of the SOC, what all services it can provide or integrate within. Threat intel, threat hunting, security monitoring, vulnerability management, etc.

People

Threat Intelligence Analyst	Malware Analyst	Incident Responder (Minimum)
SOC Analyst (L1, L2, L3) (Minimum)	eDiscovery and Forensics Examiner	CISO (Minimum)
SOC Manager (Minimum)	VM Analyst	External 3rd Parties

People Challenges in SOC

Challenges	What?
Deliver 24*7*365 coverage	How you are going to roate shifts to avoid burnout problem and keep the team engaged.
Determine how many head count are needed actually	Create a head acount post analysis and also think about budget allocation. Get approval from the amangement. Align business need with the head count.
Burnout problem	SOC is the scale problem, large number of repetitive work, huge amount of big data. As a manager, you need to solve the burnout problem
Keep people motivated all the time in spite of repetitive work	Develop learning mindset, look at the bigger picture, incentives, long-term learning, attention to details, out of work learning, etc.
Set proper separation of duties	Prepare a specific and detailed RACI matrix and allocate responsibilities to avoid duplication of work
Training and development ROI	How much and when you are investing in training and how you are setting S.M.A.R.T goal to utilize that knowledge into real practical world. Think of the return you will get on your investment of training.
Understanding and meeting stakeholder requirement	If you don't know what they need, you can't deliver. Understand their need, align business requirement with SOC drivers, define key metrics to deliver before starting the process

Process

Core SOC Processes

- Incident Response
- Threat hunting and Intelligence
- Vulnerability Management
- Security Monitoring
- Compliance and Governance

SOC Process Drivers

- Use case management
- Detection and engineering
- Integration
- Quality assurance
- Dashboard and visualization

Frameworks & Methods

- SOC-CMM
- NIST CSF
- Threat modelling
- TaHiTi Threat Hunting
- Other...

Gauge your current progress with the technological checklist

Prevent

- ❑ NF
- ❑ WAF
- ❑ VPN
- ❑ IDS
- ❑ Antivirus
- ❑ DLP
- ❑ IAM
- ❑ NAC
- ❑ Web gateway
- ❑ Email gateway
- ❑ Anti-DDOS
- ❑ Etc.

Detect

- ❑ Network logging
- ❑ System logging
- ❑ AV logging
- ❑ Log management
- ❑ IDS
- ❑ Threat intelligence feeds
- ❑ Etc.

Analyze

- ❑ Sandboxing
- ❑ Ticketing system
- ❑ Automation software
- ❑ eDiscovery
- ❑ Analysis tools
- ❑ Static & dynamic malware analysis
- ❑ Netflow analysis
- ❑ Etc.

Respond

- ❑ IP/domain blocking
- ❑ Endpoint containment
- ❑ Filtering
- ❑ Proxy blocking
- ❑ Etc.

For each tool, identify, discuss, and document the following (if applicable):

1. Using?
2. Integration/automation capability?
3. Priority?
4. Use case management?
5. Maturity of the implementation?
6. Maturity of the usage?

