Phenomenati's
Taxonomy of a SOC™

A Reference Model of operational needs
to guide the evolution of Security Operations

Conflict - Risk - Intelligence - Decisions

SOC Taxonomy – for Cybersecurity Operations

Challenge

- Convergence on a capability reference model for Cyber Security Operations has yet to materialize

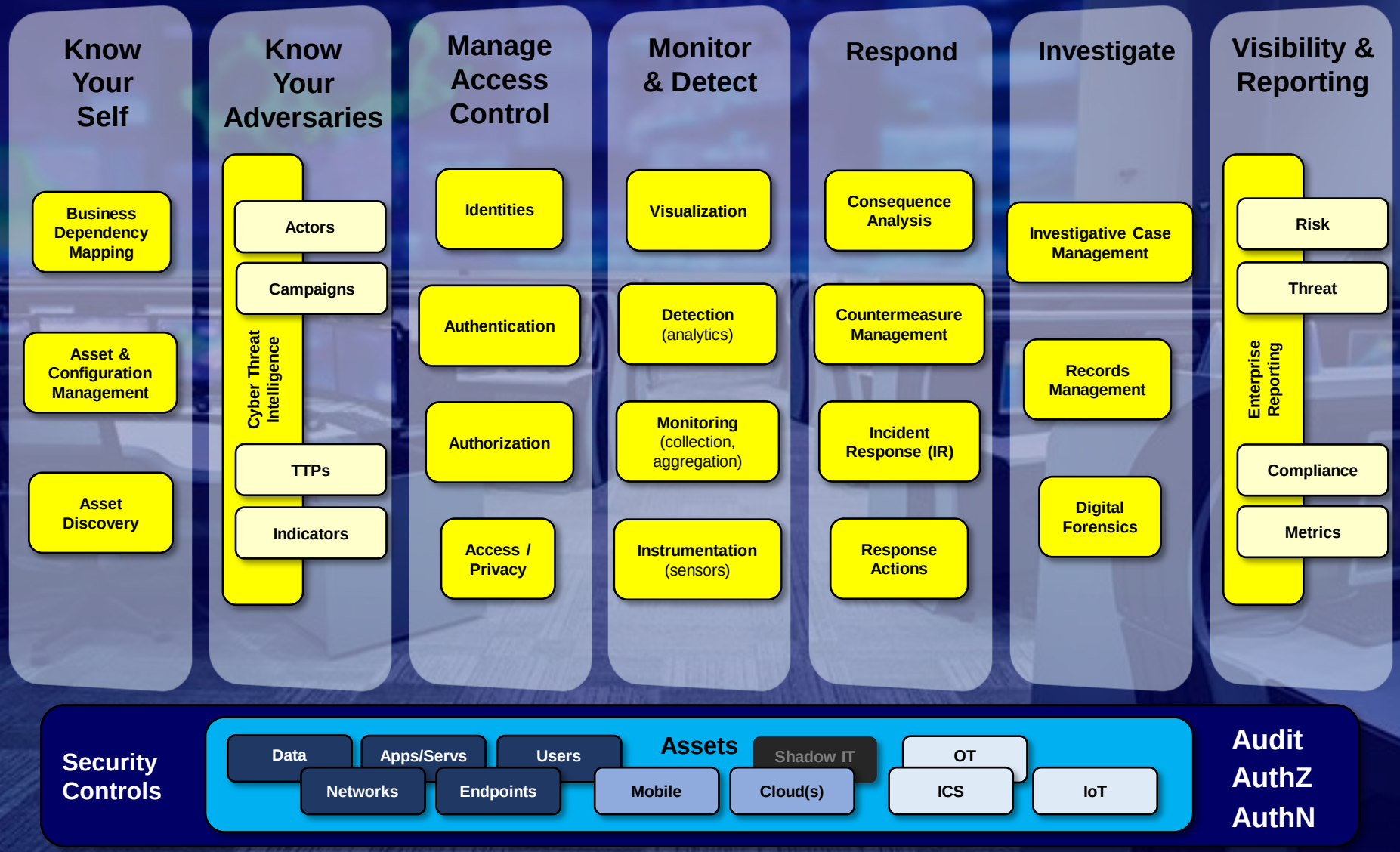
Response

- A summary of the top 20 capabilities found in more mature Cyber Security Operations Centers (SOCs)
- Grouped by the 7 challenges every cyber security operations effort ultimately needs to address

