SANS MANAGEMENT

CYBER LEADER

CURRICULUM

Get the right training to build and lead a world-class security team.

FOUNDATIONAL

MGT512
SANS Security Leadership Essentials for Managers with Knowledge Compression™
GSLC

MGT414
SANS Training Program for CISSP® Certification
GISP

SEC566
Implementing and Auditing the Critical Security Controls – In-Depth
GCCC

MGT525
IT Project Management, Effective Communication, and PMP® Exam Prep
GCPM

CORE

MGT514
IT Security Strategic Planning, Policy, and Leadership

MGT415
A Practical Introduction to Cybersecurity Risk Management

NEW!
MGT517
Managing Security Operations: Detection, Response, and Intelligence

LEG523
Law of Data Security and Investigations
GLEG

SPECIALIZATION

AUD507
Auditing & Monitoring Networks, Perimeters, and Systems
GSNA

MGT433
Securing the Human: How to Build, Maintain, and Measure a High-Impact Awareness Program

MGT305
Technical Communication and Presentation Skills for Security Professionals

SANS

Security Leadership

POSTER

CISO Mind Map

Version 1.0

AND

Security Operations Center (SOC) Essential Functions

For Cyber Leaders of Today and Tomorrow

sans.org/curricula/management

MGT-PSTR-CISO/SOC-0217-v2

CISO MIND MAP v. 1.0

Security Operations

- □ Prevention
  - Data Protection
    - Encryption, PKI, TLS
    - Data Loss Prevention (DLP)
    - Email Security
  - Network Security
    - Firewall, IDS/IPS, Proxy Filtering
    - VPN, Security Gateway
    - DDoS Protection
  - Application Security
    - Threat Modeling
    - Design Review
    - Secure Coding
    - Static Analysis
    - Web App Scanning
    - WAF, RASP
  - Endpoint Security
    - Antivirus, Anti-malware
    - HIDS/HIPS, FIM
    - App Whitelisting
  - Secure Configurations
  - Active Defense
  - Patching
- □ Detection
  - Log Management/SIEM
  - Continuous Monitoring
  - Network Security Monitoring
  - NetFlow Analysis
  - Advanced Analytics
  - Threat Hunting
  - Penetration Testing
  - Red Team
  - Vulnerability Scanning
  - Human Sensor
  - Data Loss Prevention (DLP)
  - Security Operations Center (SOC)
  - Threat Intelligence
  - Threat Information Sharing
  - Industry Partnerships
- □ Response
  - Incident Handling Plan
  - Breach Preparation
  - Tabletop Exercises
  - Forensic Analysis
  - Crisis Management
  - Breach Communications

Legal and Regulatory

- □ Compliance
  - PCI
  - SOX
  - HIPAA
  - FFIEC, CAT
  - FERPA
  - NERC CIP
  - NIST SP 800-37 and 800-53
- □ Privacy
  - Privacy Shield
  - EU GDPR
- □ Audit
  - SSAE 16
  - SOC 2
  - ISO 27001
  - FISMA and FedRAMP
  - NIST SP 800-53A
  - COSO
- □ Investigations
  - eDiscovery
  - Forensics
- □ Intellectual Property Protection
- □ Contract Review
- □ Customer Requirements
- □ Lawsuit Risk

Business Enablement

- □ Product Security
  - Secure DevOps
  - Secure Development Lifecycle
  - Bug Bounties
  - Web, Mobile, Cloud AppSec
- □ Cloud Computing
  - Cloud Security Architecture
  - Cloud Guidelines
- □ Mobile
  - Bring Your Own Device (BYOD)
  - Mobile Policy
- □ Emerging Technologies
  - Internet of Things (IoT)
  - Augmented Reality (AR)
  - Virtual Reality (VR)
- □ Mergers and Acquisitions
  - Security Due Diligence

CYBER LEADER

Identity and Access Management

- □ Provisioning/Deprovisioning
- □ Single Sign On (SSO)
- □ Federated Single Sign On (FSSO)
- □ Multi-Factor Authentication
- □ Role-Based Access Control (RBAC)
- □ Identity Store (LDAP, ActiveDirectory)

Risk Management

- □ Risk Management Frameworks
- □ Risk Assessment Methodology
- □ Business Impact Analysis
- □ Risk Assessment Process
- □ Risk Analysis and Quantification
- □ Security Awareness
- □ Vulnerability Management
- □ Vendor Risk Management
- □ Physical Security
- □ Disaster Recovery (DR)
- □ Business Continuity Planning
- □ Policies and Procedures
- □ Risk Treatment
  - Mitigation Planning, Verification
  - Remediation, Cyber Insurance

