|  |
| --- |
| *Intelligence sources*: Examines open-source/proprietary/closed-source intelligence, timeliness, relevancy, accuracy.  *Confidence levels*: Importance of levels of confidence in data.  *Indicator management*: Introduces STIX, TAXII, and OpenIOC  **STIX**: Structured Threat Information eXpression (xml, OASIS, Org for Advancement of Structured Information Standards) | **TAXII**: Trusted Automated eXchange of Indicator Information (CTI over HTTPS) | 2 services: Collections (Req & Resp) & Channels (publish/subscribe) | Sharing: Hub/spoke (central clearing house), Source/subscriber (single source), Peer-to-peer |**OpenIOC**: machine-read | XML | classify forensic artifact | 500 predefined indicators  *Threat classification*: Known (identified w/ Antivirus signatures) vs Unknown (static/dynamic file analysis, old & recycled), zero-day (vuln in live env, routing traffic thru central security service, whitelisting, honeypots), APTs (targets specific entity over long duration, large corp or gov entity, well-funded, monitor logs & perf metrics)  *Threat actors*: nation-state (foreign gov), hacktivist (for a cause), organized crime (financial services), intentional and unintentional insider threats, terrorist groups (impact countries by using internet, damage critical infra)  Categories: Human | Natural | Technical | Physical | Environmental | Operational (processes that effect CIA)  *Intelligence cycle*: Requirements (relevant info) -> collection (hardwork, AI/ML, dashboard) -> analysis (timely, actionable, consistent | most-impactful skills) -> dissemination (communication | designer & builder) -> feedback  *Commodity malware*: Types of malware that commonly infect networks | not modified & publicly available  Advanced malware: APT uses this | custom-created  *Info sharing & analysis communities*: Data sharing among healthcare (H-ISAC), financial (GLBA, FS-ISAC), aviation (CISA, AGCC/ASCC), gov (CISA), and critical infra (ENISA). |

|  |
| --- |
| *Attack frameworks*: **MITRE ATT&CK** (kb of adversary tactics & techniques, can develop specific threat models like SaaS matrix): Initial access, Persistence, Privilege Escalation, Defense Evasion, Cred Access, Discovery, Lateral Mov, Collection | **Diamond model of Intrusion Analysis**: (Adversary: Intent of attack, Infra: Set of systems to launch attack, Victim: Single or multiple, Capabilities: Intrusion tools & techniques) | **Kill chain**: Intrusion identification & prevention model (L. Martin), stages of intrusion: Recon, Weapon (put malware into payload), Delivery, Exploit (weapon triggered), Install (weapon installs persistent backdoor), C&C (server communication), Action on Objective (actual goal like exfil or destruction of data/system).  *Threat research*: **Type of threat data**: *Reputational* (past activities, IPs, Domains, URLs) & *behavioral* [(by traffic anomalies, User Entity Behavior Analytics: UEBA, Heuristics (guessing, ranks alternatives, approximate, self-learning, trial & error)], **IoC** [(activity, artifact, log entry): Virus sig, Known malicious file types, Domain names of botnets, uses Traffic Light Protocol (TLP) to classify IoC, 4 colors], **CVSS** [rank vuln, 0.1-3.9 low, 4.0-6.9 medium, 7.0-8.9 high, 9.0-10.0 critical,  **Base** (constant): Attack Vector (Local, Adjacent, Network, Physical) | Attack Complexity (High, Low) | Privileges Req (High, Low, None) | User Interaction (None, Required) | Scope & **Impact**: Availability, Confidentiality, Integrity (None, Low, High) & **Temporal** (change) & **Environmental** metrics]: CVSS2#AV:L/AC:H/Pr:L/UI:R/S:U/C:L/I:N/A:N  *Threat modeling*: Adversary capabilities (Internal [employee, partner, gov spy, vendor, thief] vs External [Anarchist, Competitor, Data miner, corrupt gov official, legal adversary, Mobster, Activist, Terrorist, Vandal]) non-hostile or hostile, Analyze actors by Skill level: None, minimal, operational, adept | Resources: Individual, team, organization, government | Limits: Code of conduct, legal, extra-legal (minor), extra-legal (major) | Visibility: Overt, covert, clandestine, don’t care | Objective: Copy, destroy, injure, take, don’t care | Outcome: Acquisition/theft, business advantage, damage, embarrassment, technical advantage.  