SOC Architecture Requirements

Drew Blandford-Williams

1. SOC Charter
   Definition & Primary Objective of the <<CLIENT>>Security Operations Center:

   a. Capture, Analyze & Monitor all data and traffic activity for security assessment, response and mitigation purposes;
   b. Monitor and defend the enterprise against all measures of cyberattack;
   c. Track and audit *Privileged User Accessibility* and access to all proprietary content/elements throughout the organization;
   d. Provide immediate response, mitigation and resolution to <u>all</u> security events;
   e. Develop, maintain and continually revise/ensure SOC processes comply with industry best practices and ISO27K standards.

2. <<CLIENT's>> SOC "Mission"
   Should be to:

   a. Prevent of cybersecurity incidents through proactive:
      i. Continuous threat analysis;
      ii. Network & host scanning for vulnerabilities;
      iii. Countermeasure deployment coordination;
      iv. Security policy and architecture consulting.
   b. Monitor, detect, analyze potential intrusions in real time and through historical trending on security-relevant data sources;
   c. Respond to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures;
   d. Provide situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior to appropriate organizations;
   e. Engineer and operate Computer Network Defense technologies such as IDS's and data collection/analysis systems;
   f. Provide a means for constituents to report suspected cybersecurity incidents;
   g. Provide incident handling assistance to constituents;
   h. Disseminate incident-related information to constituents and external parties.

3. Fundamentals

   a. TIER ONE PROCESSES
      Collection & Reporting/Escalation I

      i. Central repository for ALL security logs being collected
         1. Access Logs
         2. Application Logs
         3. Firewall Logs
         4. IDS / IPS Logs (including firewalls & routers)
         5. Switch Logs
         6. Server Logs
         7. VA Scanner Logs

8. Net Traffic Flow
9. External Data Sources

ii. Responses include:
1. Authentication of data collected
2. Evaluation of events flagged
3. Notification of incidents
4. Resolution
5. Escalation to Tier Two Analysts (“Triage”)
6. Documentation

b. TIER TWO PROCESSES
Collaboration & Evaluation/Escalation II

i. Aggregation of files and log data
1. Sanitized files
2. Assessment & Filtering of Extemporaneous Information

ii. Normalization of Logs
1. What is “Expected”
2. What are “Anomalies”

iii. Correlation of data from collection sources
1. Should be as automated as possible
2. Requires comprehensive rule sets & application algorithms

iv. Begin any appropriate forensics pathology needed

v. Responses include:
1. Validation of reported activity
2. Evaluation of events flagged
3. Collaboration with Tier One analysts
4. Resolution of open ticket
5. Escalation to Tier Three Security Engineers (“Triage”)
6. Initiate a DRP or Containment Strategy
7. Documentation

c. TIER THREE PROCESSES
Risk-based Prioritization of data (automated with “Eyes-on” layer)

i. Bug/Patch/Hack ID (CVE, Etc.)

ii. INCIDENT EVALUATION
1. Collaboration with Tier Two Analyst team
2. Remediation
3. Resolution & Incident Report
4. Escalation to SOC Supervisor(s)
5. Prepare responses for legal evaluation
6. Coordinate event response for public release

d. Automated as fully as it can be
i. Dell SecureWorks
ii. Endpoint Threat & Attack Tracerouting & Forensics

iii. Automated Firewall rulesets
iv. NIDS / HIDS Policies & Rulesets

e. Ensure the confidentiality, integrity, and availability throughout the <<CLIENT>> enterprise should be the principle objective.