Intended Usage

- Educate Senior Leadership (execs, board) on breadth of Security Operations
- Foundation for Planning and Prioritizing capabilities
- Baseline Functional Requirements for Acquiring specific capabilities

SOC Taxonomy – for Cybersecurity Operations



Challenge #1 – Know Your Self (a-la Sun Tzu)

Cap Area #1 – Asset & Configuration Management

Challenge

- You can't secure/defend what you don't know about

Response

- Asset & Configuration Management (ACM) processes and capabilities
  - e.g., A Configuration Management System (CMS)
- Vulnerability (Patch) Lifecycle Management (VLMS) processes/capabilities

Caveats

- ACM/CMS are ***not*** the responsibility of Security Operations
  - However, Security Operations do have a critical dependency on this info
- Scope Creep:
  - "Mobile" devices, apps, and data; "Cloud" apps, data, etc.
  - Operational Technology (OT) and Industrial Control Systems (ICS)
- VLMS is basic hygiene; ***not*** a panacea; ***not*** a useful perspective of Risk

Cap Area #2 – Asset Discovery

Challenge

- "Cyber Entropy": shadow IT, virtualized assets, cloud apps, smart IoT devices, etc.

Response

- Continuous Asset Discovery capabilities
- Regular wireless "site surveys"

Caveats

- Asset Discovery is ***not*** the responsibility of Security Operations
- But "Cyber Entropy" creates an ever-expanding attack surface

Cap Area #3 – Business Dependency Mapping

Challenge

- "Context is Everything"
  - Decisions made without Context are, at best, educated guesses

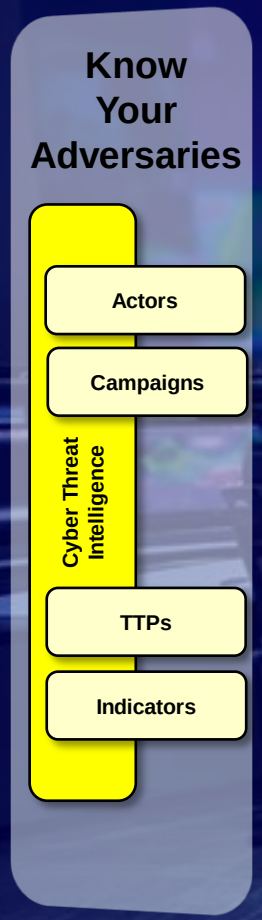
Response

- Business Dependency Mapping processes and capabilities

Caveats

- Mapping the organization's mission-critical dependencies should ***not*** be the responsibility of Security Operations
- But knowledge of *dependencies* is critical to expose consequences, prioritize incident response, and inform cybersecurity decisions
- Discovering and describing dependencies is ***NOT*** automatable

Challenge #2 – Know Your Adversaries



Cap Area #4 – Cyber Threat Intelligence

Challenges

- You can't defend against what you don't know about
- Your adversaries evolve daily
  - their capabilities, tactics, techniques, and procedures (TTP)

Response

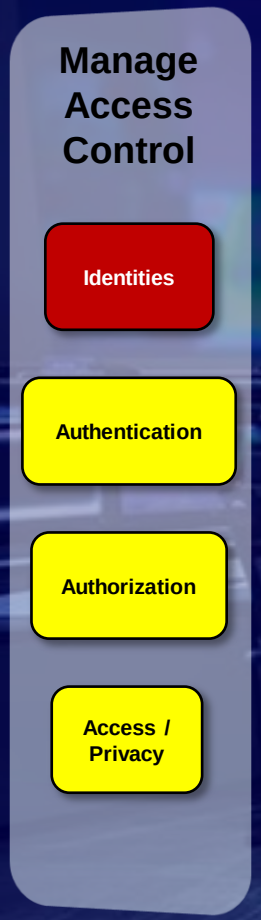
- Cyber Threat Intelligence (CTI) processes and capabilities
  - e.g., the Cyber "Kill Chain™"; Indicators of XXX (recon, attack, compromise, etc.)
  - e.g., Threat Intelligence Platforms (TIP)
  - e.g., Threat Intelligence sharing and standards (STIX, TAXII)
  - e.g., Threat Intelligence Sharing & Analysis Centers (ISACs)

Caveats

- An extension of earlier "signature-based" defense
- Attackers will always be ahead of defenders
- Attribution is more "*art*" than "*science*"

