Cybersecurity Terminology

This is an optional reading material for students with non-cyber security background.

1: Inventory Management

Cybersecurity inventory Management involves tracking and managing all IT assets, including hardware, software, and data, to ensure security and compliance. It helps identify vulnerabilities, assess risks, and optimize resource use. Regular updates, access controls, and employee training are crucial.

- **Importance:** Risk management, compliance, efficient operations.
- **Best Practices:** Regular updates, security measures, training.
- **References:** CISA Asset Inventories, SANS Institute Asset Inventories, Palo Alto Networks Asset Inventories.

2: Controls Log Data

Controls Log Data refers to records from security controls like firewalls and antivirus, which are vital for monitoring and analyzing events. It aids in threat detection, incident response, and compliance. Centralized logging, regular reviews, and secure storage are essential.

- **Importance:** Threat detection, incident response, compliance.
- **Best Practices:** Centralized logging, regular review, secure storage.
- **References:** CISA Log Analysis, Splunk Log Analysis, Fortinet Log Analysis.

3: Policies

Policies are formal guidelines for managing and protecting information assets, ensuring consistency, risk mitigation, and legal compliance. Clear communication, regular updates, and enforcement mechanisms are key.

- **Importance:** Consistency, risk mitigation, legal compliance.
- **Best Practices:** Clear communication, regular updates, and enforcement.
- **References:** CISA Policies, ISACA Cybersecurity Professional, SANS Institute Policies.

Cybersecurity Terminology

4: Alerts & Rules

Alerts & Rules involve setting conditions to trigger notifications for security events, aiding early detection and efficient response. Customization, prioritization, and regular testing are crucial.

- **Importance:** Early detection, efficient response, customization.
- **Best Practices:** Prioritization, regular testing, integration.
- **References:** CISA Alerts, Splunk Alerts, Fortinet Alerts.

5: Behavior Data

Behavior Data involves collecting and analyzing user activities to detect anomalies, aiding insider threat detection and risk management. Continuous monitoring, machine learning, and data privacy are essential.

- **Importance:** Anomaly detection, user profiling, insider threat detection.
- **Best Practices:** Continuous monitoring, machine learning, data privacy.
- **References:** CISA Behavior Analysis, SANS Institute Behavior Analysis, Palo Alto Networks Behavior Analysis.

6: Threat Intelligence

Threat Intelligence involves collecting and analyzing information about potential threats to inform security decisions. It aids proactive defense, risk management, and informed decision-making. Diverse sources, timeliness, and actionable insights are key.

- **Importance:** Proactive defense, informed decision-making, risk management.
- **Best Practices:** Sources diversity, timeliness, actionable insights.
- **References:** CISA Threat Intelligence, SANS Institute Threat Intelligence, Fortinet Threat Intelligence.

7: Web Application Firewall (WAF)

Cybersecurity Terminology

A Web Application Firewall (WAF) protects web applications from attacks like SQL injection and XSS, offering customizable rules and real-time monitoring. Regular updates, integration, and testing are crucial.

- **Importance:** Protection from attacks, customizable rules, real-time monitoring.
- **Best Practices:** Regular updates, integration, testing.
- **References:** CISA Web Application Firewall, OWASP Web Application Firewall, SANS Institute Web Application Firewall.

8: Cloud Posture Management

Cloud Posture Management ensures secure cloud configurations, aiding security, compliance, and risk reduction. Regular assessments, automated tools, and employee training are essential.

- **Importance:** Security configuration, compliance, risk reduction.
- **Best Practices:** Regular assessments, automated tools, employee training.
- **References:** CISA Cloud Security, NIST SP 800-144, SANS Institute Cloud Posture Management.

9: Extended Detection & Response (XDR)

Extended Detection & Response (XDR) integrates security data for comprehensive visibility, aiding efficient response and scalability. Data integration, automated processes, and regular updates are key.

- **Importance:** Unified visibility, efficient response, scalability.
- **Best Practices:** Data integration, automated processes, regular updates.
- **References:** CISA Extended Detection Response, SANS Institute Extended Detection Response, Fortinet Extended Detection Response.

10: Information Protection

Cybersecurity Terminology

Information Protection safeguards sensitive data from unauthorized access, ensuring confidentiality, integrity, and availability. Encryption, access controls, and regular backups are crucial.