2. Task-oriented Analytics & Activities

a. Should incorporate SPECIFIC tasks, which include (but are not limited to):
    i. Systemwide Status/Health Checking
    ii. Audit sampling from cyber security and traffic flow applications/devices
    iii. Scheduled review of remediation tactics and ticketing process
    iv. SIEM *Tweaking* (MITRE "Red Queen")
    v. Configuration management (CM) monitoring and remediation
    vi. Sandboxing (in an autonomous testing lab)
    vii. Effective cybersecurity AND information assurance (IA) policy implementation
    viii. Maintaining & Recertifying SOC team
    ix. Comprehensive workforce training (Top to Bottom)
    x. Ensure all SOC staff is contributing to attain baseline ISO27K Security Compliance
b. Security 360° Analysis
    i. System Integrity
        1. Data Security
            a. Encryption
            b. Log Monitoring
            c. Token/Authentication
        2. Application Security
            a. WAS
                i. OWASP Top 20
                ii. SANS Top 20 WAS
            b. Database Monitoring
            c. Content Security
            d. Secure File Transfer Protocols
        3. O/S Security
            a. Microsoft Security
                i. Patches & Updates
            b. UNIX / RedHat
                i. Default Services
                ii. ROOT Privilege Access
        4. Network Security
            a. Firewall Management
                i. Rulesets
                ii. NextGen
            b. NAC
            c. IDS/IPS
                i. False Reporting remediation/reduction
                ii. DDoS Mitigation & Contingency
    ii. Advance Threat Protection

1. APT/Zero-day Exploits
2. Botnet / Ransomware Contingencies
3. Whitelisting
4. Attack Emulation
    a. Sandboxing
    b. Test Lab

iii. Infrastructure Security
1. DNS Security
2. Mail Security

iv. Mobile Access & Integrity
1. Authentication
2. Rogue Access Monitoring
3. Wireless & BYO* Protocols

v. GRC
1. SIEM + (Compliance Rule sets)
2. Firewall Compliance
3. Vulnerability Management
4. Pen-Testing & Integrity Management
5. Configuration Management & Compliance

vi. Cloud Security
1. CSA Top 10
2. Cloud Service SLAs
3. Third-party Connectivity & Monitoring
    a. Customers
    b. Vendors
    c. Service Providers
    d. Auditors

3. Five-tier SOC Response-Defense-Countermand Architecture
    a. Baseline Defense
        i. Establish solid technology rollout plans for security tools
            1. SIEM
            2. IDS / IPS
            3. Firewalls
            4. Routers / Switches
            5. Misc Applications
            6. SLA Reviews & Updates
            7. SAAS(?)
    b. Proactive Risk Management & Contingency Planning
        i. Identify, Resolve & Anticipate Known Attack Protocols
            1. OWASP Top 10
            2. CSA Top 10
            3. SANS TOP 10
            4. FBI Top 10

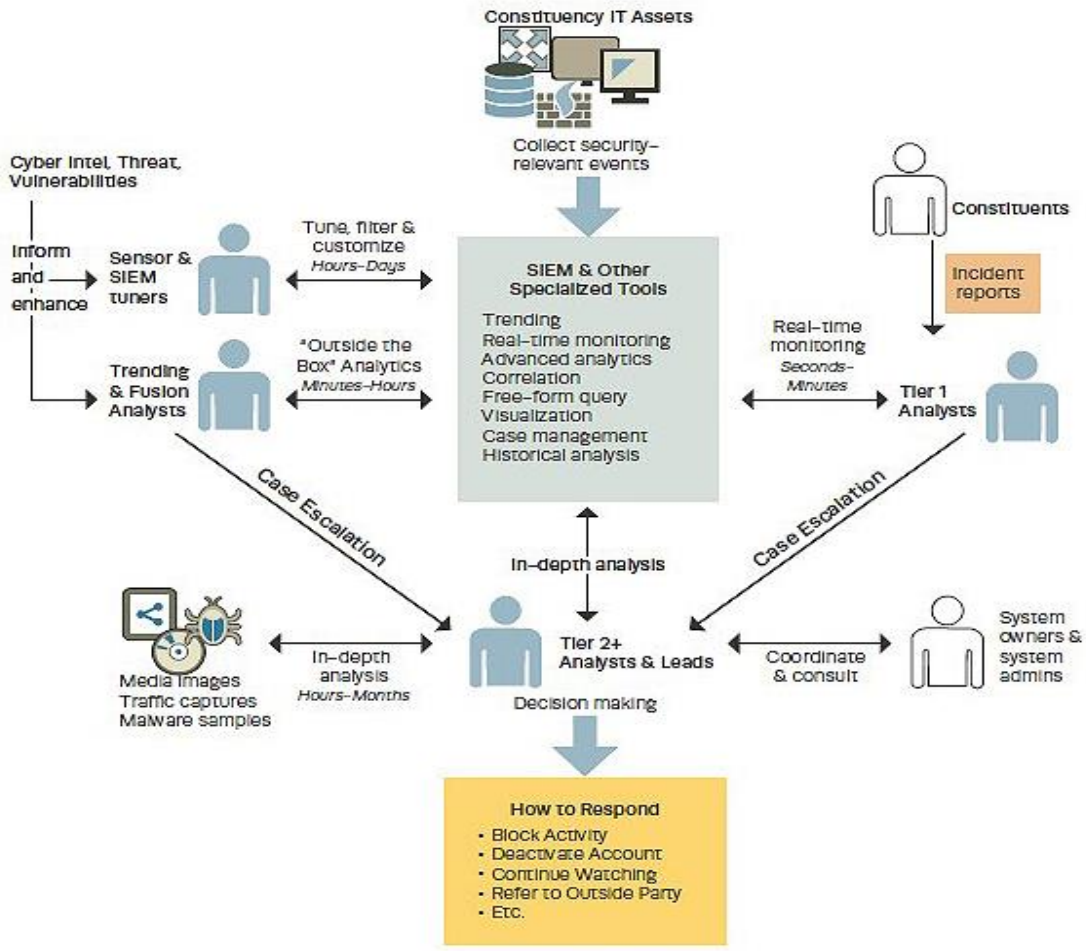
ii. Identify Known Vulnerabilities
    1. Configuration Management
    2. Network Vulnerabilities
    3. Application Flaws
    4. Patch Management