Governance

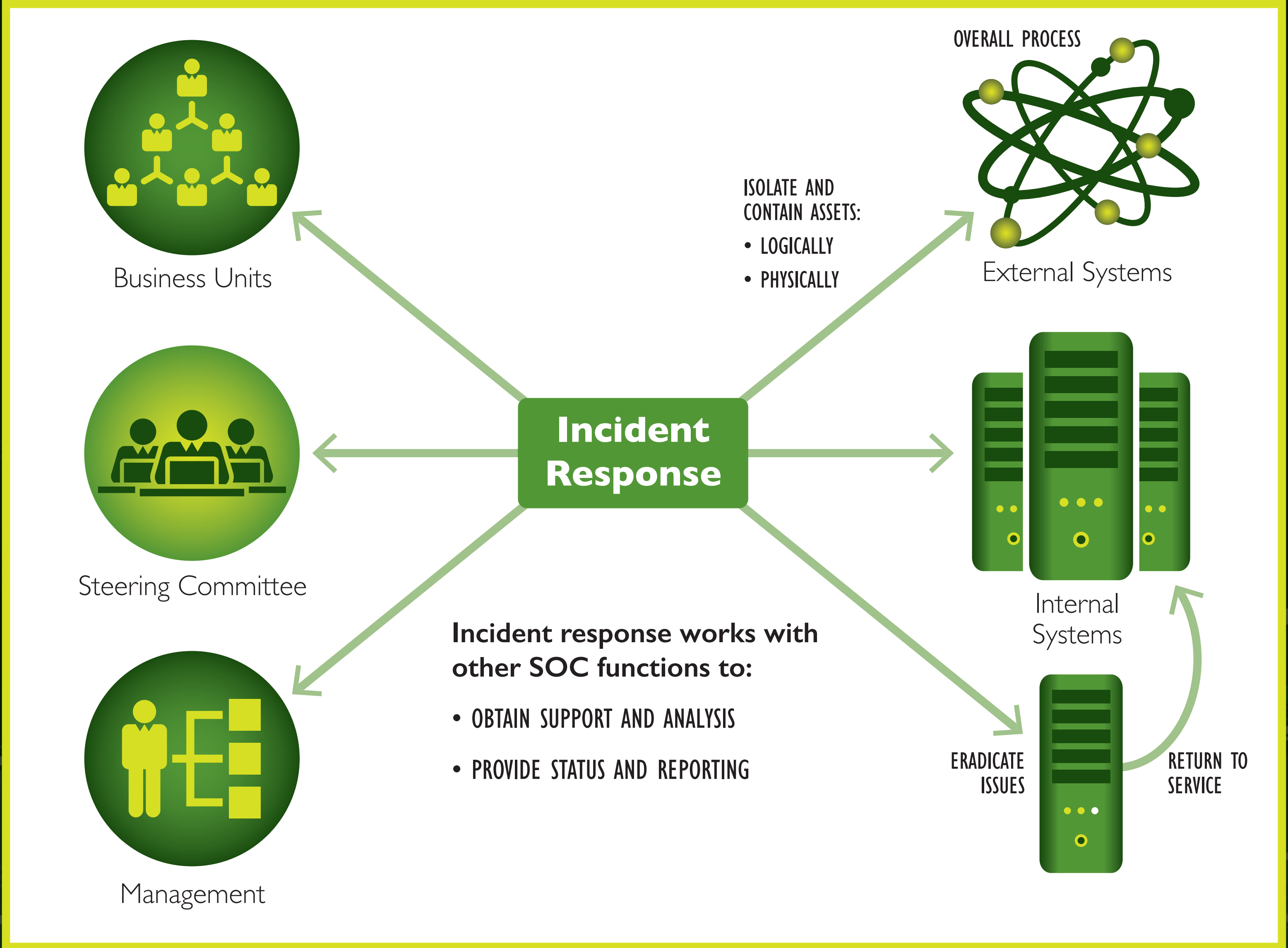
- □ Strategy
- □ Business Alignment
- □ Risk Management
- □ Program Framework
  - NIST CSF
  - ISO 27000
- □ Control Frameworks
  - NIST 800-53
  - Critical Security Controls (CSC)
- □ Program Structure
- □ Program Management
- □ Communications Plan
- □ Roles and Responsibilities
- □ Workforce Planning
- □ Resource Management
- □ Data Classification
- □ Security Policy
- □ Creating a Security Culture
- □ Security Training
  - Awareness Training
  - Role-Based Training
- □ Metrics and Reporting
- □ IT Portfolio Management
- □ Change Management
- □ Board Communications