- **Importance:** Data confidentiality, integrity, availability.
- **Best Practices:** Encryption, access controls, regular backups.
- **References:** CISA Information Protection, NIST SP 800-53, SANS Institute Information Protection.

11: Secure Web Gateway (SWG)

A Secure Web Gateway (SWG) provides secure internet access, filtering web traffic to block malicious content and enforce policies. Regular updates, user training, and monitoring are essential.

- **Importance:** Web security, policy enforcement, data protection.
- **Best Practices:** Regular updates, user training, monitoring.
- **References:** CISA Secure Web Gateway, SANS Institute Secure Web Gateway, Fortinet Secure Web Gateway.

12: SIEM & Graphs

SIEM systems collect and analyze security events, using graphs for visualization, aiding centralized monitoring, threat detection, and compliance reporting. Proper configuration, regular testing, and integration are key.

- **Importance:** Centralized monitoring, threat detection, and compliance reporting.
- **Best Practices:** Proper configuration, regular testing, integration.
- **References:** CISA SIEM, SANS Institute SIEM, Palo Alto Networks SIEM.

Cybersecurity Terminology

13: Big Data Analytics

Big Data Analytics processes large data volumes to detect patterns and threats, aiding threat detection, predictive analysis, and efficiency. Data quality, security measures, and continuous learning are crucial.

- **Importance:** Threat detection, predictive analysis, efficiency.
- **Best Practices:** Data quality, security measures, continuous learning.
- **References:** CISA Big Data Analytics, SANS Institute Big Data Analytics, Fortinet Big Data Analytics.

14: ML Analytics

ML Analytics uses machine learning to detect security threats, offering automated detection, adaptive defense, and efficiency. Data preparation, model validation, and ethical considerations are key.

- **Importance:** Automated threat detection, adaptive defense, efficiency.
- **Best Practices:** Data preparation, model validation, ethical considerations.
- **References:** CISA Machine Learning, SANS Institute Machine Learning, Palo Alto Networks Machine Learning.

15: User Behavior Analytics (UBA)

UBA monitors user activities to detect anomalies, aiding insider threat detection and risk management. Baseline establishment, continuous monitoring, and integration are essential.

- **Importance:** Insider threat detection, anomaly detection, risk management.
- **Best Practices:** Baseline establishment, continuous monitoring, integration.
- **References:** CISA User Behavior Analytics, SANS Institute User Behavior Analytics, Fortinet User Behavior Analytics.

Cybersecurity Terminology

16: Traffic Pattern Analysis

Traffic Pattern Analysis examines network traffic to detect anomalies, aiding threat detection, performance monitoring, and incident response. Continuous monitoring, anomaly detection tools, and collaboration are key.

- **Importance:** Threat detection, performance monitoring, incident response.
- **Best Practices:** Continuous monitoring, anomaly detection tools, collaboration.
- **References:** CISA Traffic Pattern Analysis, SANS Institute Traffic Pattern Analysis, Palo Alto Networks Traffic Pattern Analysis.

17: Query Engines

Query Engines allow searching and querying security data, aiding efficient data retrieval, threat detection, and compliance reporting. Regular updates, security measures, and user training are crucial.

- **Importance:** Efficient data retrieval, threat detection, and compliance reporting.
- **Best Practices:** Regular updates, security measures, user training.
- **References:** CISA Query Engines, SANS Institute Query Engines, Fortinet Query Engines.

18: Risk Scoring

Risk Scoring quantifies risk levels for assets or systems, aiding prioritization, decision-making, and compliance. Regular assessments, standardized methodology, and communication are key.

- **Importance:** Prioritization, decision-making, compliance.
- **Best Practices:** Regular assessments, standardized methodology, and communication.
- **References:** CISA Risk Scoring, SANS Institute Risk Scoring, Palo Alto Networks Risk Scoring.

Cybersecurity Terminology

19: 1-Pane of Glass

1-Pane of Glass" provides a unified dashboard for monitoring security operations, aiding centralized visibility, efficient management, and improved decision-making. Customizable dashboards, real-time updates, and integration are key.