Challenge #3 – Manage Access Controls

Cap Area #5 – Identity Management



Challenges

- Need unique identities for everything in the environment
  - Both person and non-person entities (devices, files, processes, etc.)
- Need to provision, manage, and maintain identities for long periods of time

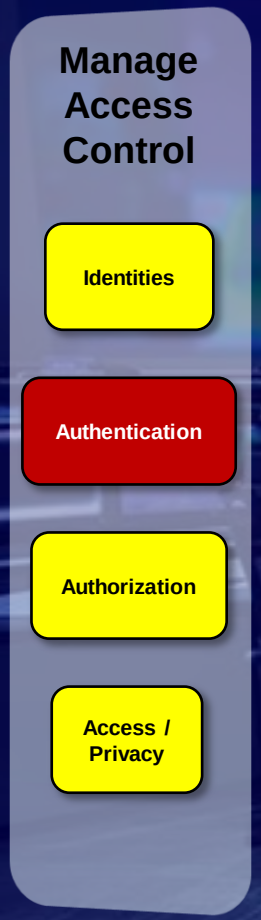
Response

- Identity & Access Management (IdAM) processes and capabilities
  - NOTE: The focus of Cap Area #5 is just on Identities
- Digital Certificates, and Digital Signatures

Caveats

- Identity related information is #1 target for Data Breaches
- Systems should provide both self- and central- registration processes
- Not all solutions deal with the full range of Identities

Cap Area #6 – Authentication Management (AuthN)



Challenges

- Need to reliably *prove* an entity is who they claim to be
  - Both person and non-person entities
- Need to provision, manage, revoke, and maintain credentials

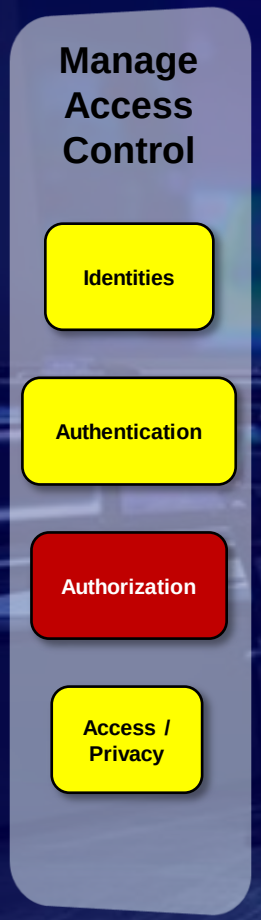
Response

- Identity & Access Management (IdAM) processes and capabilities
  - NOTE: The focus of Cap Area #6 is just on Credentials
- Multi-Factor Authentication (MFA) processes and capabilities
  - Something you (the entity) Know, Have, Are… and more recently, even "*Do*"

Caveats

- Credential information is a top target for attackers & fraudsters
- No single Authentication methodology is foolproof; Use > 1
- More Factors means more overhead performance/management

Cap Area #7 – Authorization Management (AuthZ)



Challenge

- Need to grant, revoke, and track access permissions
  - For both person and non-person entities

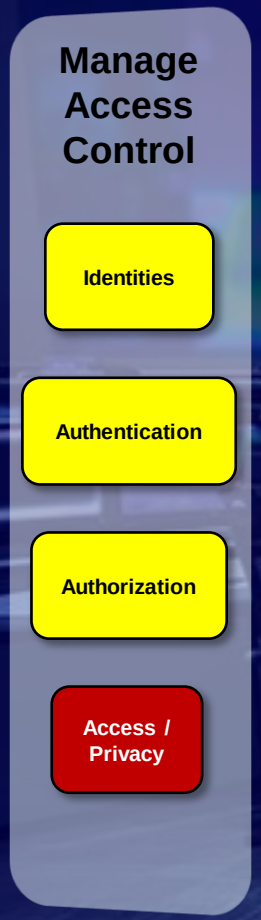
Response

- Access Control processes and capabilities
  - Group-Based Access Controls (GBAC)
  - Role-Based Access Controls (RBAC)
  - Attribute-Based Access Controls (ABAC)
  - "Cryptography-Based" Access Controls (see next slide)

Caveats

- Need to balance needs of both local and enterprise-wide authorizations
- ABAC is considerably more costly to setup and manage
- CRL checking – caching has pros (performance) and cons (latency)

Cap Area #8 – Privacy/Confidentiality Management



Challenge

- Need to ensure privacy / confidentiality of certain types of information
  - At Rest, and In Transit