Leadership Skills

- □ Business Strategy
- □ Industry Knowledge
- □ Business Acumen
- □ Communication Skills
- □ Presentation Skills
- □ Strategic Planning
- □ Technical Leadership
- □ Security Consulting
- □ Stakeholder Management
- □ Negotiations
- □ Mission and Vision
- □ Values and Culture
- □ Roadmap Development
- □ Business Case Development
- □ Project Management
- □ Employee Development
- □ Financial Planning
- □ Budgeting
- □ Innovation
- □ Marketing
- □ Leading Change
- □ Customer Relationships
- □ Team Building
- □ Mentoring

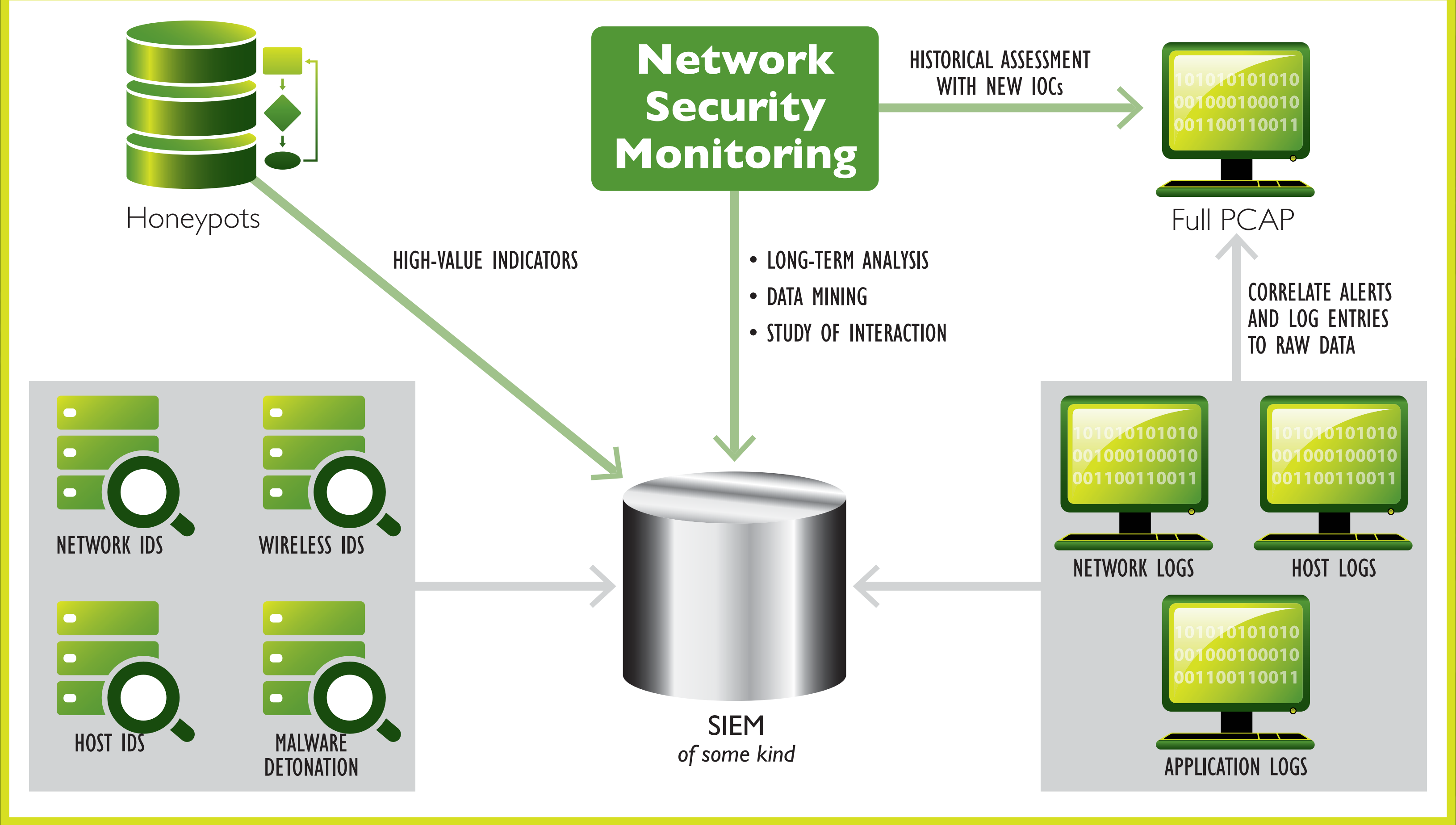
Based on CISO MindMap by Rafeeq Rehman @rafeeq_rehman http://rafeeqrehman.com Used with permission.