- **Importance:** Centralized visibility, efficient management, improved decision-making.
- **Best Practices:** Customizable dashboards, real-time updates, integration.
- **References:** CISA Cybersecurity Best Practices, Splunk Security Dashboards, Palo Alto Networks Cybersecurity Dashboard.

20: Reporting

Reporting involves generating data and insights on security events for stakeholders, aiding decision-making, compliance, and improvement. Regular reporting, clear and concise formats, and data accuracy are crucial.

- **Importance:** Decision-making, compliance, improvement.
- **Best Practices:** Regular reporting, clear and concise, data accuracy.
- **References:** CISA Reporting, SANS Institute Reporting, Fortinet Reporting.

21: Workflow Engine

A Workflow Engine automates security operations like incident response, aiding efficiency, consistency, and scalability. Clear workflows, regular testing, and human oversight are key.

- **Importance:** Efficiency, consistency, scalability.
- **Best Practices:** Clear workflows, regular testing, human oversight.
- **References:** Splunk Security Automation, Oneflow Workflow Automation, Kychub Workflow Automation.

Cybersecurity Terminology

22: Hunting Activity

Hunting Activity involves proactively searching for advanced threats, aiding proactive detection, enhanced security posture, and continuous improvement. Clear objectives, advanced tools, and regular training are key.

- **Importance:** Proactive detection, enhanced security posture, continuous improvement.
- **Best Practices:** Clear objectives, advanced tools, regular training.
- **References:** Splunk Threat Hunting, Cisco Threat Hunting, Microsoft Security Threat Hunting.

23: Prediction Analytics

Prediction Analytics uses data to predict future threats, aiding proactive management, resource optimization, and continuous improvement. Data quality, model validation, and integration are key.

- **Importance:** Proactive management, resource optimization, continuous improvement.
- **Best Practices:** Data quality, model validation, integration.
- **References:** Infosec Institute Data Analytics, DataGuard Predictive Analytics, ResearchGate Predictive Analytics.

24: Person of Interest

A Person of Interest (POI) is suspected of security incident involvement, aiding threat intelligence, incident response, and risk management. Behavioral analysis, access monitoring, and collaboration are key.

- **Importance:** Threat intelligence, incident response, risk management.
- **Best Practices:** Behavioral analysis, access monitoring, collaboration.
- **References:** Cisco Cybersecurity, GeeksforGeeks Cybersecurity, ISACA Cybersecurity Professional.

Cybersecurity Terminology

25: Data Exfiltration

Data Exfiltration is the unauthorized transfer of data, posing risks to data protection, business continuity, and national security. DLP tools, access controls, and employee training are key prevention strategies.

- **Importance:** Data protection, business continuity, national security.
- **Best Practices:** DLP tools, access controls, employee training.
- **References:** CrowdStrike Data Exfiltration, Palo Alto Networks Data Exfiltration, Fortinet Data Exfiltration.

26: Risk & Governance

Risk & Governance involves managing and overseeing cybersecurity risks, ensuring risk management, policy enforcement, and compliance. Board-level involvement, regular assessments, and training are key.

- **Importance:** Risk management, policy enforcement, regulatory compliance.
- **Best Practices:** Board-level involvement, regular assessments, training.
- **References:** CISA Cybersecurity Governance, SafetyCulture Cybersecurity Governance, Harvard Law School Cybersecurity Governance.

27: Incident Management

Incident Management involves identifying, analyzing, and responding to security incidents, minimizing damage, ensuring rapid response, and learning for improvement. Clear roles, regular drills, and continuous monitoring are key.

- **Importance:** Minimizing damage, rapid response, improvement and learning.
- **Best Practices:** Clear roles, regular drills, continuous monitoring.
- **References:** CISA Incident Response, SANS Institute Incident Response, Fortinet Incident Response.

Cybersecurity Terminology

28: Supply Chain Management

Supply Chain Management secures the supply chain against cyber threats, mitigating risks, ensuring compliance, and maintaining business continuity. Vendor assessment, contractual requirements, and monitoring are key.

- **Importance:** Risk mitigation, regulatory compliance, business continuity.
- **Best Practices:** Vendor assessment, contractual requirements, monitoring.
- **References:** CISA Supply Chain Risk, SANS Institute Supply Chain Risk, Palo Alto Networks Supply Chain Risk.

