Day-1: Building your security program

Cybersecurity leadership roadmap: -

Technical (Technology), Engineer/Analyst -> **Security Manager** (technology leadership), Technical Director, Team Lead -> **Security leadership** (Security Program), CISO, CSO, CRO, VP, Director -> **Executives** (Business Objectives), Board, CEO, CFO, CRO, CIO, CISO, CSO

Focus for security:

(In the new era) AppSec > EndPoint > Network > Data > Physical
(In the old era) Network > EndPoint > Application > Physical & Data

https://interact.f5.com/rs/653-SMC-783/images/RPRT-SEC-1167223548-global-ciso-benchmarkUPDATED.pdf
MGT512 templates -> https://drive.google.com/drive/folders/11h-IKv9EVNe__-buTVnM1UwzPcixKZeu

Plan -> Design -> Build -> Run -> Lead
Governance -> Security Architecture -> Security Engineering -> Security Operations -> Mgmt / leadership

- *Build Sec Program*: Frameworks, Understand risk, Policy, Program structure
- *Technical Sec Architecture*: Sec Architecture, Network Sec, Host Sec, Cloud Sec, Zero Trust
- *Sec Eng*: Cryptography, Encryption, Privacy Engineering, AppSec, DevSecOps
- *Sec Mgmt & leadership*: Vuln mgmt, Sec Awareness, Negotiations, Vendor analysis, Lead teams
- *Detect & Respond to attacks*: SOC, SIEM, Incident mgmt, BCP/DR, Physical Sec

1.2 Security Frameworks

- Control Frameworks
  - NIST SP 800-53 (Security & Privacy by *Family*, *Priority*, *Baseline*)
  - CIS Controls (18 control categories | 154 safeguards [57 in Group-1, 131 in Group-2, 154 in Group-3])
    - CIA CSAT (Self Assessment Tool), Free
  - ISO 27002 (Implementation guidance for controls)
  - SCF: https://securecontrolsframework.com/scf-download/

  Baseline controls | Assess state of technical capabilities | Prioritize | Develop roadmap
- Program Frameworks
  - ISO 27001: Org context, Leadership, Plan, Support, Doc, Ops, Performance, Improvement
  - NIST CSF: Identify, Protect, Detect, Respond, Recover
    - https://www.praxiom.com/nist-cybersecurity-framework.htm
    - https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf

  Measure maturity and industry comparisons
- Risk Frameworks
  - NIST 800-39 (overall), 800-37 (Risk mgmt),
  - 800-30 (Risk assess) -> Prepare, Conduct, Communicate, Maintain
  - NIST RMF: Categorize, Select, Implement, Assess, Authorize, Monitor
  - ISO 27005: Context, Risk Identify, Analysis, Evaluation, Treatment (Accept, Mitigate, ..)
  - FAIR: FAIR institute & Open Group | Quantifying Risk, measuring risk in $$
    - https://www.fairinstitute.org/mission
    - Loss event frequency & Loss magnitude
    - LEF, TEF, CF, PoA, Vuln, TCap, LM, PL, SL
- Third-party certifications: Neutral third-party validation
  - SOC2 Type II: Privacy, Security, Availability, Processing Integrity, Confidentiality
    - SOC 1 -> review of financial reporting controls
    - SOC 2 -> review of Trust services principles controls
    - SOC 3 -> same as SOC2 but resulting report is for general use
  - ISO 27001
  - FedRAMP: US gov program for cloud products and services

1.3 Risk Assessment and Management

Asset: Anything that has value and can introduce liability to the owner when hurt
Threat: Potential hard to asset
Vulnerability: Weakness that can be exploited by a threat source

Risk = Impact x Likelihood = Impact x (Vulnerability x Threat)
Probable frequency and magnitude of future loss