Security Operations Center (SOC) Essential Functions



Incident response works with other SOC functions to:

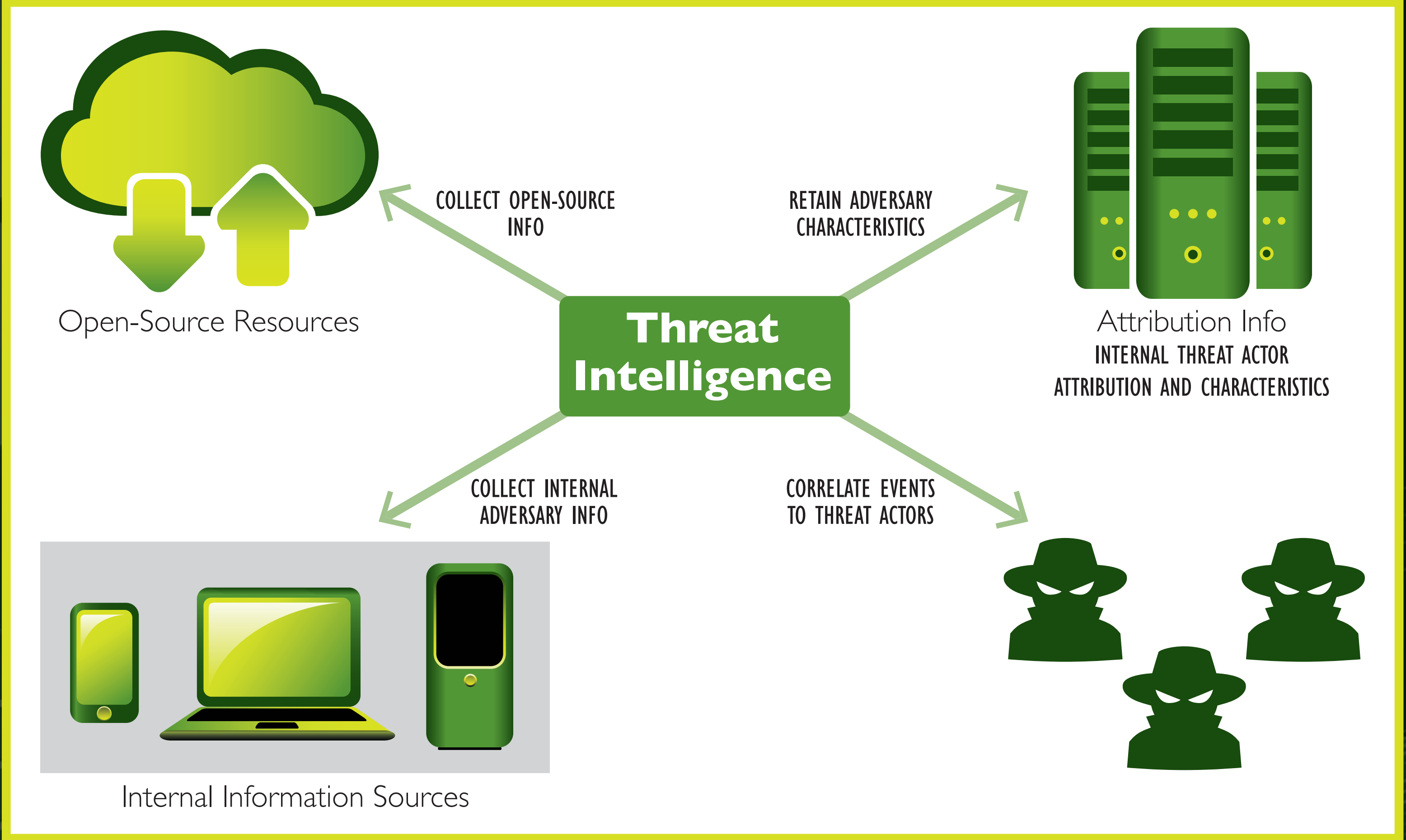
- OBTAIN SUPPORT AND ANALYSIS
- PROVIDE STATUS AND REPORTING