Response

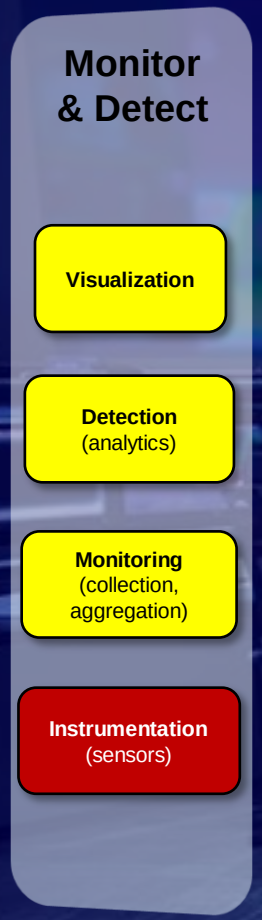
- Cryptography-Based Access Control processes and capabilities
  - Encrypted Data (e.g., files, devices, etc.)
  - Encrypted Communications (e.g., SSL/TLS, WEP/WPA/WPA2, VPN, etc.)
  - Secret (“shared”) Key vs. Public Key (e.g., PKI)
- Data Labeling, and Data Segmentation processes and capabilities

Caveats

- Key Management is a significant challenge to “Crypto-Based” access control
- Data Labeling and Data Segmentation involve significant management and performance overhead

Challenge #4 – Monitoring, Aggregation, and Detection

Cap Area #9 – Instrumentation (Sensors)



Challenges

- Need eyes & ears for Security Operations team
- Need to instrument the "entire" environment for *reliable* monitoring
  - IT, ICS/OT, IoT, etc.

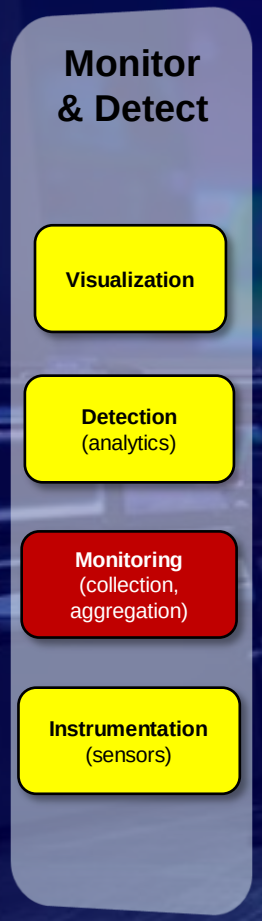
Response

- Host-Based "Sensors" – logfiles, agents, etc.
- Network-Based "Sensors" – Probes, TAPs/SPANs, IDS, etc.

Caveats

- Monitoring introduces performance overhead
- Need to continuously "tune" (dynamically re-config) these sensors
- "Sensors" themselves can be compromised, can dis-inform
- "Cloud" based infrastructure typically lacks sufficient instrumentation

Cap Area #10 – Monitoring (Collection, Aggregation)



Challenges

- Need to aggregate, filter, and fuse sensor data into *actionable* information
- Need to drill down into specific host/network activity

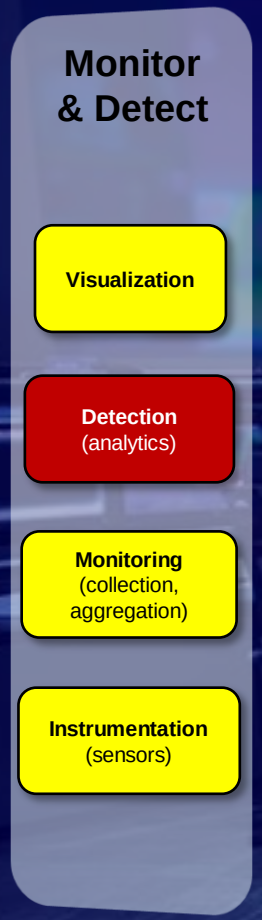
Response

- Vulnerability Lifecycle Management (VLMS) processes and capabilities
- Syslog, SNMP, SCAP standards, processes, and capabilities
- Security Information & Event Management (SIEM) capabilities
- Netflows, Superflows, and full packet captures (PCAP)

Caveats

- The "*collect everything, continuously*" approach does not scale
  - There are practical limitations to what can be collected continuously
- "Boil the ocean" approach leads to Analyst burn-out and turn-over
- Most contemporary approaches use ***in-band*** communications