c. Active Countermeasures against APTs
    i. Zero-day Attack Profile & Analysis
    ii. Sandboxing & Pre-attack Scenarios

d. WhiteHat Management & Skills
    i. Train Staff on Relevant Content
    ii. Coordinate and Establish a CIRT
        1. Know THEY know who they are
        2. Roles & Responsibilities
        3. Lead the Drills
    iii. Rotation of Teams Keeps SOC "Fresh"
    iv. Define, Articulate & Understand Roles & Rules
        1. Who does what?
        2. What Gets Escalated?
        3. Who Gets Contacted?
        4. What happens "Next?"

e. Defense Mechanisms
    i. Active Segment Testing
        1. In real-time
    ii. Controlled Intrusion Tests (CIT)
        1. Internal breach
        2. External Penetration
    iii. Triage
        1. Environmental
        2. "Stupid User Tricks"
        3. Malicious or Hostile Attack

4. Graphic Representation of what the <<CLIENT>> SOC Process SHOULD resemble:



5. <<CLIENT>> SOC Functionality & Capabilities
    a. Real-time Analysis
        i. Call Center
            1. Tips, incident reports, and requests for CND services from constituents received via phone, email, SOC website postings, or other methods.
            2. This is roughly analogous to a traditional IT help desk, except that it is CND specific.
        ii. Real-Time Monitoring and Triage
            1. Triage and short-turn analysis of real-time data feeds (such as system logs and alerts) for potential intrusions.
            2. After a specified time threshold, suspected incidents are escalated to an incident analysis and response team for further study.
            3. Usually synonymous with a SOC's Tier 1 analysts, focusing on real-time feeds of events and other data visualizations.
    b. Intel-gathering & Trending
        i. Cyber-intelligence Collection / Analysis
            1. Collection, consumption, and analysis of cyber intelligence reports, cyber intrusion reports, and news related to information security, covering new threats, vulnerabilities, products, and research.