Intrusion Kill Chain: Recon, Weaponization, Delivery, Exploitation, Installation, C2, Actions
High-level view of what adversaries are doing.
Doesn't get into details, of what orgs can do on day-to-day basis
MITRE ATT&CK: Tactics, Techniques, and Procedures (TTPs)
Concepts: https://www.fairinstitute.org/fair-book
Possibility vs. Probability | Prediction vs. Forecast | Subjectivity vs. Objectivity | Precision vs. Accuracy
Risk is a **curve** (credit risk, financial risk, etc.)
Confidence Interval (CI) [range of vales with lower and upper bound] &
Equivalent Bet Test (method to determine if CI is correct)
Calibration -> Method to estimate effectively

- *Avoid Anchoring* (don't begin with a specific number)
- *Start with the absurd* (Extremely high and low values and narrow down)
- *Identify related values* (that can help in accurate estimation)
- *Do the equivalent bet test*
- *Repeat tests* (improves accuracy)

Enterprise Risk Management > Risk Management > Risk Assessment > Risk Analysis
Qualitative vs. Quantitative risk assessment -> with pros and cons
Tools for Quantitative (FAIR-U online, ModelRisk Excel plugin)
ERM: Strategic, Financial, Operational, Regulatory & Compliance, Reputational

1.4 Security Policy

Protects People and Organization
Reasonable Person Rule -> Exceptions to the policy
Policy Pyramid: Principle > Policy > Standard > Guideline > Procedure > Baseline
RAS (Risk Appetite Statement): risk org is willing to take to meet business objectives

- Balance risk and growth

https://www.occ.treas.gov/publications-and-resources/publications/banker-education/files/risk-appetite-statement.html
Risk Profile | Risk Capacity | Risk Appetite | Risk Tolerance

Types of policies in a org: Governance | Operational | Security | Acceptable Use Policy

Components of a policy document: Overview, Purpose, Scope, Policy statement, History, Enforcement, Responsible parties, and Related documents, Action

Guidelines use the wording as 'avoid', 'should', etc.
'Shall' must never be used in any legal document.

Security policy life cycle: Develop => Socialize (distribute) => Measure (review compliance, identify gaps) => Assess (review policies as new threats emerge)

1.5 Program Reporting structure and functions

Three pillars to change the business
Outcome-focused culture | Frictionless security | Risk-aware culture

Three lines of defense model

- Separation of duties

RACI matrix (w/ example)
Evolution: Security as cost center -> as compliance -> as technology -> as enabler
Board committee: Executive, Compensation, Nominating & Governance, Audit, Risk
Security functions:

Identify: Governance, Risk mgmt, Compliance mgmt, Security Architecture
Protect: Data protection (+ n/w & host & app security), Vuln mgmt, IAM
Detect: Threat management (SOC, Logging & Monitoring / SIEM, Threat intel, Pen test)
Respond: Incident mgmt (PICERL), and Forensics
Change: Culture & change execution (Awareness training, succession planning)

Day-2: Technical Security Architecture

2.1 Security Architecture

Security Architecture frameworks: TOGAF (process), SABSA (requirements), O-ESA (best practices), OSA (design patterns)

CyberDefense Matrix (Identify,Protect,Detect,Respond,Recover vs. Devices,Apps,N/w,Data,Users)
Gartner Hype Cycle

2.2 Network Security

Proxies, NGFW, NSM, NIDS -> Application/Presentation/Session layer of OSI
Packet & Stateful Firewall -> Transport layer
Routers, IP, IPSec -> Network later
Switches, VLAN -> Data Link layer (Frame header)
Cabling, Hubs -> Physical layer

MAC: OUI + NIC
CAM Table: MAC and switch port combination
DHCP Snooping: Switch configured to drop unacceptable DHCP traffic; Allowed f/ trusted ports
DAI: Dynamic ARP inspection; validates MAC/IP pairs before updating ARP cache
ARP IDS: arpwatch generates logs for MAP/IP pairings
VLAN hopping: Gain access to another VLAN without authz |
Switch spoofing or Double tagging (native VLAN, destination VLAN)
VLAN mitigations: Disable trunking, Configure VLAN accordingly
SPAN/Mirror ports: For monitoring purposes, copying frames to a specific port
Network Tap (Terminal access point): Forwards all data including malformed frames | Inline to network, possible short disruption in live