Cap Area #11 – Detection Analytics



Challenges

- Need to detect incidents, malicious activity, etc.
- Need to perform both manual ("hunt") and automated analyses

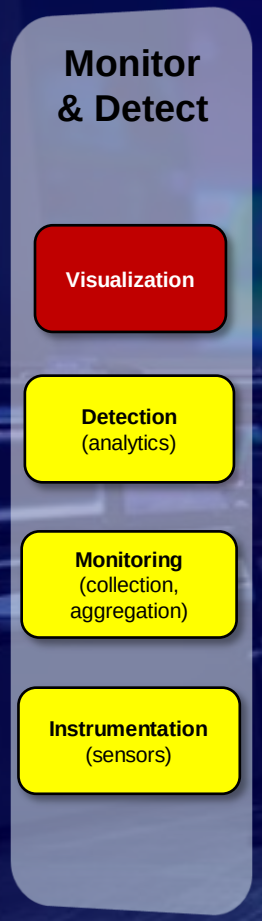
Response

- Log Analyzers, "signature-based" AV, "IOC-based" detection, etc.
- "Big Data" Security Analytics, processes and capabilities
- "User/Entity Behavior Analytics" (UEBA)
- "Artificial Intelligence" and "Machine Learning" based solutions

Caveats

- Garbage-in, Garbage-out
  - e.g., Basic "Correlation" of events/activity is very difficult without clock synchronization
- "Big Data" analytics employs a lot of simple statistical analysis
  - for data reduction and elementary anomaly detection

Cap Area #12 – Visualization, Notification



Challenges

- Need visualizations that help Analysts detect incidents
- Need visualizations that answer questions (e.g., the 5 "What Imperatives")
- Need visualizations that convey reports to Stakeholders (e.g., sr. leaders)

Response

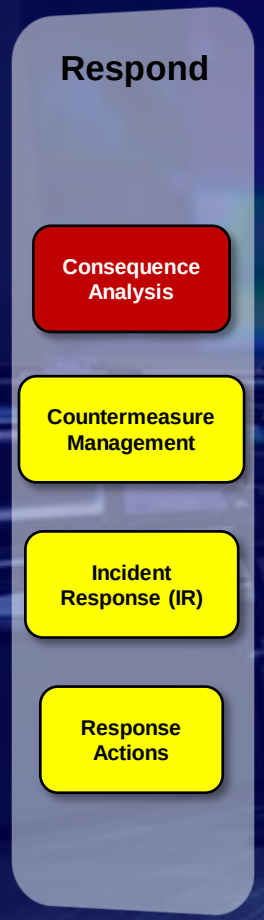
- "Single pane-of-glass" dashboards, "Common Operational Picture" (COP)
- Business Intelligence (BI) reporting applied to Cyber Security information

Caveats

- Complex, data-intense visualizations
  - typically aren't very useful to the majority of Security Operations
  - without CONTEXT can be confusing, even misleading
- Most impactful visualizations cast events in the context of the Business
  - vulnerabilities, threats, incidents, etc.

Challenge #5 – Informed Incident Response

Cap Area #13 – Consequence Analysis



Challenge

- Need to identify Consequences of a Situation, to articulate "*Risk*"
- Need to identify "*Risk*" to prioritize incidents, and investment in response
- Need to identify Consequences of a specific *Countermeasure*
  - Prior to recommending, deciding upon a response

Response

- Wait until an incident actually occurs to gather information about potential Consequences ("business impact")
- Reliance on anecdotal understanding of mission-critical dependencies

Caveats

- Useful Consequence Analysis leverages Business Dependency Mapping capabilities (described earlier)

Cap Area #14 – Incident Response (IR) Workflow

Challenges

- Need to formally identify, prioritize, direct, and track incidents
- Need to report on incident management statistics

Response

- Incident "Ticketing" processes and capabilities

Caveats

- "Ticketing" systems only manage IR process workflow
- No capability to auto-establish priorities based on consequences
- No capability to auto-identify relevant countermeasures
- No digital forensics capabilities, analysis or evidence tracking

Cap Area #15 – Countermeasure Management ("Playbooks")

Challenges

- Maintaining an evolving knowledgebase of relevant Countermeasures
  - To specific Adversary TTPs
- Track Countermeasure attributes: Objective, Cost, Effectiveness, etc.