Total attack surface, attack vector (path/means of attack: phishing, malware, code injection, social engineering, APTs), impact (high/medium/low), likelihood (risk matrix)  *Threat intel sharing w/ supported functions*: Incident resp, vuln & risk mgmt., security eng, detection & monitor. |

|  |
| --- |
| *Vulnerability identification*: asset criticality (sensitivity), active [block attack]/passive [gather info] scan, mapping/enumeration (listing vulns, CWE, > 600 categories, by SCAP) | Validation: True Positive, False Positive, True Negative, False Negative | *Remediation/Mitigation*: Config baseline, patching, hardening, compensate control (countermeasures or safeguard. E.g. ACL), risk acceptance (avoid, transfer, mitigate, accept), mitigation [patch, permissions, scanning, verify logs] | Steps: priority/schedule -> validate in test -> Install -> validate in prod  *Scanning parameters and criteria*: vuln feed (RSS), scope, cred/non-cred scan, server[push]/agent[pull] based scan, IPS/IDS | **Risks with scan**: False sense of security, rely on known vuln/latest updates, identify vuln itself doesn’t reduce risk | Special considerations: Types of data, technical constraints, Workflow, Sensitivity levels (Discovery scans, Assessment scans) | Regulatory reqs: Finance, Medical, Retail [SOX for publicly traded, HIPPA: Kennedy-Kassebaum Act & enfoced by OCR & for PHI, GLBA 1999: Financial and PII, PCI-DSS] | Segmentation (VLANs, Security borders) | IDS/IPS, Firewall settings | **Signature based** (Pattern or Stateful match), **Anomaly based** (Statistical, Protocol, Traffic), **Rule or Heuristic based** (expert system, uses KB, rule-based programming IF/THEN) | HIDS/NIDS | **Firewall** (packet-filtering [only header inspection], stateful-inspection (TCP handshake, track of session), proxy firewall [circuit-level proxy (OSI layer 5, SOCKS), app-level proxy (OSI layer 7)], Dynamic packet filtering [adds rule to the list, doesn’t describe f/w type, describes functionality], kernel-proxy firewall (5th generation f/w), inspects every-layer of OSI) | Bastion host (computer that 1st connects to internet) | dual-homed f/w (2 n/w interfaces, internal & external, routing between them is OFF, **risk of SPOF**) | screen-subnet (2 firewalls) | **three-legged f/w**: 1 to internet, 1 to internal n/w, 1 to DMZ)  *Inhibitors to remediation*: MOU (not legal, agreement), SLA (service expectation), Op Gov (process, org activities, red-tape mgmt), business process interruption, degrading functionality, legacy, proprietary systems |

|  |
| --- |
| *Web application scanner*: ZAP, BurpSuite, Nikto [Windows, Perl, Fast], Arachni [Ruby, all OS]| Synthetic transaction monitoring (STM) vs Real user monitoring (RUM)  *Infra vuln scan* (misconfig, out-of-date s/w, missing patch, open ports): Nessus, OpenVAS (Linux, NVT, Greenbone console), Qualys.  *Software assessment tools and techniques*: SDLC (Plan, Req, Design, Develop, Test, Release, Certify, Change mgmt), Static analysis (**code review** [formal (tough, line-by-line) & lightweight (Pair, email, shoulder, tool)] **& testing thru out SDLC**)[bad prog pattern, misconfig, bugs, logic flaws] (data flow analysis, control flow graph, taint analysis (user i/p variables), lexical analysis[tokens, abstract code]), dynamic analysis, reverse engineering (IEEE, apply to IR & malware analysis), fuzzing (inject faults) [mutation vs. generation-based] (Prevent fault injection: Do fuzz, safe coding and proj mgmt. practices, WAF).  *Enumeration*: Discover & list Info. **Nmap** (flags: URG, ACK, PSH, RST, SYN, FIN) [**null scan** **-sN** (seq 0 and no flags)(no resp: port open, RST: port closed), **FIN scan** **-sF** (No resp: port open, RST/ACK: port closed), **XMAS scan** **-sX** FIN/PSH/URG flags set (no resp: port open, RST: port closed)], Host/Ping scan (**-sP**), **sudo** **hping3 -i u1** (wait1 microsecond for packet) (tcp/udp/icmp/raw-ip, traceroute mode) [f/w test, port scan, n/w test, MTU discover, Remote OS fingerprint, uptime guess, tcp/ip stack guess, adv traceroute], DoS (SYN flood), active vs. passive enumeration, Responder (Windows LLMNR, NBT-NS)[obtain hashes, creds].  *Wireless assessment tools*: **Aircrack-ng** (Monitor, Attack, Test, Crack), **Reaver** (attack WPS, **wash**: WPS scan), **oclHashcat** (GP-GPU based multi-hash cracker, bruteforce).  *Cloud infrastructure assessment tools*: **ScoutSuite** (data collection, longitudinal survey panels) (all CSPs), **Prowler** (AWS, Assess/Audit/Forensic readiness/Harden), **Pacu** (AWS exploit framework) [Enumerate/Priv esc/Data exfil/Serv Exploit/Log manipulate]. |

|  |
| --- |
| **Mobile** (MDM/MAM) [Threats: Insecure web browsing, Insecure Wi-Fi connectivity, Lost or stolen devices holding company data, Corrupt application downloads & installations, Missing security patches, Constant upgrading of personal devices, Use of location services, BYOD policies, USB-OTG (USB host), Push Notification Services (Do not send confidential or IP data, Do not store SSL cert & tokens in web-root, Do not expose APN certs or device tokens), Geotagging (add location metadata to media, enabled by default), Android fragmentation (too many versions), Mobile payment (NFC [interception possible]: lock device, stop NFC when unuse, use RFID/NFC blocking device, scan mobile for spyware/apps), Inductance (used in NFC, transmit info, coils made of ferrite, EMI), Mobile wallet (paypal, AMZ payment, PIN used to authorize payments on card), Peripheral-Enabled payments (remote locations like cabs, food trucks, flea markets), Unauthz Domain Bridging (hotspot)  **IoT** (smart home, Wearables, Smart cities, Connected cars, Business automation [HVAC, fire detect]) (Secure logs of IoT devices, encrypted protocols, secure pwd policy, vLANs, update device firmware) (*vendor side*: design privacy & security, bug bounty program / vuln report mechanism, manual overrides for disconnected operations)  **Embedded** (small s/w on large s/w) | **Real-time OS** (process data as it comes w/o delay, **IoT devices use RTOS**) e.g. VxWorks 6.5 | **System-on-Chip (SoC)** (lower energy use, in cell phones, *baseband processor chip* for radio, own RAM/Firmware), **Field programmable gate array (FPGA)** (type of PLD, high-voltage, *cloud-scenarios/IoT*) | **Physical access control** (mantrap w/ proximity readers, IP-based access control/video systems [high bandwidth, QoS/Perf, Storage, high initial cost]) | **Building automation systems** (Lighting, HVAC, Water, Security alarms) (*wireless issues*: Inference/Security/Power), *BACnet* (control n/w for app/network/**MAC** layer service, 4byte IP & 2byte UDP port), Sensors (gather info to large system)| **Vehicles & drones** (CAN controller area n/w bus: allows to vehicle devices to talk without host, no security at all) | **Workflow & process automation systems** (puppet/chef/ansible) | **Incident Command Systems** (ICS) (**FEMA**) (domestic IM) | Supervisory control & data acquisition (SCADA, ICS): coded signals, ICS components (sensors, *RTUs* (w/ telemetry h/w), *PLCs* (w/o telemetry h/w), *Telemetry system* (RTUs & PLCs), *Human interface*) (Stuxnet hit SCADA), control physical & logical access, protect exploitation, unauthz modify, detect security events/incidents, maintain func during adverse conditions, Restore system after incident.  ICS implements: Modbus (port 50), BACnet (port 47808), LonWorks/LonTalk (port 1679), DNP3 (port 1999/2000) | use Zigbee or Bluetooth or IEEE 802.1X |