2. Materials are inspected for information requiring a response from the SOC or distribution to the constituency. Intel can be culled from coordinating SOCs, vendors, news media websites, online forums, and email distribution lists.

ii. Cyber-intelligence Distribution
    1. Synthesis, summarization, and redistribution of cyber intelligence reports, cyber intrusion reports, and news related to information security to members of the constituency on either a routine basis (such as a weekly or monthly cyber newsletter) or a non-routine basis (such as an emergency patch notice or phishing campaign alert).

iii. Cyber-intelligence Creation
    1. Primary authorship of new cyber intelligence reporting, such as threat notices or highlights, based on primary research performed by the SOC. (For example, analysis of a new threat or vulnerability not previously seen elsewhere.)
    2. This is usually driven by the SOC's own incidents, forensic analysis, malware analysis, and adversary engagements.

iv. Trending
    1. Long-term analysis of event feeds, collected malware, and incident data for evidence of malicious or anomalous activity or to better understand the constituency or adversary TTPs.
    2. This may include unstructured, open-ended, deep-dive analysis on various data feeds, trending and correlation over weeks or months of log data, "low and slow" data analysis, and esoteric anomaly detection methods.

v. Threat Assessment
    1. Holistic estimation of threats posed by various actors against the constituency, its enclaves, or lines of business, within the cyber realm.
    2. This will include leveraging existing resources such as cyber intel feeds and trending, along with the enterprise's architecture and vulnerability status.
    3. Often performed in coordination with other cybersecurity stakeholders.

c. Real-time Analysis

i. Call Center Operations
    1. Tips, incident reports, and requests for CND services from constituents received via phone, email, SOC website postings, or other methods.
    2. This is roughly analogous to a traditional IT help desk, except that it is CND specific.

ii. Real-time Monitoring & Triage
    1. Triage and short-turn analysis of real-time data feeds (such as system logs and alerts) for potential intrusions.
    2. After a specified time threshold, suspected incidents are escalated to an incident analysis and response team for further study.
    3. Usually synonymous with a SOC's Tier 1 analysts, focusing on real-time feeds of events and other data visualizations.

d. Incident Analysis & Response

i. Incident Analysis

1. Prolonged, in-depth analysis of potential intrusions and of tips forwarded from other SOC members.
2. This capability is usually performed by analysts in tiers 2 and above within the SOC's incident escalation process.
3. It must be completed in a specific time span so as to support a relevant and effective response.
4. This capability will usually involve analysis leveraging various data artifacts to determine the who, what, when, where, and why of an intrusion—its extent, how to limit damage, and how to recover.
5. An analyst will document the details of this analysis, usually with a recommendation for further action.

ii. Tradecraft Analysis
1. Carefully coordinated adversary engagements, whereby SOC members perform a sustained "down-in-the-weeds" study and analysis of adversary TTPs, in an effort to better understand them and inform ongoing monitoring.
2. This activity is distinct from other capabilities because:
    a. It sometimes involves ad hoc instrumentation of networks and systems to focus on an activity of interest, such as a honeypot, and
    b. An adversary will be allowed to continue its activity without immediately being cut off completely.
3. This capability is closely supported by trending and malware and implant analysis and, in turn, can support cyber-intelligence creation.

iii. Incident Response Coordination
1. Work with affected constituents to gather further information about an incident, understand its significance, and assess mission impact.
2. More important, this function includes coordinating response actions and incident reporting. This service does not involve the SOC directly implementing countermeasures.

iv. Implementation of Countermeasures
1. Actual implementation of response actions to an incident to deter, block, or cut off adversary presence or damage.
2. Possible countermeasures include logical or physical isolation of involved systems, firewall blocks, DNS black holes, IP blocks, patch deployment, and account deactivation.

v. On-site Incident Response
1. Work with constituents to respond and recover from an incident on-site.
2. This will usually require SOC members who are already located at, or who travel to, the constituent location to apply hands-on expertise in analyzing damage, eradicating changes left by an adversary, and recovering systems to a known good state.
3. This work is done in partnership with system owners and sysadmins.

vi. Remote Incident Response
1. Work with constituents to recover from an incident remotely.
2. This involves the same work as on-site incident response.