IPv4 header
ICMP Attacks (Ping floods [lot of packets with forged source ip], Smurf attack, Ping of death [large size ping packet causing buffer overflow])
Routing attacks (disable source routing)
VPN: client-to-site and site-to-site
IPSec: encryption between users and devices | Tunnel mode and Transport mode
VPN deployment options: IPSec VPN (n/w layer) | TLS VPN (App layer) | VPN-as-a-Service
Split tunneling (organizations allowing direct connections for user for YouTube, Netflix, etc.)
Full tunneling (organizations making every connection to corporate VPN to investigate)

TCP Header (Establish connection: SYN-SYNACK-ACK | Close connection: FIN-ACK-FIN-ACK)
UDP Header

App Proxies (control data flow, limit access, analyze traffic) | forward proxy, reverse proxy
Web Proxy: Can analyze
Content, Category, Reputation, Certificates, Signatures, Protocol, URLs, Status codes, User agents
(X-Forwarded-For header has client-ip)

Domain Squatting attack (seeming similar domain names but different at Unicode level)
SMTP proxy (blocks spam, malware), Uses Bayesian analysis
Email validation: SPF, DKIM, SMARC

NGFW: deep packet inspection | benefits: intrusion prevention, n/w activirus, malware detonation & sandboxing, ssl inspection, url filtering, web proxy, data loss prevention, authentication

Security Onion -> Free linux distribution with Snort, Suricata, OSSEC, Zeek, ELK
For threat hunting, enterprise security monitoring, and log management.

NIDS: signature based, anomaly-based, protocol analysis (shallow packet vs. deep packet)
NIPS: hierarchical rule classification schemes to classify and identify traffic
Snort & Suricata
Zeek: logs correlate by timestamp, uid, etc.

2.3 Host Security

Malware: Virus, Spyware, Trojan horse, Rootkit, Worm
(Example malware: FinFisher, Node.js Cyptocurrency Trojan, Morris Worm, Mirai, Botnet)
Mirai DDoS botnet uses Default passwords to attack botnet hosts
Reconnaissance
Endpoint Protection Platform (EPP): Cloud-based Antivirus
Endpoint Detection & Response (EDR): well-suited for orgs with SOC in place (+ App Allowlisting)
HIDS: OSSEC (includes FIM capability), Wazuh
FIM (File Integrity Monitoring): Tripwire (commercial)
Application Allowlisting
Sandboxing (example: Web browser, email client, adobe acrobat, MS office)
Microsoft Defender (XDR): 365 defender (EndPoint, Office, Identity, Cloud App), Azure defender

2.4 Cloud Security

IAAS, PAAS, SAAS
AWS and Azure shared responsibility model
AWS, Azure, GCP core services
AWS Regions and Availability zones
AWS Security Reference Architecture: *Security* (OU-Security) | *Administration* (OU-Infrastructure) | *Application* (OU-Workloads)
AWS Subnets (NACL, per AZ) | AWS VPC (per AWS region) | AWS IGW (connect VPC to internet)
NAT Gateway
AWS EC2, EC2 security groups (Stateful firewall)
AWS IMDSv1:

```
$curl -s “http://169.254.169.254/latest/meta-data/iam/security-credentials/”
```

Cloud Storage Platforms: AWS S3, Azure Storage, GCP Cloud Storage
Cloud provider benchmarks (assessment checklist & Impl.)
Cloud Security Tools: **CSPM** (Posture mgmt) | **CWPP** (Protection platform) | **CASB** (Access Sec Broker)
CSA (Cloud Security Alliance) Guidance: 14 domains
CSP’s Well-architected frameworks: AWS, Azure, GCP
CSP’s Cloud Adoption frameworks: AWS, Azure, GCP
GCP’s Cloud Security Roadmap: Learn, Lead, Scale, Secure

2.5 Zero Trust (Trust nothing, verify everything)

Perimeter security has major failing!

