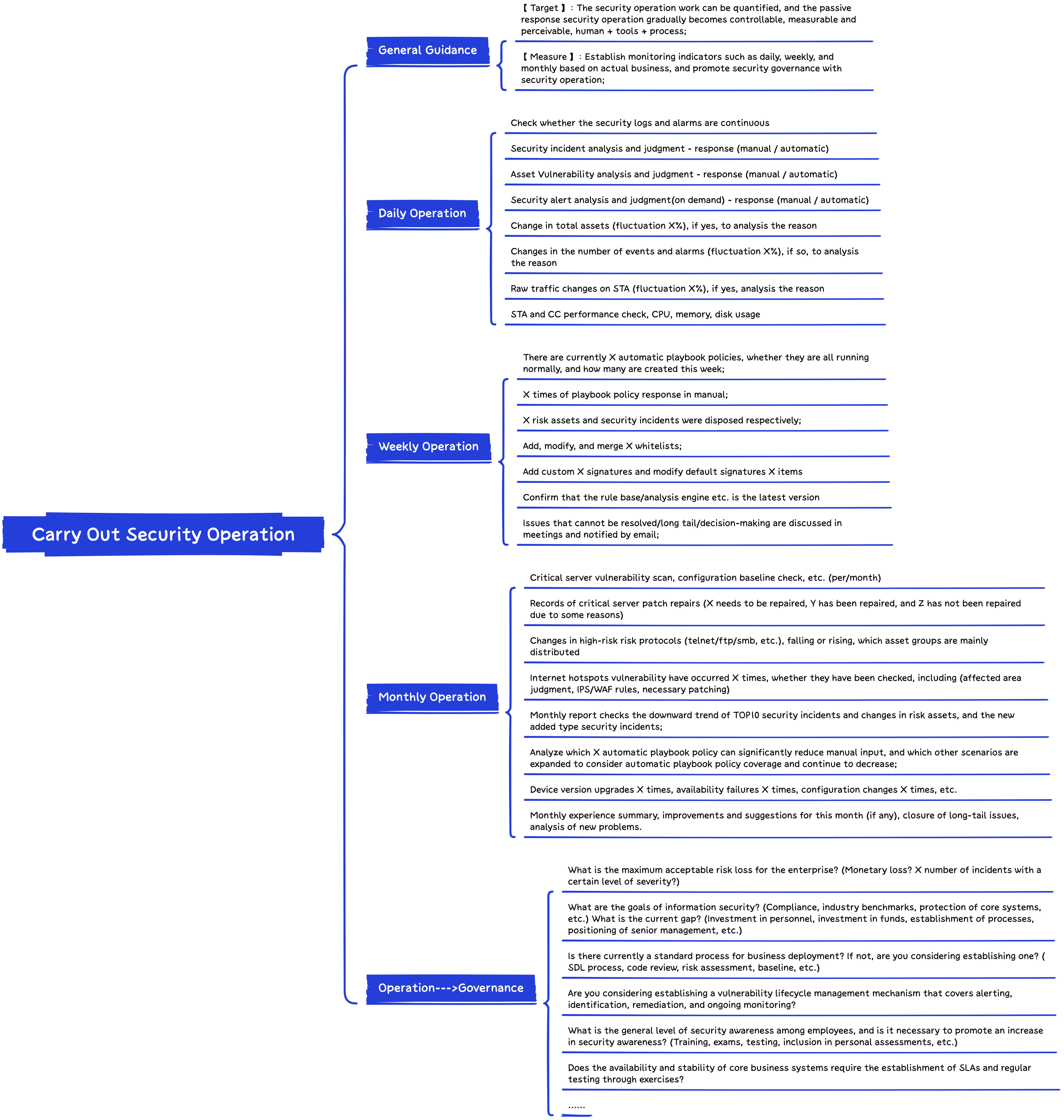

Carry Out Security Operation

General Guidance

- 【 Target 】：The security operation work can be quantified, and the passive response security operation gradually becomes controllable, measurable and perceivable, human + tools + process;
- 【 Measure 】：Establish monitoring indicators such as daily, weekly, and monthly based on actual business, and promote security governance with security operation;

Daily Operation

- Check whether the security logs and alarms are continuous
- Security incident analysis and judgment - response (manual / automatic)
- Asset Vulnerability analysis and judgment - response (manual / automatic)
- Security alert analysis and judgment(on demand) - response (manual / automatic)
- Change in total assets (fluctuation X%), if yes, to analysis the reason
- Changes in the number of events and alarms (fluctuation X%), if so, to analysis the reason
- Raw traffic changes on STA (fluctuation X%), if yes, analysis the reason
- STA and CC performance check, CPU, memory, disk usage

Weekly Operation

- There are currently X automatic playbook policies, whether they are all running normally, and how many are created this week;
- X times of playbook policy response in manual;
- X risk assets and security incidents were disposed respectively;
- Add, modify, and merge X whitelists;
- Add custom X signatures and modify default signatures X items
- Confirm that the rule base/analysis engine etc. is the latest version
- Issues that cannot be resolved/long tail/decision-making are discussed in meetings and notified by email;

Monthly Operation

- Critical server vulnerability scan, configuration baseline check, etc. (per/month)
- Records of critical server patch repairs (X needs to be repaired, Y has been repaired, and Z has not been repaired due to some reasons)
- Changes in high-risk risk protocols (telnet/ftp/smb, etc.), falling or rising, which asset groups are mainly distributed
- Internet hotspots vulnerability have occurred X times, whether they have been checked, including (affected area judgment, IPS/WAF rules, necessary patching)
- Monthly report checks the downward trend of TOP10 security incidents and changes in risk assets, and the new added type security incidents;
- Analyze which X automatic playbook policy can significantly reduce manual input, and which other scenarios are expanded to consider automatic playbook policy coverage and continue to decrease;
- Device version upgrades X times, availability failures X times, configuration changes X times, etc.
- Monthly experience summary, improvements and suggestions for this month (if any), closure of long-tail issues, analysis of new problems.

Operation--->Governance

- What is the maximum acceptable risk loss for the enterprise? (Monetary loss? X number of incidents with a certain level of severity?)
- What are the goals of information security? (Compliance, industry benchmarks, protection of core systems, etc.) What is the current gap? (Investment in personnel, investment in funds, establishment of processes, positioning of senior management, etc.)
- Is there currently a standard process for business deployment? If not, are you considering establishing one? (SDL process, code review, risk assessment, baseline, etc.)
- Are you considering establishing a vulnerability lifecycle management mechanism that covers alerting, identification, remediation, and ongoing monitoring?
- What is the general level of security awareness among employees, and is it necessary to promote an increase in security awareness? (Training, exams, testing, inclusion in personal assessments, etc.)
- Does the availability and stability of core business systems require the establishment of SLAs and regular testing through exercises?
- ......