29: Vulnerability Management

Vulnerability Management identifies and mitigates IT system vulnerabilities, preventing threats, reducing risks, and meeting compliance. Regular scanning, patch management, and employee training are key.

- **Importance:** Threat prevention, risk reduction, compliance requirements.
- **Best Practices:** Regular scanning, patch management, employee training.
- **References:** CISA Vulnerability Disclosure, SANS Institute Vulnerability Disclosure, Palo Alto Networks Vulnerability Disclosure.

30: Disaster Management

Disaster Management prepares for and responds to large-scale cybersecurity incidents, ensuring preparedness, business continuity, and compliance. Planning, response, recovery, and review are key components.

- **Importance:** Preparedness and resilience, business continuity, regulatory compliance.
- **Best Practices:** Planning and preparedness, response and containment, recovery and restoration, review and improvement.
- **References:** CISA Emergency Preparedness, FEMA Disaster Management, NIST SP 800-34.

Cybersecurity Terminology

31: Misc. Errors

"Misc. Errors" refers to unspecified security incidents, ensuring comprehensive coverage, proactive defense, and continuous improvement. Incident classification, monitoring, and response plans are key.

- **Importance:** Comprehensive coverage, proactive defense, continuous improvement.
- **Best Practices:** Incident classification, monitoring and detection, response and mitigation.
- **References:** CISA Cybersecurity Best Practices, Splunk Security Incident Response, Fortinet Incident Response.

32: Privilege Misuse

Privilege Misuse involves improper use of access privileges, risking data protection, system integrity, and compliance. Least privilege, regular reviews, and incident response plans are key.

- **Importance:** Data protection, system integrity, regulatory compliance.
- **Best Practices:** Least privilege principle, regular reviews, incident response plans.
- **References:** CISA Access Control, NIST SP 800-16, SANS Institute Privilege Misuse.

33: Social Engineering

Social Engineering exploits human psychology to compromise security, targeting human vulnerability, offering versatility, and being cost-effective. User training, MFA, and filtering are key prevention strategies.

- **Importance:** Human vulnerability, versatility, cost-effectiveness.
- **Best Practices:** User training, multi-factor authentication, email and web filtering.
- **References:** CISA Social Engineering, SANS Institute Social Engineering, Palo Alto Networks Social Engineering.

Cybersecurity Terminology

34: Everything Else

"Everything Else" covers additional security measures, ensuring comprehensive coverage, adaptability, and resilience. Continuous monitoring, updates, and employee training are key.

- **Importance:** Comprehensive coverage, adaptability, resilience.
- **Best Practices:** Continuous monitoring, regular updates and patches, employee training.
- **References:** CISA Cybersecurity Best Practices, Splunk Security Incident Response, Fortinet Incident Response.

35: Lost/Stolen Asset

Lost/Stolen Asset refers to misplaced or unauthorized taken devices or data, risking data protection, system integrity, and compliance. Asset tracking, access controls, and encryption are key.

- **Importance:** Data protection, system integrity, regulatory compliance.
- **Best Practices:** Asset tracking, access controls, encryption.
- **References:** CISA Asset Inventories, SANS Institute Lost/Stolen Devices, Palo Alto Networks Data Exfiltration.

36: Misc. Errors (Repeated)

"Misc. Errors (Repeated)" again refers to unspecified security incidents, emphasizing comprehensive coverage, proactive defense, and continuous improvement. Incident classification, monitoring, and response plans are key.

- **Importance:** Comprehensive coverage, proactive defense, continuous improvement.
- **Best Practices:** Incident classification, monitoring and detection, response and mitigation.
- **References:** CISA Cybersecurity Best Practices, Splunk Security Incident Response, Fortinet Incident Response.

Cybersecurity Terminology

37: DoS (Denial of Service)

DoS attacks flood systems with traffic, causing unavailability and risking service disruption, data inaccessibility, and resource exhaustion. Traffic filtering, load balancing, and IDS are key prevention strategies.

- **Importance:** Service disruption, data inaccessibility, resource exhaustion.
- **Best Practices:** Traffic filtering, load balancing, intrusion detection systems.
- **References:** CISA DoS Attacks, SANS Institute DoS Attacks, Palo Alto Networks DoS Attack.