Technology challenges

False positive management

Risk/Threat based prioritization

Cost challenges while increasing visibility

Log collection and integration

Logs normalization

Log storage and capabilities

Reliability

Keeping up to date with new cyber trends

Performance monitoring and optimization

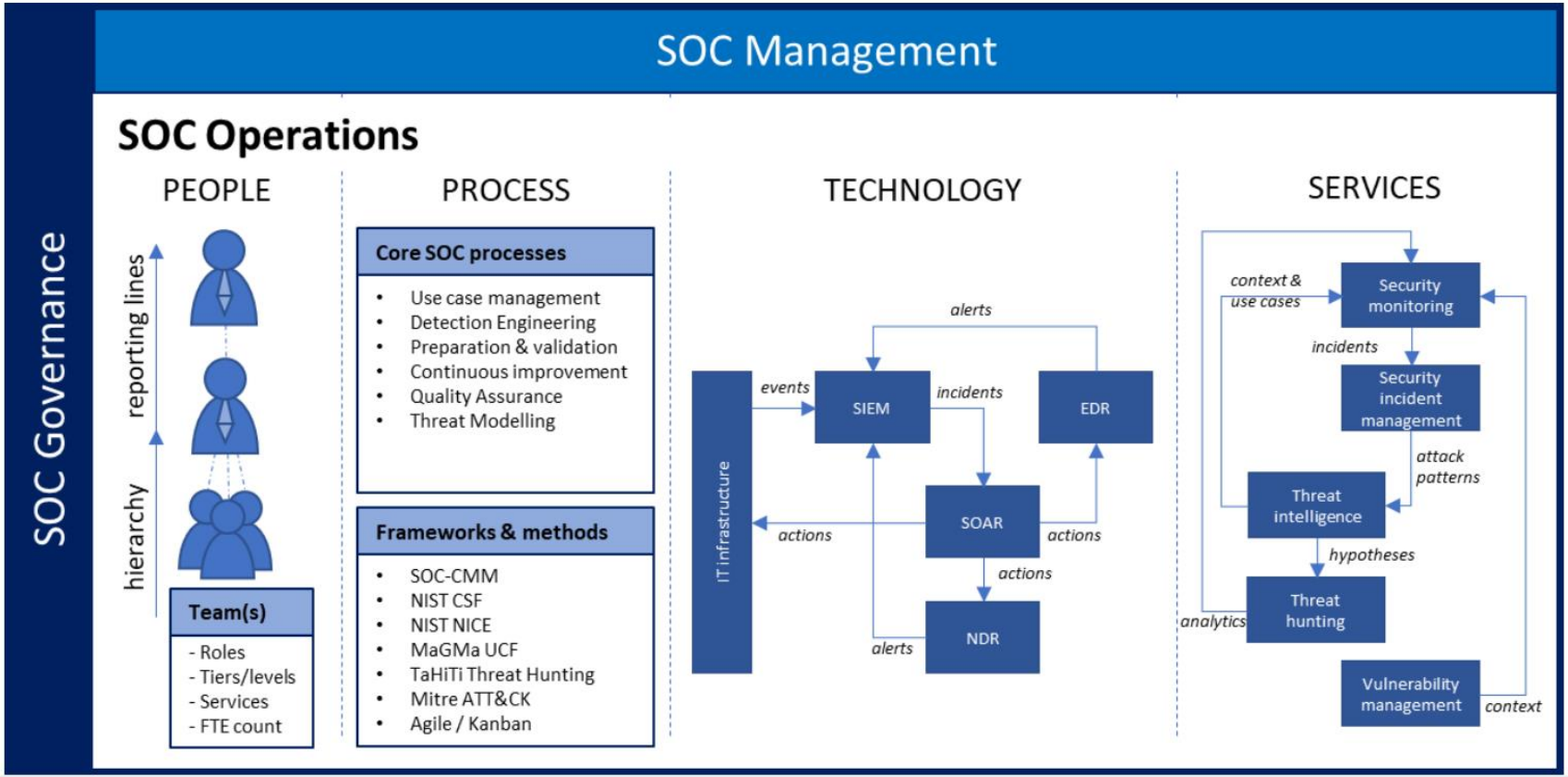
Upgrades and management

Customization and configuration

Services that can be integrated/provided through SOC

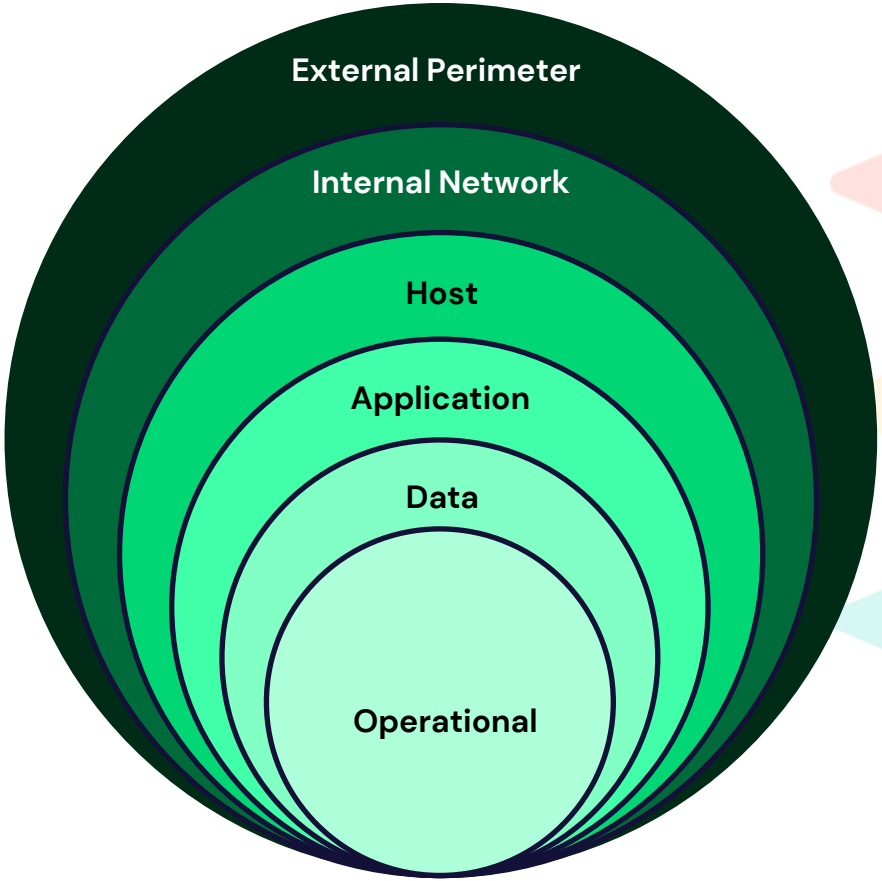
Security Monitoring	Security Incident Management & Response	Security Analytics
Threat Hunting	Threat Intelligence	Vulnerability Management
Log Management	Security Governance	Security Compliance

Putting all together – People > Process > Technology > Service



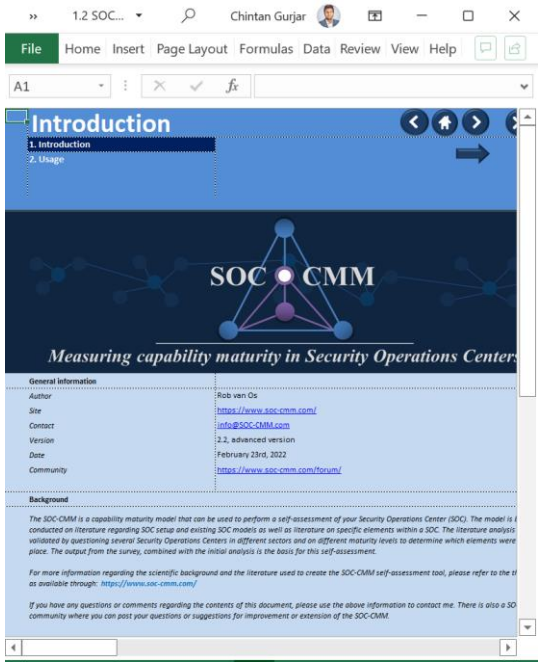
https://www.soc-cmm.com/downloads/SOCTOM%20whitepaper.pdf

SOC should cover layer defense model



1. Define attack possibilities on each layer.
2. Discuss possible attacks/threats on each layer based on the target device.
3. Discuss what devices/solutions can potentially provide log information.
4. Log information in the workbook for later implementation.

Perform SOC Maturity Assessment



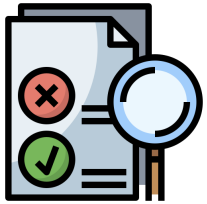
2 SOC-CMM's Maturity Assessment Tool

https://www.soc-cmm.com/

Your feedback is necessary

sarahah.top/u/chintangurjar

Phases of SOC implementation



Phase 1

Assess the current maturity state

Phase 2

Design your target SOC state

Phase 3

Develop an implementation roadmap

Phase 4

Comprehensive reporting

Phase 2

Design your target SOC state

Overview – Design your target state

Activities to be performed

- Now you know your gaps
- Design the ideal target state
- Optimize your security operations people, processes and technologies
- Prioritize your gap initiatives

Results

- A defined security and gap pressure posture
- Identified optimization opportunities
- An ideal target state (where you want to be)
- Formalized security operation SOPs

Benefits

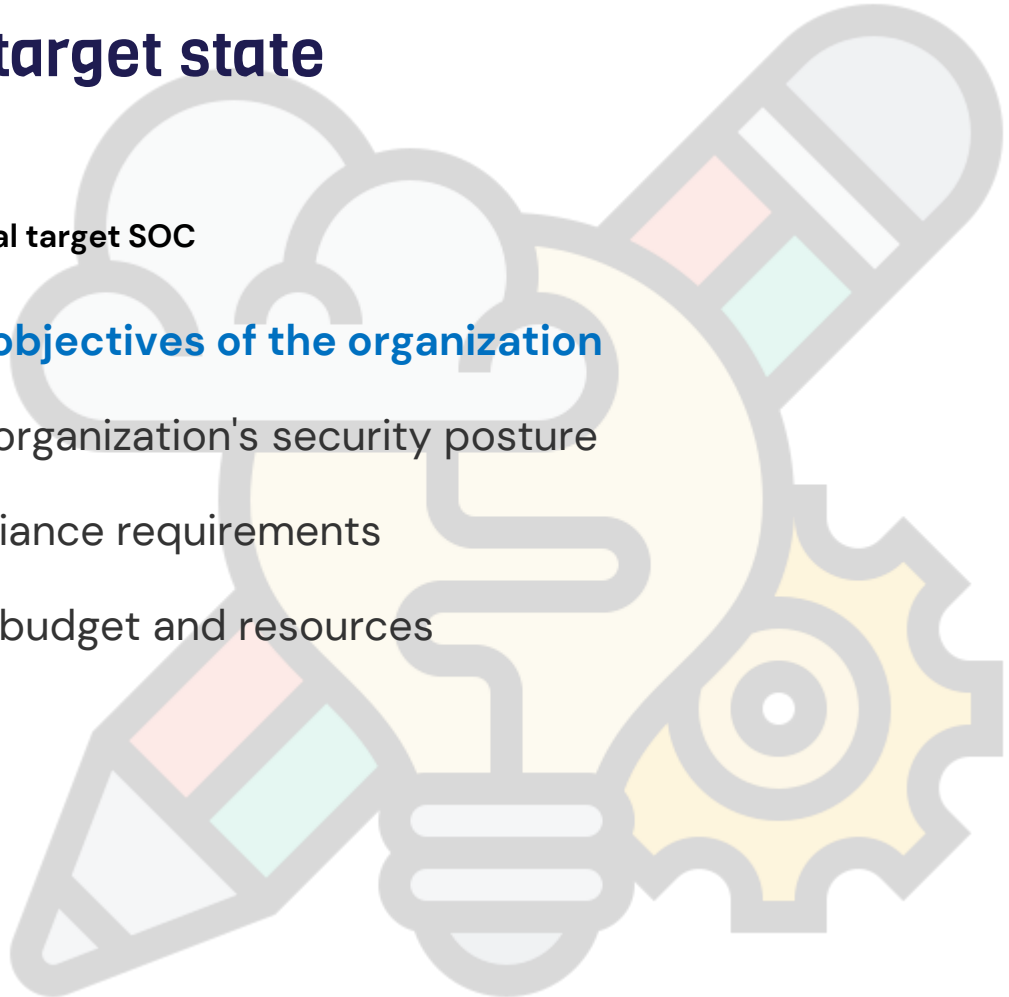
Activity will enable you to:

- Identify planning gaps specific to your organization's threat landscape.
- Formalize the implementation process with an official policy and guide.