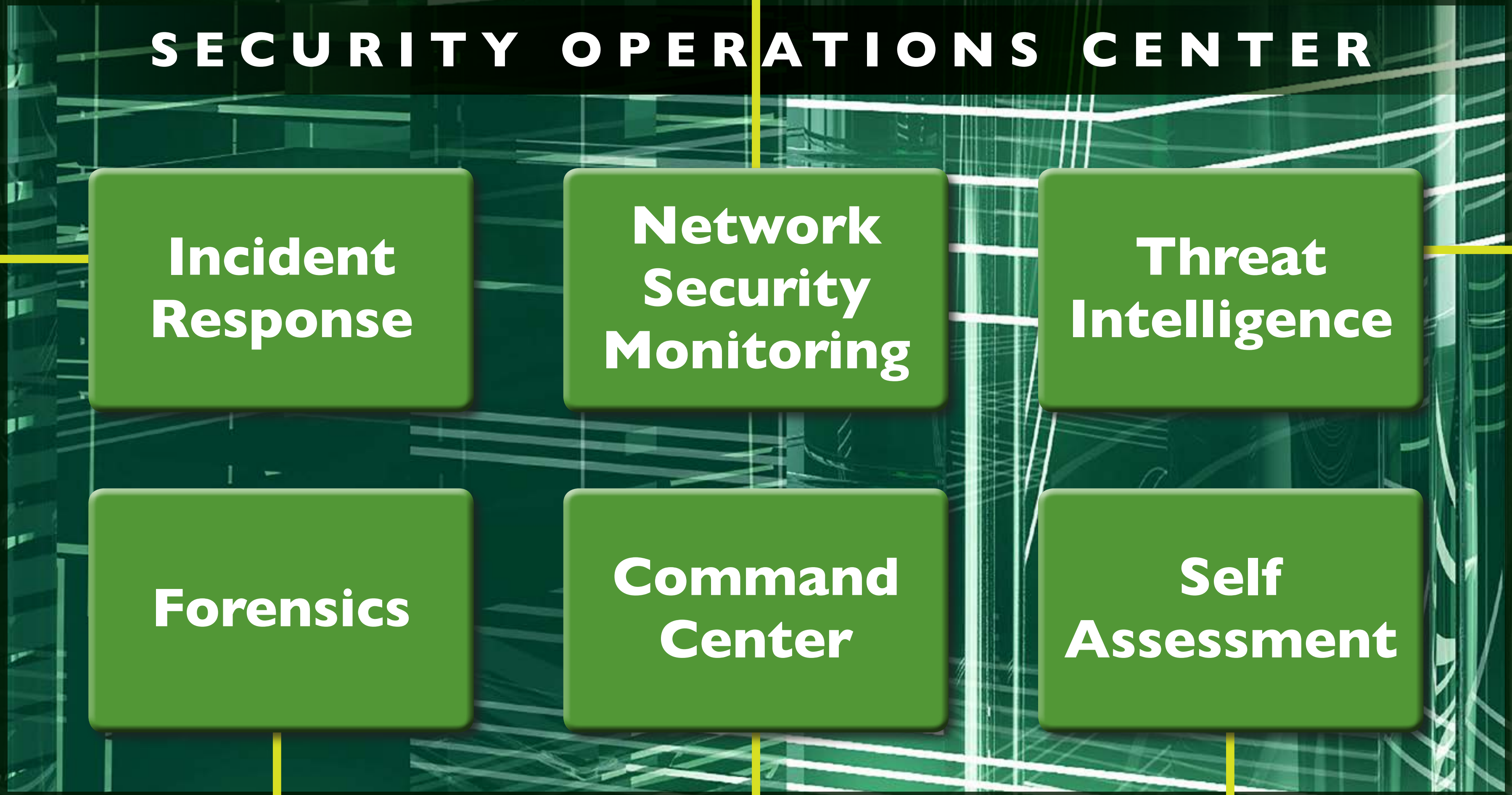


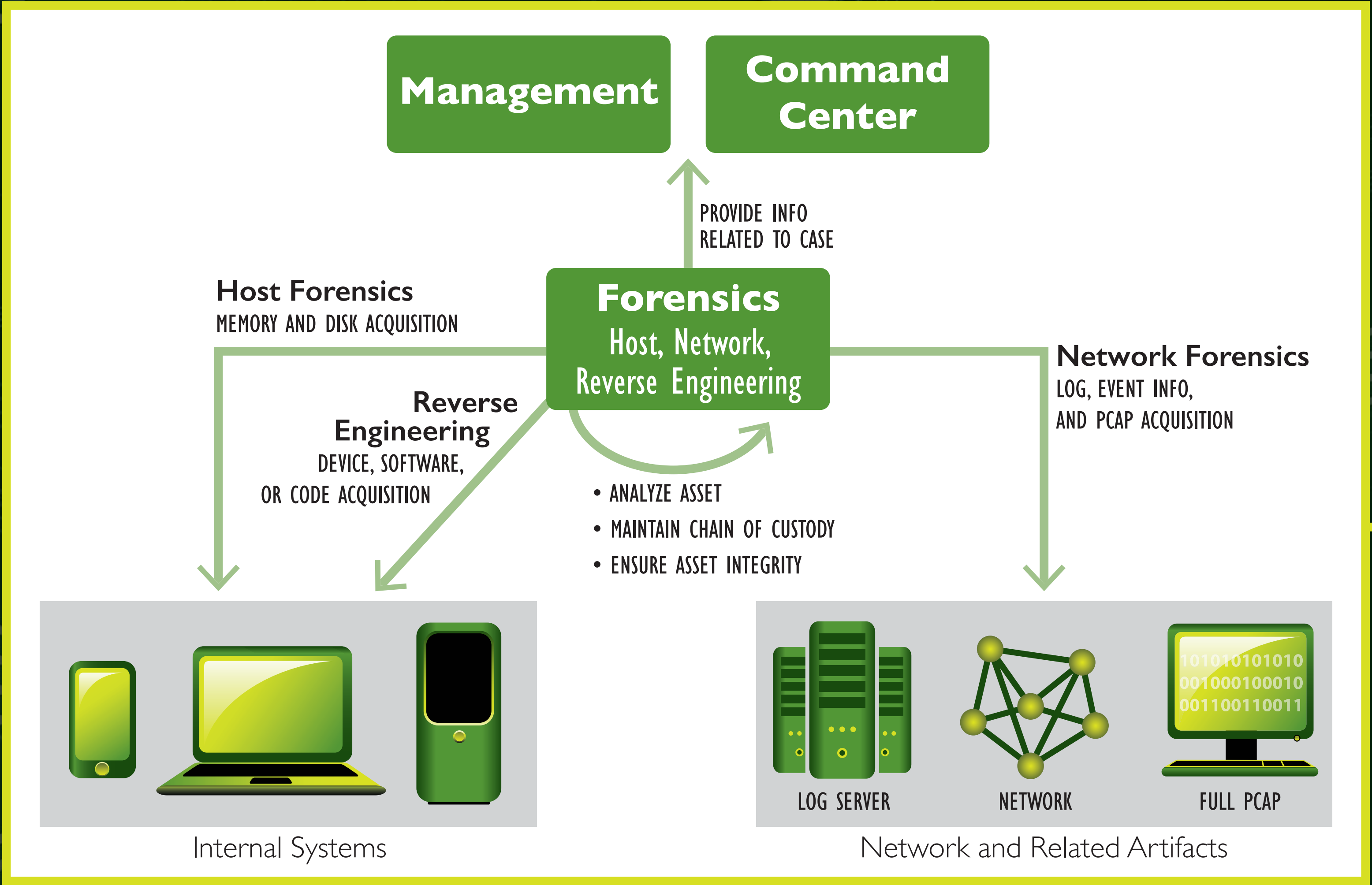
Learn how to design, build, operate, and mature a Security