Zero Trust Principles: Assume breach, Secure all traffic, Enforce least privilege, Secure all assets

SASE: Secure Access Service Edge (sassy):

- Secure Web Gateway | CASB | Firewall-as-a-Service (FWaaS) | Zero Trust Network Access (ZTNA)

ZTNA:- identity and context based & logical access boundary for apps

Microsoft ZTMM (Zero Trust Maturity Model): Traditional -> Advanced -> Optimal

Identities, Devices, Apps, Infrastructure, Network, Data

Variable Trust: e.g. access granted based on points scored

Microsoft conditional access

Trust over time: (naturally reduced trust over time)

TLS & Mutual authentication with client certificates

Windows Domain Isolation (uses IPSec, so tcpdump or wireshark communication is encrypted)

Windows IPSec

802.1X (NAC, port-based authentication) or

Single Packet Authorization (SPA): send specially crafted packet (HMAC), then target system connects

Day-3: Security Engineering

3.1 Data Protection (Cryptography)

Plain text vs Cipher text

Monoalphabetic cipher vs. Polyalphabetic cipher

Unbreakable Cipher: perfect secrey: random, as long as message, never reused

Perfect forward secrecy: using a new encryption key for every session

Vernam cipher or one-time pad (XOR is like 'not equal to' where 1 is true and o is false)

Substitution | Permutation/transposition | Hybrid

Ceasar cipher (ROT3)

Encryption algorithms: Symmetric, Asymmetric, Hashing

Stream and Block ciphers

DES: 64-bit block cipher, 56-bit key size

AES: SubBytes(), ShiftRows(), MixColumns()

Encryption Application: TLS, PKI, BlockChain, Quantum

TPM (Trusted Platform Module) <- secure storage of keys

Cryptocurrency security issues

Quantum computing: Shor's algo & Grover's algo

3.2 Privacy Primer

Data types: Anonymous data, Pseudonymous data, PII, Sensitive PII

Types of consent: Explicit, Implicit

Notice requirements: Privacy policy (why, what, how, etc.)

Australia Privacy Act, Canada PIPEDA, Europe GDPR & ePrivacy Regulation

GDPR requirements: Breach disclosure penalties, Personal data requirements, Security program reqs.

UN org for economic co-operation & development privacy rules

USA: Finance (Gramm-leach-biley act, Dodd-frank), Government (Privacy act), Healthcare (HIPPA), Protection of children (COPPA) | CCPA (California)

Predictability, Manageability, Disassociability | Confidentiality, Integrity, Availability

NIST Privacy Framework (Identify-P, Govern-P, Control-P, Communicate-P, Protect-P)

Privacy Engineering

3.3 Application Security

Secure SDLC
OWASP Top 10
SQL injection
XSS
Vulnerable and outdated components
Bugs (simple coding errors) vs. Flaws (deeper-level problems like architecture or design issue)
Security tools in SDLC
SAST, SCA, DAST, WAF (mostly deployed in monitor mode only), IAST, RASP
BSIMM, OWASP SAMM

3.4 DevSecOps

<u>*DevOps KPI*</u>: Deploy more frequently, Have shorter lead times to fix, Recover from failures faster, Spend less time to remediate security issues, make employees recommend their company as great place to work

CALMS
Culture conflict
Everything as code
CICD pipeline | Git Workflow
Risks with DevOps (+ mitigation)

3.5 Infrastructure as code

Infra as code tools: Config mgmt tools | Cloud IaC tools
Infra as code – hardening
Containers (vs VM) | Docker (Engine, Client)
Security issues: lightweight isolation, user namespacing (root in image is root in host), untrusted content, runtime issues
Docker daemon attack surface: Runs as root | access permissions
Container security tools: NIST SP 800-190 App Container Security Guide
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf

Day-4: Security Management & Leadership

4.1 Vulnerability Management (MGT516)

Create policy, Define process, Publish metrics, Develop roadmap
PIACT process: Prepare | Identify | Analyze (risk) | Communicate | Treat
CIS Control #7: Continuous Vulnerability Management (7.1 to 7.7)
NIST CSF to CIS Control mapping to PIACT process
Vuln mgmt policy: Statement | SLAs by Severity
Asset inventory
Obtaining buy-in
Scanning tool deployment considerations
CVE and NVD | CVSS (temporal metrics: exploitability and compensating controls)
cvss = base score x exploit code maturity x remediation level x report confidence
Focus on vulns that have public exploits and that doesn't have enough compensating controls
<u>Vuln prioritization tools</u>: Kenna Security | Nopsec | Skybox Security | RiskSense
Vuln metrics hierarchy: NIST CSF mapping to Technical / Operational / Executive metrics
Example security dashboard
Patch management process: identify a lead to own the overall patch mgmt process
Build RACI per task | Separate patching emergency / pre-approved / sensitive systems
Build SLAs based on priority
Patch mgmt tools: Adhoc | native | Centralized
EndPoint patching | Application patching | Server patching tools

4.2 Security Awareness (MGT433)

Education | Training | Awareness

Security Awareness Maturity Model: Non-existent -> Compliance focused -> Promoting awareness & behavior change -> Long term sustainment & culture change -> Metrics framework

Security awareness programs are focused on managing human risk

Social Engineering

Fogg Behavior Model: Motivation & Ability graph

Identify the top human risks:

- Create an internal advisory board to get answers
  - HR, Marketing, Legal, IT admins, Helpdesk, Accounts payable, SOC, Executives

Strategic plan for awareness progress:

- RISKS | BEHAVIORS | CHANGE
  - Core risks vs. Role based risk

Learning Objectives to be defined

Motivating change: Start with WHY, then HOW, then WHAT (golden circle)

Communicate: Primary and Reinforcement

Branding the program: Mascot / Logo / Tagline

AIDA marketing funnel: Attention | Interest | Desire | Action

Culture change takes time

Human Emotions

Security awareness *metrics*: Impact metrics, Compliance metrics, Ambassador pgm metrics,..

4.3 Negotiations Primer

Strategies: Distributive (win-lose), Integrative (win-win), Mixed-motive

BATNA: Best Alternative to a Negotiated Agreement <- Distributive bargaining

ZOPA (Zone of Possible Agreement): min value to max value

Never internalize (don't make it personal)

Don't negotiate against yourself

Speed kills in a negotiation

Walk away

A good negotiation (when both wins)

4.4 Vendor Analysis

Vendor analysis requirements: Data in and out, storage, speed, cost, platform, business needs,..

Secret life of a salesperson

Analyze vendor responses

Price and value

Procurement: make vs. buy

- contract types: Fixed-price or lump-sum, Cost-reimburse, Time and material contracts

TCO (Total cost of ownership): direct costs + indirect costs + depreciation

Analytical hierarchy process (AHP) (gets management buy-in)

4.5 Management and Leading Teams

Managing projects | Leading Teams <= Good to Great!

Death via over managing

PMO (Project mgmt Office): Supportive, Controlling, Directive

Proj mgr responsibilities: Scope, Time, Cost

Waterfall (plan rules), Agile (trust rules), DevOps (trust & automation rule)

Initiating (identify stakeholders, create project charter, scope) -> Planning -> Executing -> Monitoring -> Closing (PMBOK)

WBS (Work Breakdown Structure)

Leading Teams: Recruiting security talent

Presentation techniques (KISS mentality:- Keep it simple stupid); Don't use too many sub-bullets

Elevator Pitch: WIIFM (Whats in it for me) | BLUF (Bottom line up front)

Principles of Persuasion: Reciprocity, Scarcity, Authority, Consistency, Liking, Social Proof

Good to great: Flywheel:

Level-5 leadership! (Skilled worker, Reliable Teammate, Organized Manager, Visionary, Humility & Resolve)

BHAG -> Big Hairy Audacious Goal (Passionate / Best at / Economic)

Culture of discipline

Day-5: Detecting & Responding to Attacks

5.1 Detecting & Responding to Attacks (SIEM) (SEC555)

Average time to detect threats -> 56 days!