Overview – Design your target state

Follow the below process to design your ideal target SOC

1. **Gather the overall goals and objectives of the organization**
2. Know the current state of the organization's security posture
3. Know the organization's compliance requirements
4. Determine your organization's budget and resources
5. Follow industry best practices



Gather the overall goals and objectives of the organization

- Describe the organization's mission, vision, strategies and values.
- Explain how the organization's goals and objectives align with its security operations.
- Include any relevant formulas, methodologies, metrics, compliance (e.g., return on investment, cost-benefit analysis, Business impact analysis) that can help demonstrate the value of the ideal target SOC of the organization that you want to develop.
- When drafting all these, it is important to organize it in a way that will make it easy for the audience to comprehend and follow. Utilize a logical and straightforward structure to arrange the information to ensure maximum clarity and comprehension.

Business requirements & SOC drivers

Business Requirement	SOC Drivers
High-quality customer service	Should focus ensuring the security and reliability of the systems and processes that support customer service.
Become a leader in its industry	Should focus on continually improving the security posture and resilience of the organization to maintain a competitive advantage.
Provide transparency and accountability	Should prioritize transparency in its communication and reporting and accountability in its incident response processes.
Increase revenue	Should focus minimizing the risk of security breaches, downtime that could disrupt business operations and damage the organization's reputation.

Business requirements & SOC drivers cont.

Business Requirement	SOC Drivers
A healthcare organization's mission is to provide high-quality patient care	SOC's goals and objectives should focus on ensuring the security and reliability of the systems and processes that support patient care, such as electronic health records and telemedicine platforms.
A retail company's mission is to offer a wide range of products at competitive prices.	SOC's goals and objectives should focus on protecting the organization's e-commerce platform and customer data to prevent disruptions to online sales and maintain customer trust.
A software company's vision is to become a leader in the industry by offering innovative products and services.	SOC's long-term objectives should focus on continuously improving the security posture and resilience of the organization to protect against emerging threats and maintain a competitive advantage.
A financial services company's vision is to be the preferred choice for customers seeking investment and wealth management services	SOC's long-term objectives should focus on protecting the organization's systems and data from threats such as cyber-attacks and data breaches to maintain customer trust and confidence.

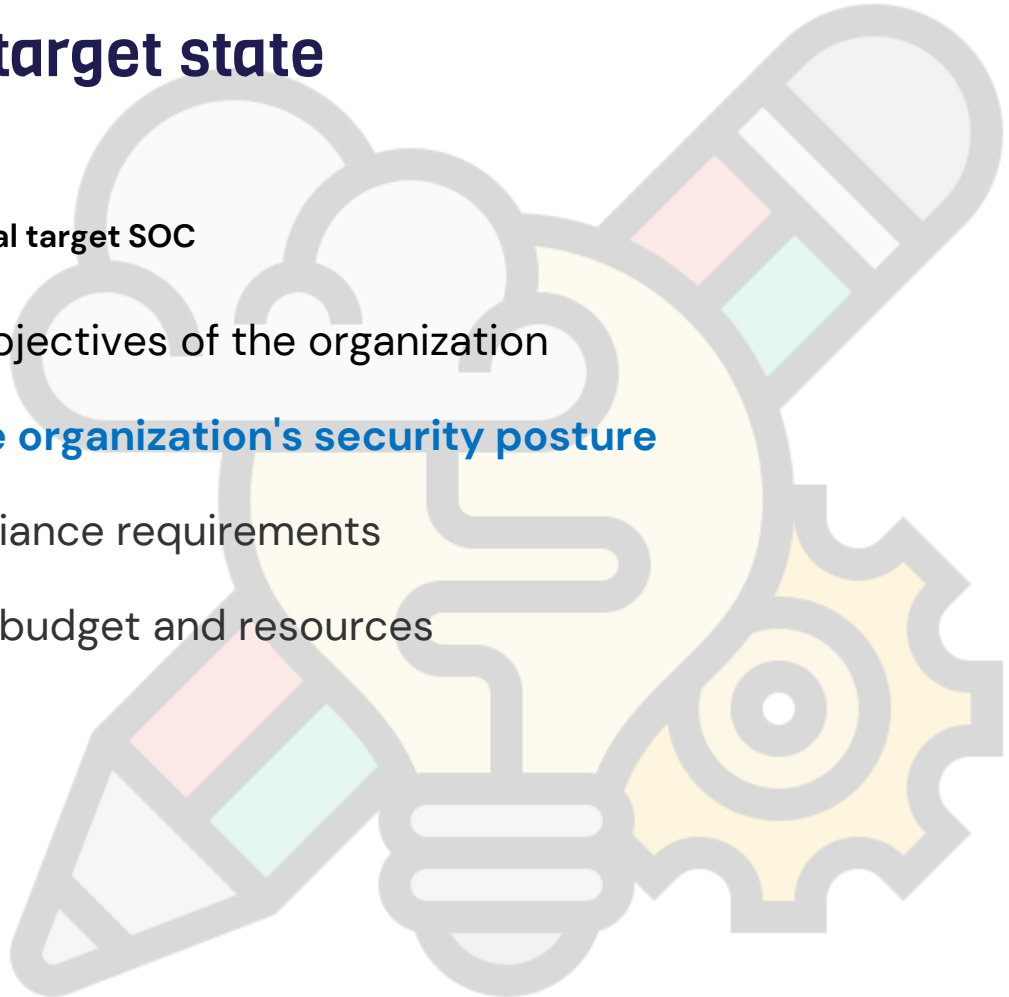
Business requirements & SOC drivers cont.

Business Requirement	SOC Drivers
A nonprofit organization's values include social responsibility and sustainability.	SOC's principles and practices should prioritize environmental sustainability in its operations, such as by implementing energy-efficient security controls and reducing paper consumption.
A government agency's values include transparency and accountability.	SOC's principles and practices should prioritize transparency in its communication and reporting and accountability in its incident response processes.
A manufacturing company's goal is to increase efficiency and reduce costs.	SOC's outcomes should focus on implementing security controls that minimize the risk of disruptions to production and reduce the time and resources required for incident response.
A professional services company's goal is to attract and retain top talent.	SOC's outcomes should focus on implementing security controls that protect the organization's systems and data from threats such as ransomware and data breaches to maintain a positive employee experience and reduce the risk of turnover.

Overview – Design your target state

Follow the below process to design your ideal target SOC

1. Gather the overall goals and objectives of the organization
2. **Know the current state of the organization's security posture**
3. Know the organization's compliance requirements
4. Determine your organization's budget and resources
5. Follow industry best practices