Operations Center (SOC)

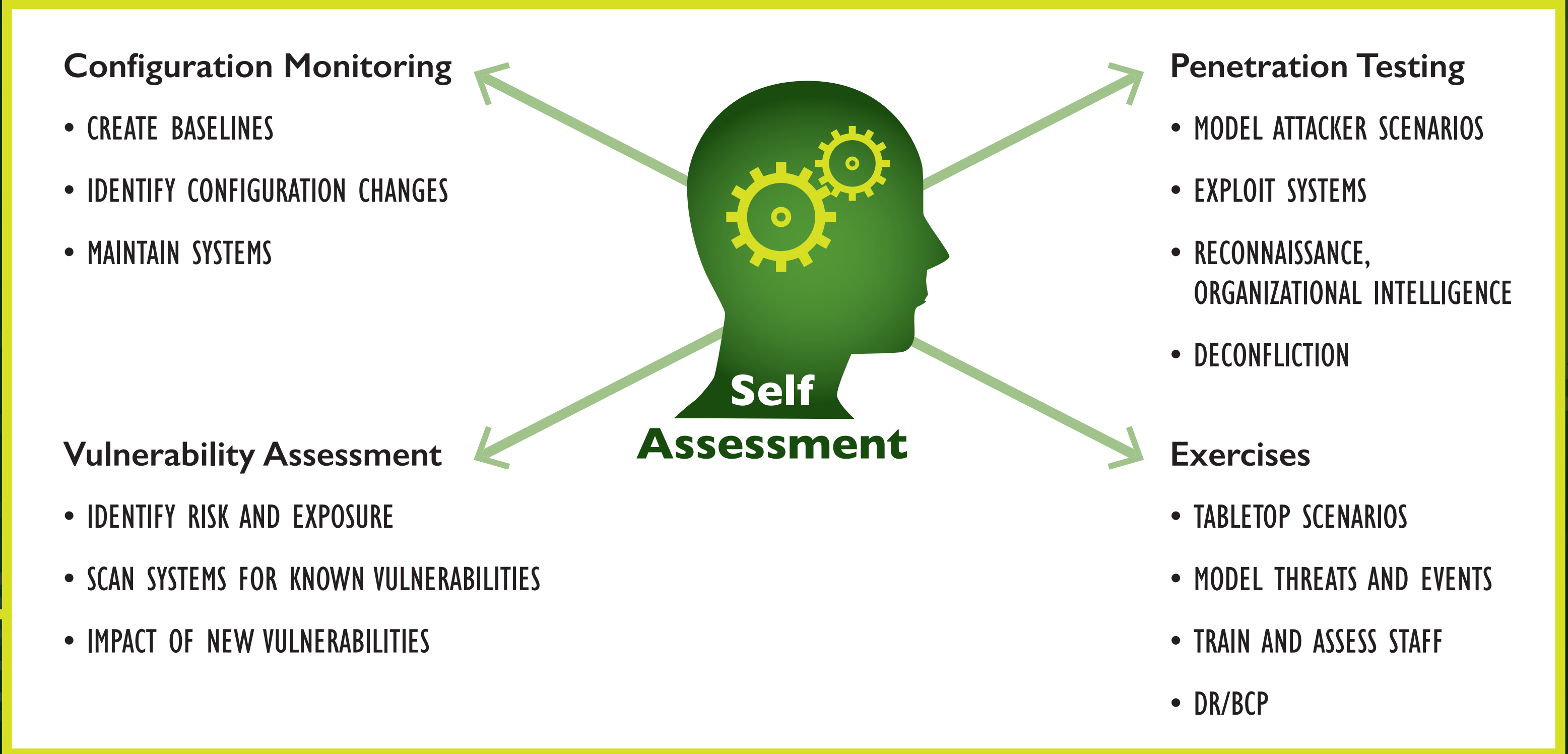
MGT517: Managing Security Operations: Detection, Response, and Intelligence