3. However, SOC members have comparatively less hands-on involvement in gathering artifacts or recovering systems.
4. Remote support will usually be done via phone and email or, in rarer cases, remote terminal or administrative interfaces such as Microsoft Terminal Services or Secure Shell (SSH).

e. Artifact Analysis
    i. Forensic Artifact Containment & Management
        1. Gathering and storing forensic artifacts (such as hard drives or removable media) related to an incident in a manner that supports its use in legal proceedings.
        2. Depending on jurisdiction, this may involve handling media while documenting chain of custody, ensuring secure storage, and supporting verifiable bit-by-bit copies of evidence.
    ii. Malware Reverse Engineering
        1. Extracting malware (viruses, Trojans, implants, droppers, etc.) from network traffic or media images and analyzing them to determine their nature.
        2. SOC members will typically look for initial infection vector, behavior, and, potentially, informal attribution to determine the extent of an intrusion and to support timely response.
        3. This may include either static code analysis through de-compilation or runtime/execution analysis (e.g., “detonation”) or both.
        4. This capability is primarily meant to support effective monitoring and response.
        5. Although it leverages some of the same techniques as traditional “forensics,” it is not necessarily executed to support legal prosecution.
    iii. Forensic Artifact Analysis
        1. Analysis of digital artifacts (media, network traffic, mobile devices) to determine the full extent and ground truth of an incident, usually by establishing a detailed timeline of events.
        2. This leverages techniques similar to some aspects of malware and implant analysis but follows a more exhaustive, documented process.
        3. This is often performed using processes and procedures such that its findings can support legal action against those who may be implicated in an incident.

f. SOC Tool Lifecycle Support
    i. Border Protection Device Operation & Maintenance
        1. Operation and maintenance (O&M) of border protection devices (e.g., firewalls, Web proxies, email proxies, and content filters).
        2. Includes updates and CM of device policies, sometimes in response to a threat or incident.
        3. This activity is closely coordinated with a NOC.
    ii. SOC Infrastructure Operation & Maintenance
        1. O&M of SOC technologies outside the scope of sensor tuning.
        2. This includes care and feeding of SOC IT equipment: servers, workstations, printers, relational databases, trouble-ticketing systems, storage area networks (SANs), and tape backup.

3. If the SOC has its own enclave, this will likely include maintenance of its routers, switches, firewalls, and domain controllers, if any.
4. This also may include O&M of monitoring systems, operating systems (OSes), and hardware.
5. Personnel who support this service have "root" privileges on SOC equipment.

iii. Sensor Tuning & Maintenance
1. Care and feeding of sensor platforms owned and operated by the SOC: IDS, IPS, SIEM, etc.
2. This includes updating IDS/IPS and SIEM systems with new signatures, tuning their signature sets to keep event volume at acceptable levels, minimizing false positives, and maintaining up/down health status of sensors and data feeds.
3. SOC members involved in this service must have a keen awareness of the monitoring needs of the SOC so that the SOC may keep pace with a constantly evolving consistency and threat environment.
4. Changes to any in-line prevention devices (HIPS/NIPS) are usually coordinated with the NOC or other areas of IT operations.
5. This capability may involve a significant ad hoc scripting to move data around and to integrate tools and data feeds.

iv. Custom Signature Creation
1. Authoring and implementing original detection content for monitoring systems (IDS signatures, SIEM use cases, etc.) on the basis of current threats, vulnerabilities, protocols, missions, or other specifics to the constituency environment.
2. This capability leverages tools at the SOC's disposal to fill gaps left by commercially or community provided signatures.
3. The SOC may share its custom signatures with other SOCs.

v. Tool Engineering & Deployment
1. Market research, product evaluation, prototyping, engineering, integration, deployment, and upgrades of SOC equipment, principally based on free or open source software (FOSS) or commercial off-the-shelf (COTS) technologies.
2. This service includes budgeting, acquisition, and regular recapitalization of SOC systems.
3. Personnel supporting this service must maintain a keen eye on a changing threat environment, bringing new capabilities to bear in a matter of weeks or months, in accordance with the demands of the mission.

vi. Tool Research & Development
1. Research and development (R&D) of custom tools where no suitable commercial or open source capability fits an operational need.
2. This activity's scope spans from code development for a known, structured problem to multiyear academic research applied to a more complex challenge.

g. Audit & Insider Threat Assessment/Mitigation
i. Audit Data Collection & Distribution