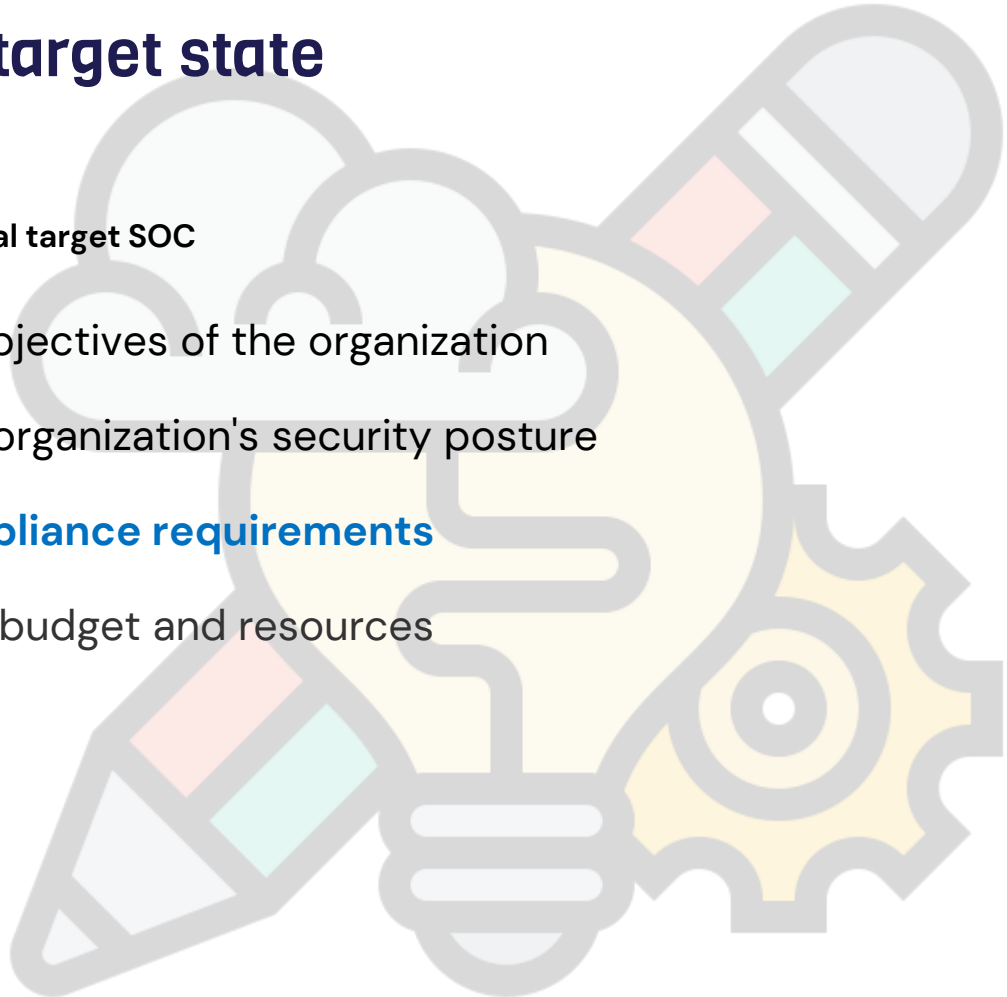
Know the current state of the organization's security posture

- This has been already completed on the slide no. **27**.

Overview – Design your target state

Follow the below process to design your ideal target SOC

1. Gather the overall goals and objectives of the organization
2. Know the current state of the organization's security posture
3. **Know the organization's compliance requirements**
4. Determine your organization's budget and resources
5. Follow industry best practices



Know the organization's regulatory and compliance requirements

- **Data protection laws**: such as the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore.
- **Cybersecurity standards:** such as the Payment Card Industry Data Security Standard (PCI DSS) for organizations that handle credit card transactions, the National Institute of Standards and Technology (NIST) Cybersecurity Framework for federal agencies in the United States, and the Cybersecurity Law in China.
- **Industry-specific regulations:** such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare organizations in the United States, the Gramm-Leach-Bliley Act (GLBA) for financial institutions in the United States, and the Basel III regulatory framework for banks internationally.
- **Information security management systems:** such as the ISO/IEC 27001 standard for information security management systems.
- **Network and infrastructure security:** such as the Federal Information Processing Standard (FIPS) 140-2 for cryptographic modules and the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Assessment Tool (CMAT) for federal agencies in the United States.

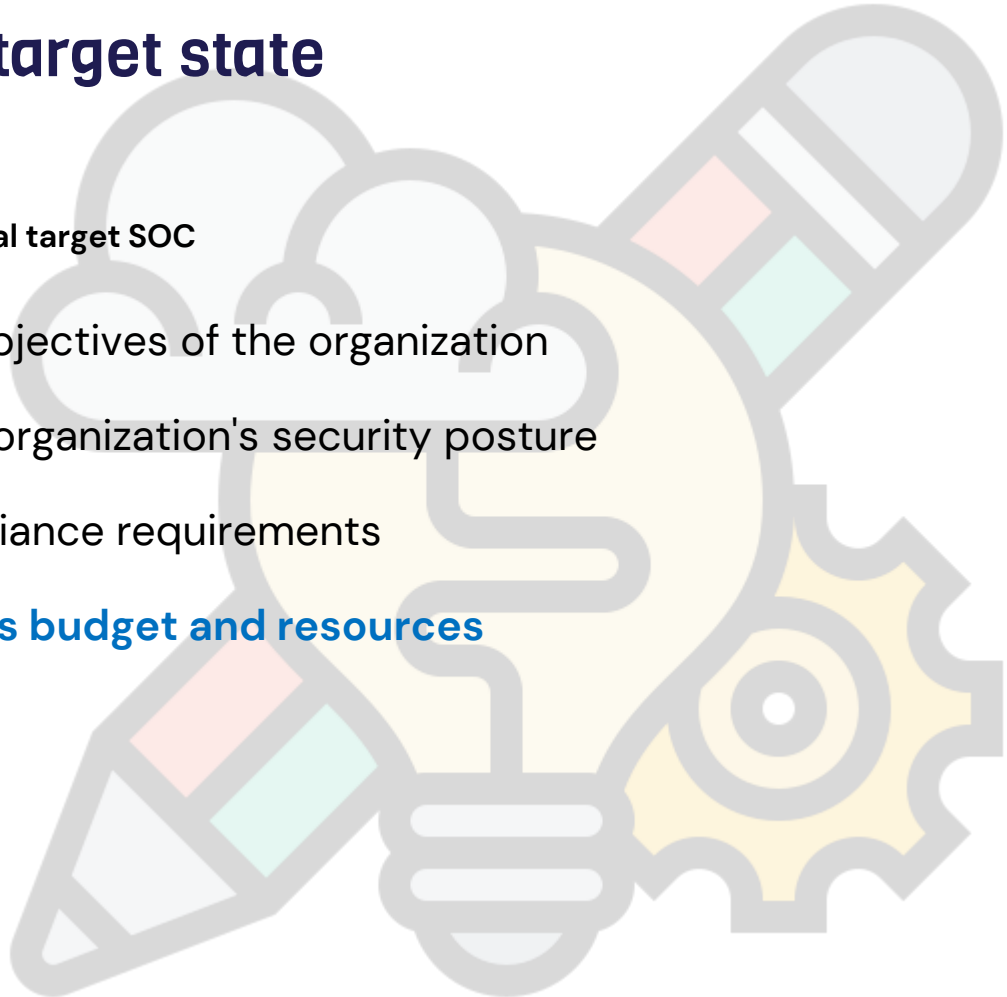
Know the organization's regulatory and compliance requirements

- **Endpoint security:** such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) for federal agencies in the United States.
- **Cloud security:** such as the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) and the ISO/IEC 27017 standard for cloud security.
- **Application security:** such as the Open Web Application Security Project (OWASP) Top Ten and the ISO/IEC 27034 standard for application security.
- **Physical security:** such as the National Institute of Standards and Technology (NIST) Physical Security Handbook and the International Organization for Standardization (ISO) 7498-2 standard for physical security.
- **Cloud security:** such as the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) and the ISO/IEC 27017 standard for cloud security.
- **Application security:** such as the Open Web Application Security Project (OWASP) Top Ten and the ISO/IEC 27034 standard for application security.
- **Physical security**: such as the National Institute of Standards and Technology (NIST) Physical Security Handbook and the International Organization for Standardization (ISO) 7498-2 standard for physical security.