www.sans.org/MGT517


Open-Source Resources
COLLECT OPEN-SOURCE INFO
Threat Intelligence
RETAIN ADVERSARY CHARACTERISTICS
Attribution Info
INTERNAL THREAT ACTOR ATTRIBUTION AND CHARACTERISTICS
COLLECT INTERNAL ADVERSARY INFO
CORRELATE EVENTS TO THREAT ACTORS
Internal Information Sources




Management
Command Center
PROVIDE INFO RELATED TO CASE
Forensics
Host, Network, Reverse Engineering
Host Forensics
MEMORY AND DISK ACQUISITION
Reverse Engineering
DEVICE, SOFTWARE, OR CODE ACQUISITION
Network Forensics
LOG, EVENT INFO, AND PCAP ACQUISITION
• ANALYZE ASSET
• MAINTAIN CHAIN OF CUSTODY
• ENSURE ASSET INTEGRITY
Internal Systems
LOG SERVER
NETWORK
FULL PCAP
Network and Related Artifacts



Configuration Monitoring

- CREATE BASELINES
- IDENTIFY CONFIGURATION CHANGES
- MAINTAIN SYSTEMS

Vulnerability Assessment

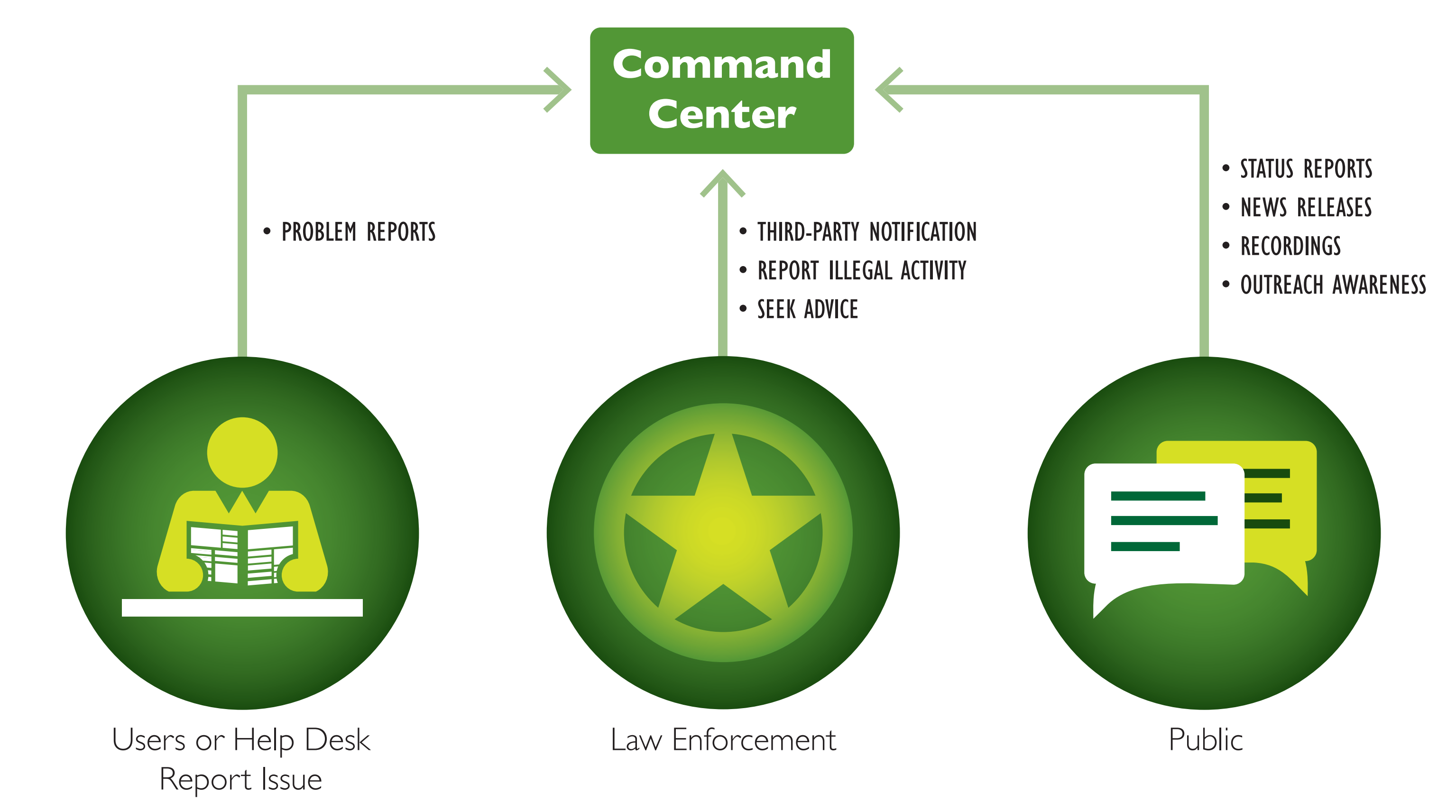
- IDENTIFY RISK AND EXPOSURE
- SCAN SYSTEMS FOR KNOWN VULNERABILITIES
- IMPACT OF NEW VULNERABILITIES

Penetration Testing

- MODEL ATTACKER SCENARIOS
- EXPLOIT SYSTEMS
- RECONNAISSANCE, ORGANIZATIONAL INTELLIGENCE
- DECONFLICTION

Exercises

- TABLETOP SCENARIOS
- MODEL THREATS AND EVENTS
- TRAIN AND ASSESS STAFF
- DR/BCP



MSSP Onboarding Checklist

Organizational Requirements

☐ Defined ownership of security
☐ Good cultural fit
☐ Business partnership

Hiring Standards

☐ Background checks
☐ Credit checks
☐ Security clearance
☐ References
☐ Certifications

Adequately Staffed

☐ Staffing member ratios

Hiring Practices

☐ Drug tests
☐ Citizenship requirements

Suppliers, Partners, and Resellers

☐ Access to customer data
☐ Connection to network

Communication Tools

☐ Case management solution
☐ Information sharing portal
☐ Secure chat

Reports