1. Collection of a number of security-relevant data feeds for correlation and incident analysis purposes.
2. This collection architecture may also be leveraged to support distribution and later retrieval of audit data for on-demand investigative or analysis purposes outside the scope of the SOC mission.
3. This capability encompasses long-term retention of security-relevant data for use by constituents outside the SOC.

ii. Audit Content & Creation Management
1. Creation and tailoring of SIEM or log maintenance (LM) content (correlation, dashboards, reports, etc.) for purposes of serving constituents' audit review and misuse detection.
2. This service builds off the audit data distribution capability, providing not only a raw data feed but also content built for constituents outside the SOC.

iii. Insider Threat Case Support
1. Support to insider threat analysis and investigation in two related but distinct areas:
    a. Finding tip-offs for potential insider threat cases (e.g., misuse of IT resources, time card fraud, financial fraud, industrial espionage, or theft).
    The SOC will tip off appropriate investigative bodies (law enforcement, Inspector General [IG], etc.) with a case of interest.
    b. On behalf of these investigative bodies, the SOC will provide further monitoring, information collection, and analysis in support of an insider threat case.

iv. Insider Threat Case Investigation
1. The SOC leveraging its own independent regulatory or legal authority to investigate insider threat, to include focused or prolonged monitoring of specific individuals, without needing support or authorities from an external entity.
2. In practice, few SOCs outside the law enforcement community have such authorities, so they usually act under another organization's direction.

h. Scanning & Assessment
i. Network Mapping
1. Sustained, regular mapping of constituency networks to understand the size, shape, makeup, and perimeter interfaces of the constituency, through automated or manual techniques.
2. These maps often are built in cooperation with—and distributed to—other constituents.

ii. Vulnerability Scanning
1. Interrogation of consistency hosts for vulnerability status, usually focusing on each system's patch level and security compliance, typically through automated, distributed tools.
2. As with network mapping, this allows the SOC to better understand what it must defend.
3. The SOC can provide this data back to members of the constituency—perhaps in report or summary form.

4. This function is performed regularly (not part of a specific assessment).

iii. Vulnerability Assessment
   1. Full-knowledge, open-security assessment of a constituency site, enclave, or system, sometimes known as “Blue Teaming.”
   2. SOC members work with system owners and sysadmins to holistically examine the security architecture and vulnerabilities of their systems, through scans, examining system configuration, reviewing system design documentation, and interviews.
   3. Activity may leverage network & vulnerability scanning tools, plus more invasive technologies used to check systems for configuration and status.
   4. Team members produce a report of their findings & remediation.
   5. SOCs leverage vulnerability assessments as an opportunity to expand monitoring coverage and their analysts’ knowledge of the constituency.

iv. Penetration Testing
   1. Red Teaming (having no knowledge or limited-knowledge assessment of a specific area of the constituency).
   2. Members of the SOC conduct a simulated attack against a segment of the constituency to assess the target’s resiliency to an actual attack.
   3. These operations usually are conducted only with the knowledge and authorization of the highest level executives within the consistency and without forewarning system owners.
   4. Tools used will actually execute attacks through various means:
      a. Buffer Overflows,
      b. Structured Query Language (SQL) injection,
      c. Input fuzzing.
   5. Red Teams usually will limit their objectives and resources to model that of a specific actor, perhaps simulating an adversary’s campaign that might begin with a phishing attack.
   6. When the operation is over, the team will produce a report with its findings, in the same manner as a vulnerability assessment.
   7. However, because penetration testing activities have a narrow set of goals, they do not cover as many aspects of system configuration and best practices as a vulnerability assessment would.
   8. In some cases, SOC personnel will only coordinate Red-Teaming activities, with a designated third party performing most of the actual testing to ensure that testers have no previous knowledge of constituency systems or vulnerabilities

6. DEFINITIONS:
   a. CND
      i. Computer Network Defense
   b. CM
      i. Configuration Management
   c. IA

i. Information Assurance

d. CSOC
    i. Cybersecurity Operations Center
e. CSIRC
    i. Computer Security Incident Response Capability
f. CSIRT
    i. Computer Security Incident Response Team
        1.