Central log collection and correlation

SIEM deployment approaches:

1. Tactical considerations: Log ingestion, alerts, dashboard detection
2. Security Effectiveness: Measure security controls, eliminating false positives
3. Business Effectiveness: Knowing thyself, make informed decisions

Data collection: Input-driven, Output-driven, Hybrid

Collect logs from a subset of client desktops and all servers

Right logs at the right time

Windows Audit Policies control what to log

Sysmon -> Sysinternals tool that provides process hashes and parent processes for analysis

Linux Auditing System (auditd), Snoopy Logger, go-audit, Auditbeat

SIEM Sizing recommendations: Try a POC to estimate | scripts to understand events per second | plan to over purchase

SIEM components: Log collectors, Aggregator, Broker, Storage, Search/Report, Alert engine

Traditional approach vs. Network approach to collect logs

Logs context enrichment

Pros and Cons

Dashboards

Alerting: Alert rule types: Denylisting, Allowlisting, New Term, Frequency, Threasholds

Security testing

False positives reduction

Business Decision Making | **ElastAlert**: can be used to make system up (with RDP request)

5.2 Security Operations Center (SOC) (MGT551)

Purpose: To answer: Who or what was targeted for the attack? Was adversary successful? How do we continue business mission?

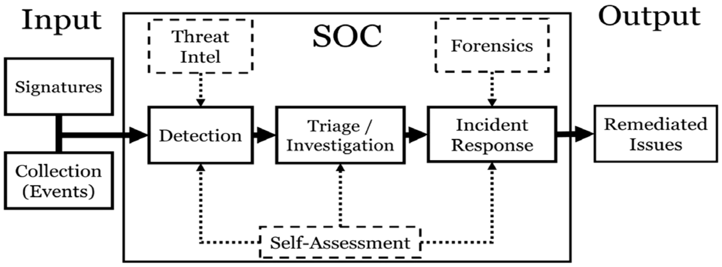
CSOC, CIRT, CSIRT, CERT, NOSC

Threat intel + env data as input -> SOC -> identified/managed/remediated incidents as output

SOC functions: Collection -> Detection -> Triage -> Investigation -> Incident Response

Core SOC: Collection, Detection, Triage, Investigation, IR

Speciality/Auxiliary SOC: Threat Intel, Forensics, Self-assessment (VA, PT, Red team)



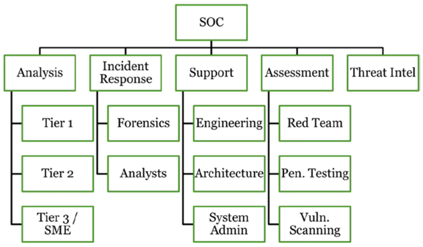
Event, Incident, Breach

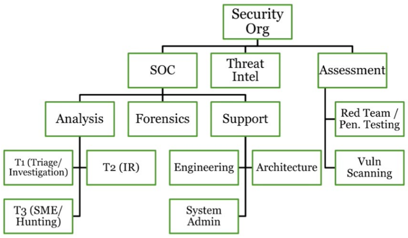
Operations flow: Tier 1, Tier 2, Tier 3

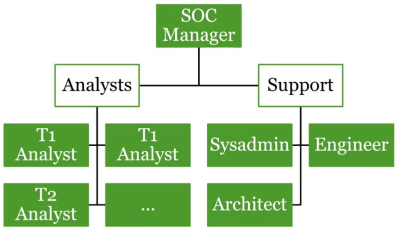
Do we need a SOC?