Overview – Design your target state

Follow the below process to design your ideal target SOC

1. Gather the overall goals and objectives of the organization
2. Know the current state of the organization's security posture
3. Know the organization's compliance requirements
4. **Determine your organization's budget and resources**
5. Follow industry best practices



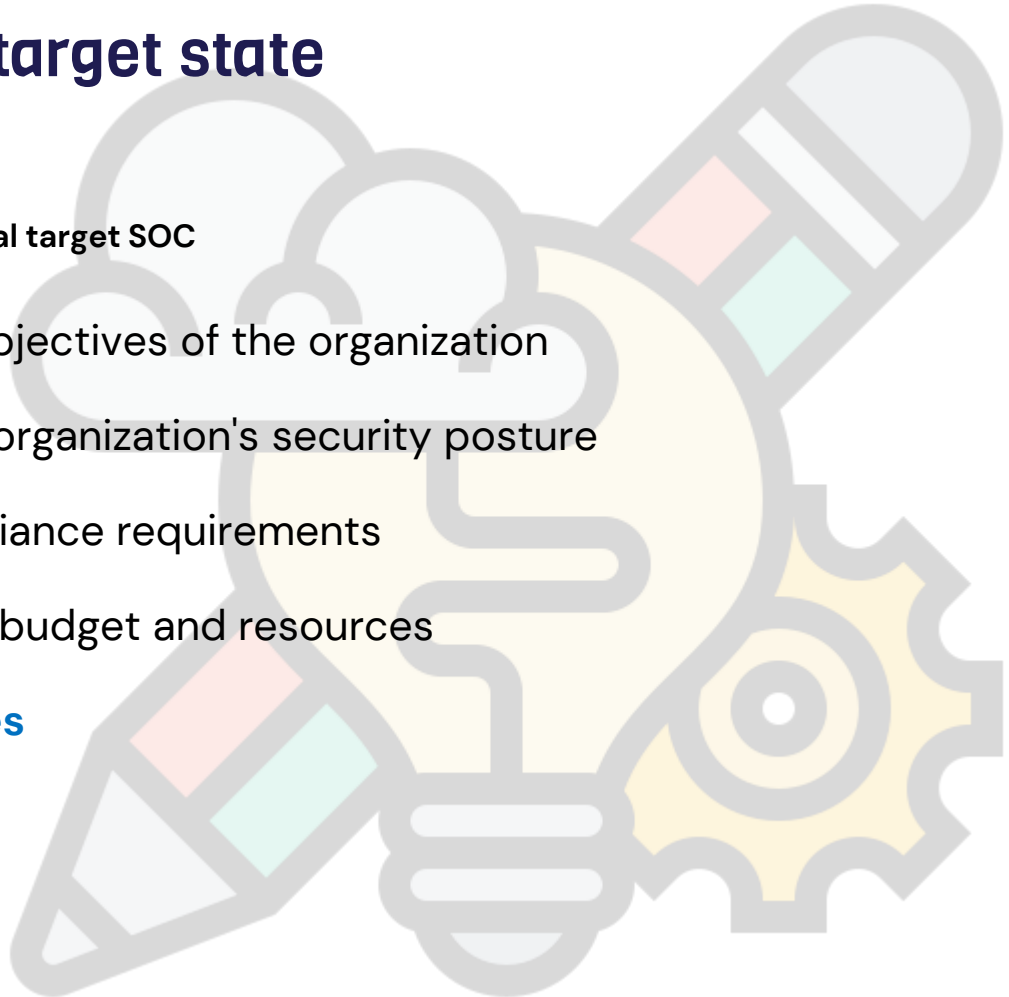
Determine your organization's budget and resources

- Describe the organization’s resources available to allocate to its security operations, including people, tools, infrastructure, support and maintenance.
- Explain how these resources align with the organization's goals and objectives or business’s requirements.
- Identify any areas where additional resources may be needed to support the target SOC.
- Identify how existing resources can be utilized with time allocation, priority setting, cross-team training and functioning.

Overview – Design your target state

Follow the below process to design your ideal target SOC

1. Gather the overall goals and objectives of the organization
2. Know the current state of the organization's security posture
3. Know the organization's compliance requirements
4. Determine your organization's budget and resources
5. **Follow industry best practices**



All the SIEM best practicies you need so far

- ❑ Developing a clear security strategy
- ❑ Implementing robust security monitoring and detection capabilities
- ❑ Establishing effective communication and collaboration
- ❑ Ensuring the SOC team has the necessary skills and resources
- ❑ Establishing regular testing and training
- ❑ Providing adequate staffing and coverage
- ❑ Ensuring that all security-related information is documented
- ❑ Continuous improvement through process engineering
- ❑ Establishing clear roles and responsibilities
- ❑ Ensuring that the SOC has the necessary tools and technologies
- ❑ Establishing incident response protocols
- ❑ Measuring and reporting on the effectiveness of the SOC
- ❑ Implementing a security information and event management (SIEM) system
- ❑ Maintaining up-to-date knowledge of the threat landscape
- ❑ Establishing strong partnerships with cybersecurity vendors
- ❑ Providing regular training and education to the SOC team
- ❑ Define the scope and purpose of the SOC
- ❑ Implement a centralized management and monitoring system
- ❑ Ensure compliance with relevant regulations and standards
- ❑ Foster a culture of security

Consider the following when refining or reconfiguring security operations

People

- ❑ Will staffing levels be altered?
- ❑ Will certain individuals be assigned to different job titles or roles?
- ❑ How will personnel be organized in the new structure?
- ❑ Is relocation to one location necessary, and will this be feasible?
- ❑ Will reporting relationships be adjusted?
- ❑ How can performance measurements be unified across teams and departments to ensure alignment with the business objectives?
- ❑ Will career paths be affected, and if so, how?

Process

- ❑ What processes need to be put in place to enable knowledge sharing so that all analysts can quickly access known errors and resolve problems?
- ❑ How can procedures be documented in a way that will ensure proper escalation of processes?
- ❑ Are any changes needed to the ticket classification and prioritization schemes?
- ❑ What is the best way for tickets to be submitted?
- ❑ How will resolution be defined, and how will users be notified of the resolution?

Technology

- ❑ Is the current tool customizable?
- ❑ Can it be integrated with necessary non-IT systems?
- ❑ Does the tool have the capability to accommodate a bigger user base?
- ❑ Will the tool cover all the areas, departments, and technologies required after consolidation?
- ❑ What measures must be taken to migrate existing data to the new tool?
- ❑ What implementation or configuration expenses should be anticipated?
- ❑ What kind of training is essential for proper usage of the tool?
- ❑ What other new tools and technologies will be necessary to sustain the optimized state of security operations?

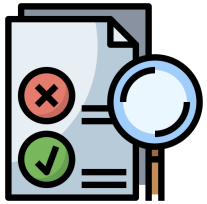
Optimize SOC Technically

- ❑ Provide **centralized dashboard** with threat analytics data.
- ❑ **Automate L1 tasks** (collection, parsing, storage, triage, ticket creation, automated sandboxing, escalation etc.)
- ❑ Only **add necessary logs** and don't add so many logs to increase visibility without use case management and quality control checking of logs
- ❑ Work with use **case management** only
- ❑ **Use tags** everywhere for asset, data, owner and location classification
- ❑ **Enable SIEM workflow** to automate complex requirements write playbooks
- ❑ **Tune platforms, logs,** any other data that gives actionable insights
- ❑ Define **service level agreements (SLAs)** with customers or internal stakeholders
- ❑ **Automate operational/'respond' tasks**
  - ❑ Cross product orchestration/integration
  - ❑ Delete file
  - ❑ Network isolation
  - ❑ Kill process
  - ❑ Reboot/Shutdown
  - ❑ Start/Stop windows services

Your feedback is necessary

sarahah.top/u/chintangurjar

Phases of SOC implementation



Phase 1

Assess your current state

Phase 2

Design your target state

Phase 3

Develop an implementation roadmap

Phase 4

Provide comprehensive reporting

Phase 3

Develop an implementation roadmap

Overview – Develop an implementation roadmap

Activities to be performed

- Present your argument to management in order to create an effective sourcing strategy.
- Assign duties and duties to the implementation plan
- Develop a comprehensive program to measure progress.