☐ Metrics and dashboards
☐ Status delivery frequency
☐ MTTD, MTTR

Organizational Stability

☐ Years in business
☐ Financially stable
☐ SLAs and failover capability
☐ Exit strategy

Getting C-Level Support to Ensure a High-Impact SOC Rollout

http://www.sans.org/u/nnD

By John Pescatore

Building a SOC

What do you need to consider when utilizing a Managed Security Service Provider (MSSP) vs. building a SOC in-house?

Outsourcing Pros

- Potential cost savings – building a SOC is expensive
- Fully trained and qualified staff
- Experience handling stressful situations
- Experience handling all types of security events effectively and efficiently
- Augments existing staff/fills gaps in hiring skills professionals
- Threat Intelligence – keeps you current on emerging threats
- Helps you leverage security intelligence across industries
- Industry information sharing
- Enables organizations to focus on core tasks
- Breaks down barriers in organizations where silos exist
- Enables 24x7x365 requirement
- Provides SLAs on how service will be provided
- Well-defined run book

Outsourcing Cons

- Unfamiliar with organization's business drivers/industry
- Limited on depth of service and capabilities
- Optimizes its systems to scale and services a large volume of customers
- Large customer base, lacks intimate knowledge
- Lack of dedicated resources & support for your organization
- Focused on maximizing profits
- Lack of specialization, excels at providing standard security services vs. customized
- Minimal opportunities for correlation unless all data are sent to the MSSP
- Outsourced threat intelligence has a short lifespan
- No incentive to help improve your operations
- Limited ability to store data