Can leverage the SOC of a parent company | Hire a third-party

SOC models: Virtual SOC (1k IPs), Small SOC (10k IPs), Large SOC (50k IPs), Tiered SOC (500k IPs), National SOC (50,000k IPs)







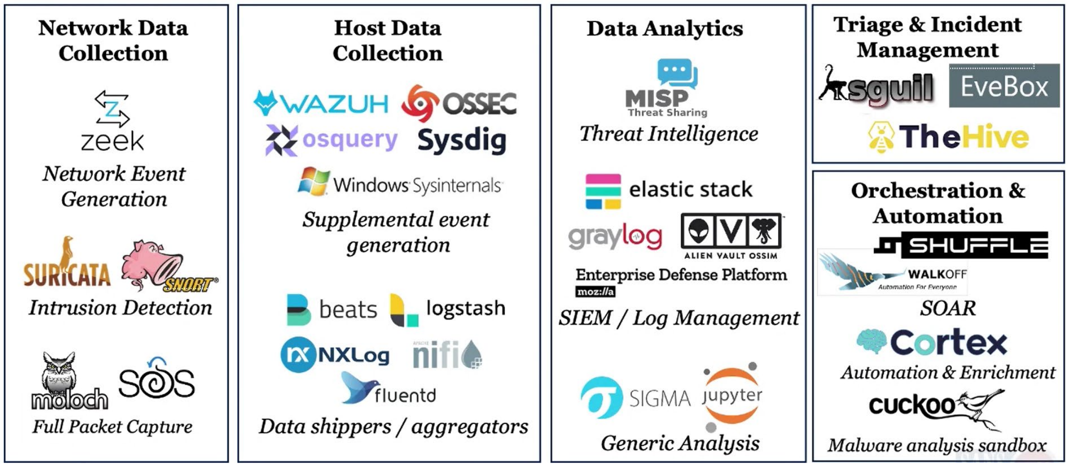
Tiered vs Tierless (pros and cons)

24x7 SOC

Resource constraints (5 FTEs for 24x7)

SOC Data Flow: pcaps, log files, etc. into SIEM -> alerts into EvBox, etc.

OpenSource SOC tools



SOAR tools: Security Orchestration Automation & Response

SIEM: Log aggregation, Filtering & Enrichment, Indexing and Storage

Threat Intel platform: Indicator lookup, Threat context & Info

Incident mgmt system

Playbooks: step of known steps to activities

No playbooks, Strick playbooks, Too many playbooks -> Bad

SOAR-based playbooks

Hiring Staff

Minimize turnover

Managing career opportunities

SOC metrics: Detection time, Containment time, Attacker dwell time, Incidents with same root cause, cost and downtime per incident

5.3 Incident Handling and Response

IR: identify, analyze, contain an incident (done by SOC)

IH: coordination, communications, planning to resolve an incident (or IM)

PICERL process:

Prepare, Identify, Contain, Eradicate, Recover, Lesson learned

NIST IH lifecycle: Prepare, Detect & Analyze, Containment Eradicate & Recovery, Post-incident activity

- NIST SP 800-61r2

Prepare to respond vs Prepare to detect incidents

Chain of Custody

Tabletop exercises

- Basic tabletop exercise (phishing case)

Time to discovery

Categorize the incident (functional impact, Information impact, Recoverability effort)

Containment: Short-term actions, Backup, Long-term containment

- Physical disconnection, Logical isolation, Block by IP, by domain name, by port, by app, ..

5.4 Contingency Planning

BCP (run business) /DR (restoration of info):

Classic: Hot site, Warm site, Cold site

- Checklist test, tabletop test, walkthrough test, functional test, full-scale test

Modern: two or more sites geographically located (cloud regions)

Business impact analysis (BIA)

- Overall process: Project initiation -> Risk analysis -> BIA -> build the plan -> test & validate the plan -> modify & update plan -> approve and implement the plan

Top BCP/DR mistakes

5.5 Physical Security

Technical, Administrative, Physical controls

Admin controls for physical security

Managing power and cooling (availability issue)

Smoke and Fire (detectors in place)

Proximity to explosive effects | building characteristics | structural concerns

Deter, Deny, Detect, Delay <- security controls

Types of locks & bypassing locks

Safety and InfoSec (human safety first -> business emergency and evacuation plan)

Safety walkthrough

*** END OF DOCUMENT ***