Outcomes

- Establishing a formal agreement with stakeholders to secure their backing
- Creating a comprehensive approach to acquiring materials and resources
- Allocating specific roles and tasks to personnel involved in the project
- Producing a timeline with the most important goals and objectives listed first
- Developing a system to track progress and make necessary adjustments

Key Benefits

- Support your decision to implement a security operations program with the approval of stakeholders.
- Identify the appropriate sourcing strategy and subsequent SLAs.
- Formalize the implementation process with an official and prioritized roadmap.

Create RACI Matrix for SOC initiatives

A RACI matrix is a tool used in project management to assign roles and responsibilities to team members for the completion of specific tasks or objectives. It stands for Responsible, Accountable, Consulted, and Informed.

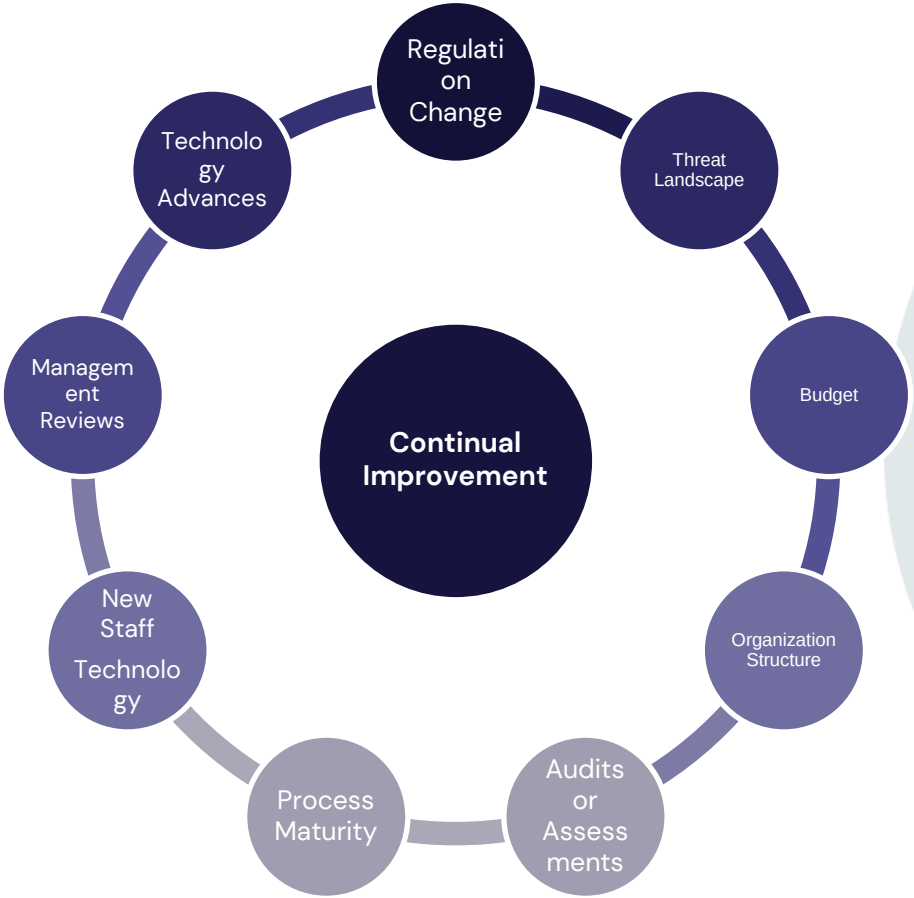
Define all the SOC roles and responsibilities, along with specific initiatives, objectives, goals, tasks and log them into RACI matrix.

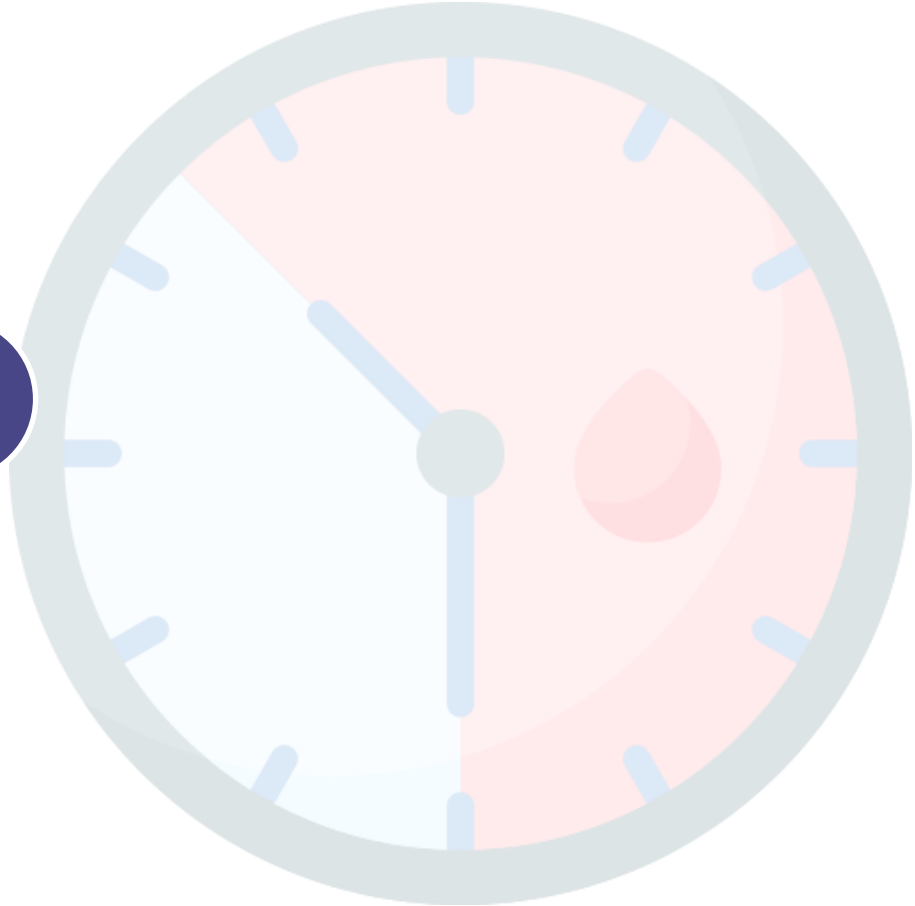
Post this, use any project charter document to formalize everything.

Identify stakeholders that are:

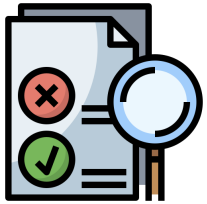
- **Responsible:** This person is responsible for completing the task. There can be multiple people with this role for a single task.
- **Accountable:** This person is ultimately accountable for the successful completion of the task. There should only be one person with this role for each task.
- **Consulted:** These are the people who need to be consulted before the task can be completed. They may have expertise or information that is necessary for the task to be done effectively.
- **Informed:** These are the people who need to be kept informed about the task, but are not directly involved in its completion.

Identify drivers of continual improvements (Revisit 6 month)





Phases of SOC implementation



Phase 1

Assess your current state

Phase 2

Design your target state

Phase 3

Develop an implementation roadmap

Phase 4

Provide comprehensive reporting

Phase 4

Provide comprehensive reporting

Factors that can change the way you report

Type of audience
(Strategic, Operational, Technical)

Type of Service
(In-house SOC, MSSP)

Type of Activities
(SOC is big, what are you doing?)

Type of company
(Industry, Consulting)

Type of project
(One off, Short term, Yearly, Compliance requirement)

Project duration
(Yearly, Reoccurring, Short term, Long term)

Metrics agreed upon
(What you can do vs. what they want)

Frequency of the reports
(Daily, Weekly, Monthly, Quarterly, Yearly)

Format of Report
(PPT, Excel, Word, Automated through Portal)

Compliance
(What compliance is chosen)

SOC Reporting by Audience

For the strategic audience:

- An overview of the key security risks and challenges facing the client, and how the SOC is addressing these risks and challenges.
- A summary of the key security metrics and performance indicators for the quarter, such as the number and severity of security incidents, the effectiveness of security controls, and the level of compliance with security standards and regulations.
- An overview of the key security trends and developments, such as new technologies, threats, and regulations, and how they are affecting the client's security posture.

For the operational audience:

- A detailed description of the security services provided by the SOC during the quarter, including the scope of the services, the key activities and tasks performed, and the outcomes achieved.
- An overview of the security operations and processes in place, and how they are being used to detect, investigate, and respond to security incidents.
- A description of the security tools and technologies used by the SOC, and how they are being used to monitor and protect the client's systems and networks.

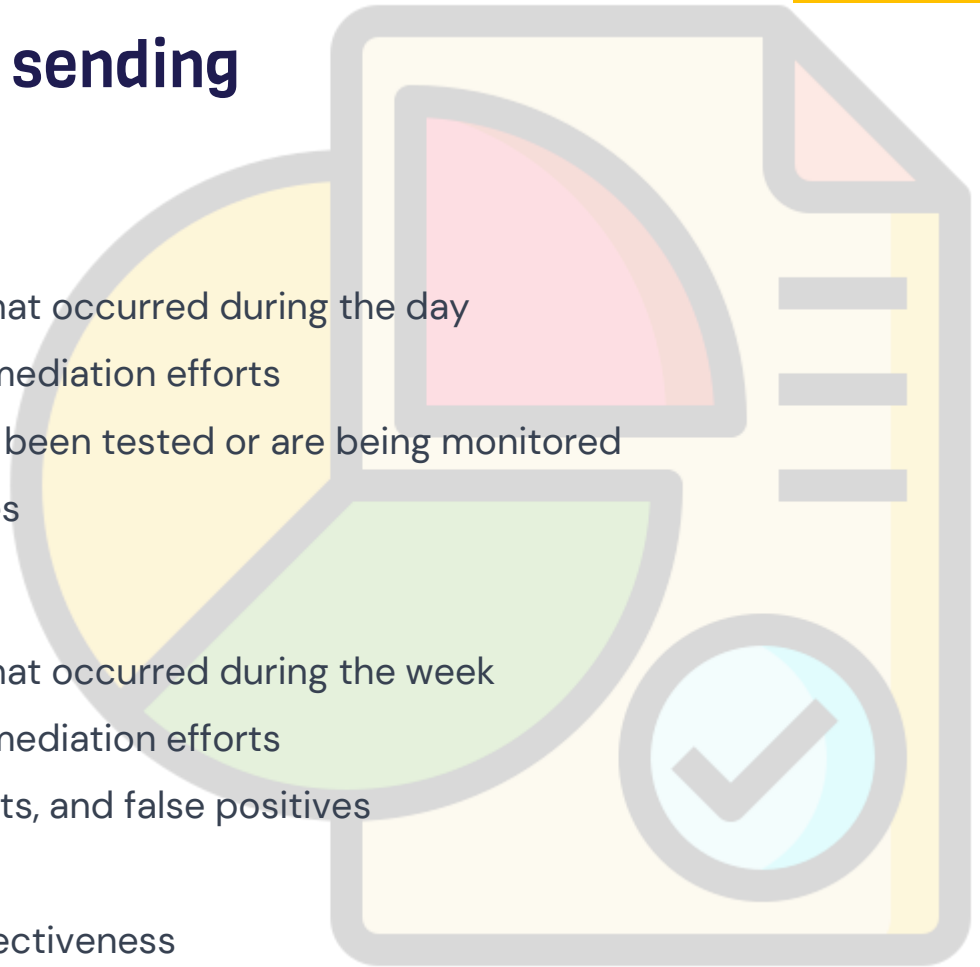
For the technical audience:

- A detailed description of the security controls and monitoring systems in place, including the technologies used and the specific security policies and rules that are being enforced.
- A description of any security vulnerabilities or threats that were identified during the quarter, and the actions taken to address them.
- A summary of any security updates, patches, or other changes made to the client's systems and networks during the quarter, and an assessment of their impact on the security posture.

Reporting by Activities

- Summary of all security incidents and response activities.
- Summary of risk assessment and vulnerability scans.
- Summary of security policy and procedure enforcement.
- Summary of patch management and application updates.
- Summary of network and system monitoring activities.
- Summary of user training and awareness activities.
- Summary of user access control and privileges.
- Summary of security architecture status and security events.
- Summary of security posture and performance metrics.
- Summary of security incident management process.
- Summary of security incident response and remediation activities.
- Summary of security audits and compliance activities.
- Summary of third-party vendor assessment and risk management.
- Summary of physical security measures and access control.
- Summary of incident response and forensics activities.

Reporting by frequency of sending



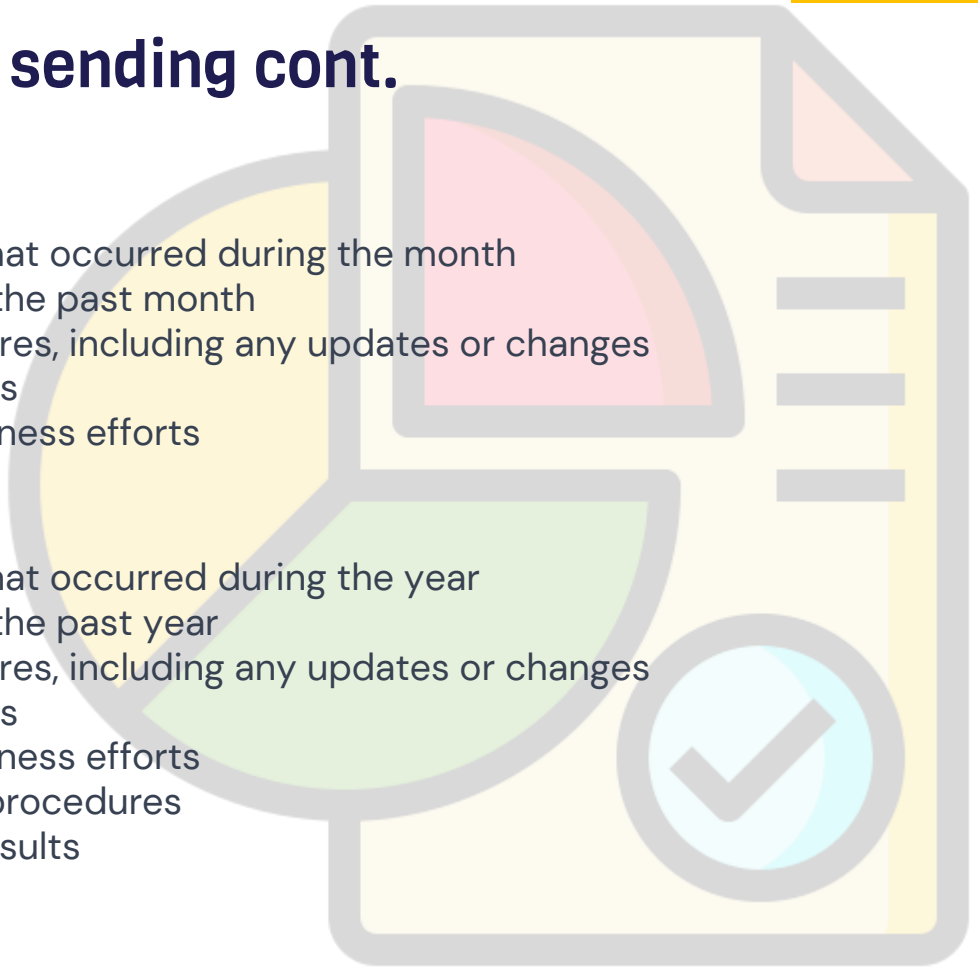
Daily reports

- Summary of key events and incidents that occurred during the day
- Status of ongoing investigations and remediation efforts
- Summary of security controls that have been tested or are being monitored
- Status of security projects and initiatives

Weekly reports

- Summary of key events and incidents that occurred during the week
- Status of ongoing investigations and remediation efforts
- Metrics on the number of alerts, incidents, and false positives
- Trends in attack types and vectors
- Status of security controls and their effectiveness

Reporting by frequency of sending cont.



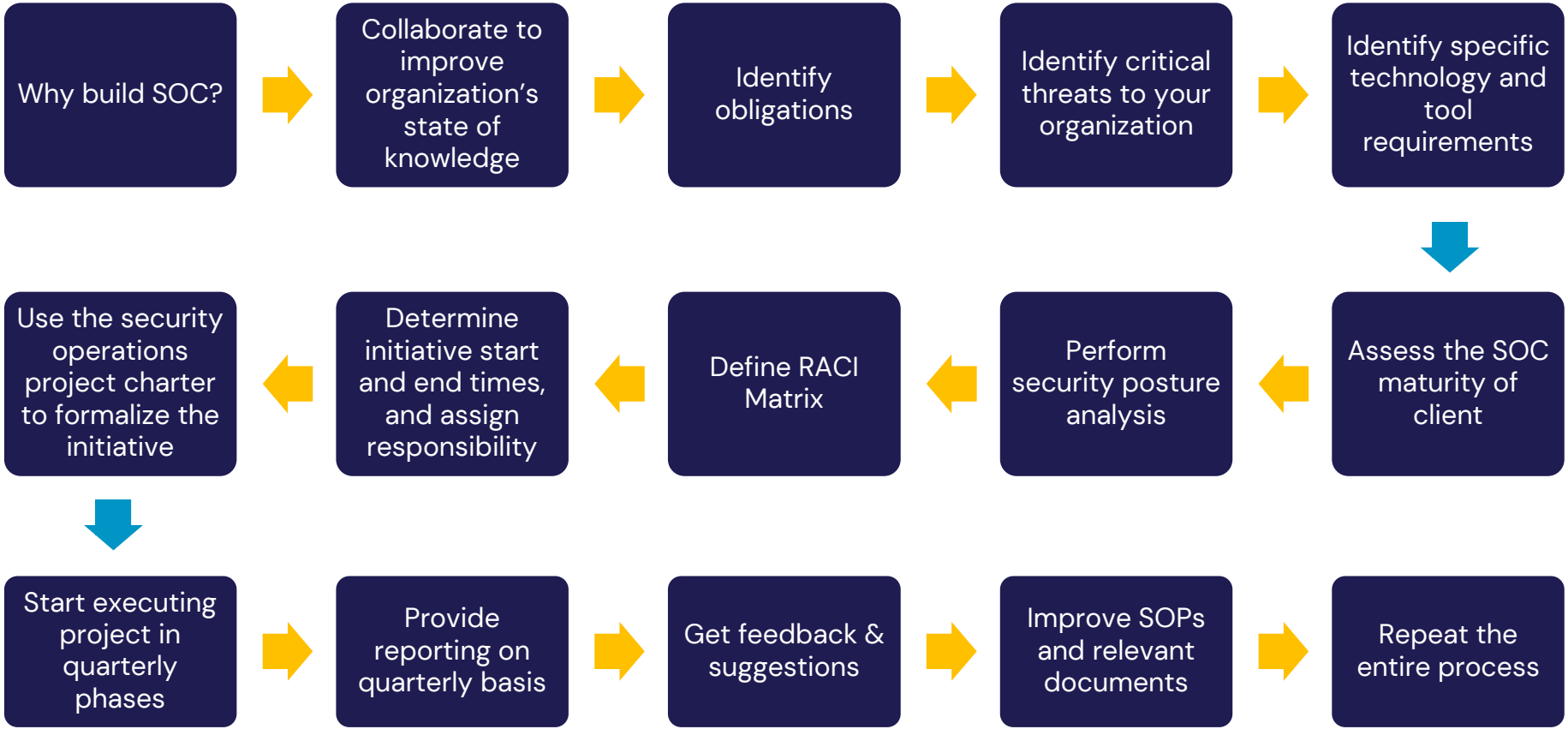
Monthly reports

- Summary of key events and incidents that occurred during the month
- Trend analysis of security metrics over the past month
- Review of security policies and procedures, including any updates or changes
- Status of security projects and initiatives
- Summary of security training and awareness efforts

Yearly reports

- Summary of key events and incidents that occurred during the year
- Trend analysis of security metrics over the past year
- Review of security policies and procedures, including any updates or changes
- Status of security projects and initiatives
- Summary of security training and awareness efforts
- Review of incident response plans and procedures
- Summary of security risk assessment results

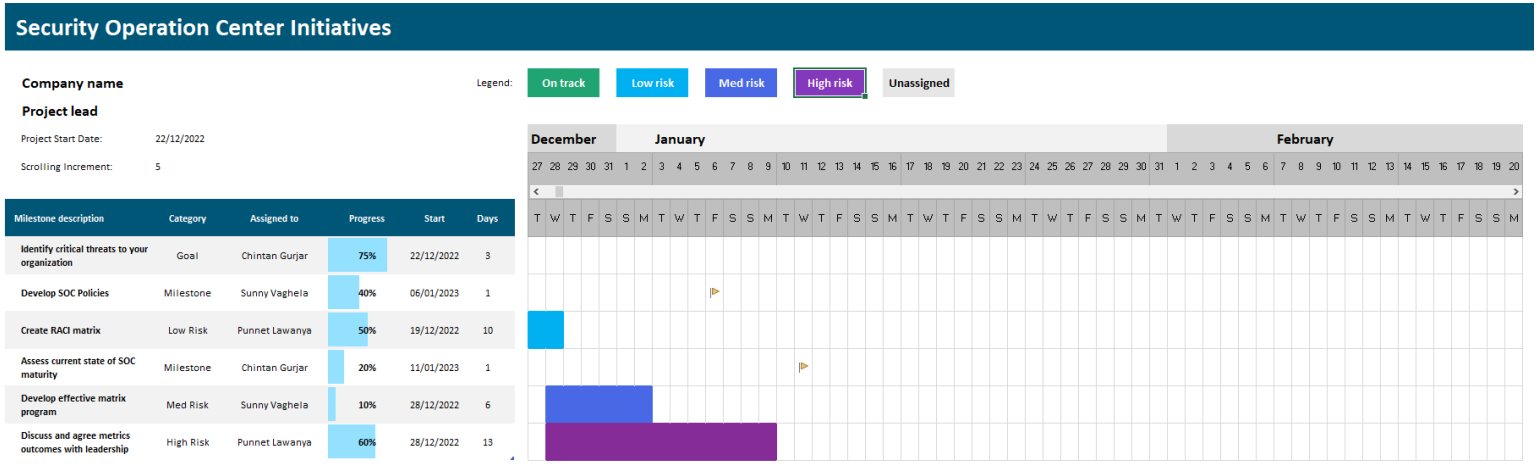
Project Execution Summary



Define initiative start and end date with responsibilities

Questions to think about:

- Does this roadmap align with the goals of our organization?
- Are we dedicating adequate resources to each quarter?
- Is the proposed implementation the most practical option?
- Should any initiatives be rescheduled for a different quarter due to resource constraints?
- Are there any major organizational shifts planned in the near future that could affect the project?




Q&A

Your feedback is necessary

sarahah.top/u/chintangurjar

Contact Me:

chintangurjar@outlook.com

@iamthefrogy

Chintan Gurjar