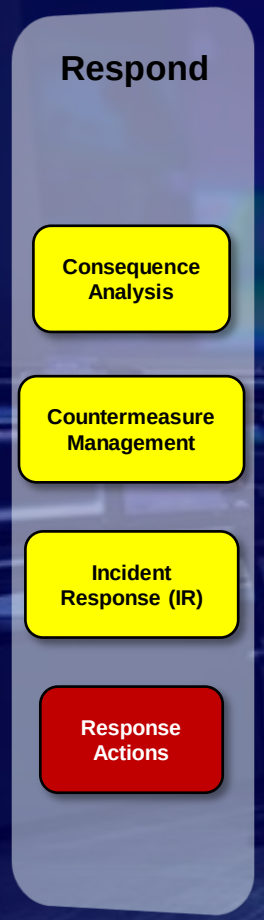
Response

- Today's "playbooks" document commodity response actions, not Countermeasures
  - e.g., take system offline, preserve hard drive, etc.

Caveats

- Monitoring, Detection Analysis, and Ticketing need to id and track TTPs
- Relevant Countermeasures should be evaluated based on their specific potential business impact
- Countermeasures may include Deception, Active Defense, etc.

Cap Area #16 – Response Action Management



Challenges

- Need to identify WHO has Authority to decide upon a response action
- Need to identify WHO will actually take the response action
- Need remote access w/ admin privileges on the target system(s)

Response

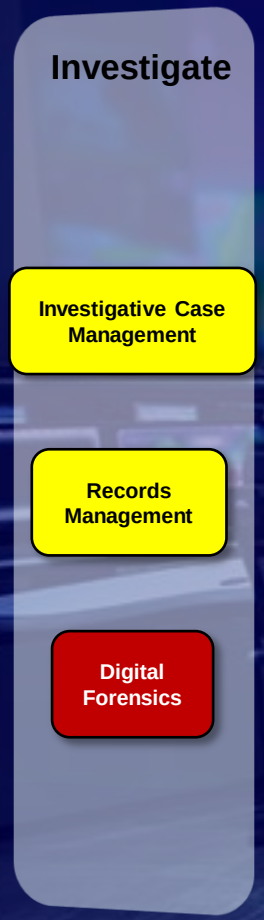
- Security Operations often decides, w/ some cross-team coordination
- Security Operations often executes the response action(s)
- Solutions include remote access tools (e.g., SSH, RDP, psexec, VNC, etc.)
- Emergent "Security Automation" solutions show promise to address commodity types of incidents

Caveats

- Security Automation is only appropriate with known TTPs and tested Countermeasures

Challenge #6 – In-Depth Investigations

Cap Area #17 – Digital Forensics (DF) Analysis



Challenge

- Need to follow strict processes for evidence gathering, analysis, and handling
- Need capabilities for a wide range of sophisticated analytics
- Expert staff, possibly with relevant certifications

Response

- Highly specialized teams
- Specialized processes & capabilities
  - network forensics, computer forensics, mobile device forensics, database forensics, forensic data analysis, malware analysis (reverse engineering), tradecraft analysis, etc.

Caveats

- Many forensics capabilities rely directly upon existing Instrumentation and Sensor capabilities and Security Controls
- Most small-to-medium size Security Operations teams choose to outsource this activity

Cap Area #18 – Case Management

Challenge

- Need to formally coordinate a broad range of staff and investigative activities
- Need structured investigative analysis and reporting capabilities
- Need to demonstrate legally defensible practices

Response

- Formal Case Management Systems (CMS) and practices
- Often out-sourced to 3rd parties specializing in Digital Forensics

Caveats

- "Ticketing" solutions are not sufficient "Case Management" solutions
- Particularly challenging with multi-national organizations dealing with global-scale incidents

Cap Area #19 – Records / Evidence Management

Challenge

- Need for formal practices and capabilities for evidence handling and retention
- May require 3rd party certification

Response

- Very well-documented policies & procedures
- Some type of “vault” capability to properly handle and secure the volumes of digital evidence being collected

Caveats

- This is a non-trivial set of processes and capabilities that will be scrutinized in every legal situation encountered

Challenge #7 – Visibility, Reporting

Cap Area #20 – Enterprise Reporting

Challenges

- Need to report on Cybersecurity Metrics (e.g., statistics)
- Need to report on Compliance with relevant policies, regulations, laws
- Need to report on ever-evolving Cyber Threat landscape
- Need to report on the actual Risk to the Business due to all of the above

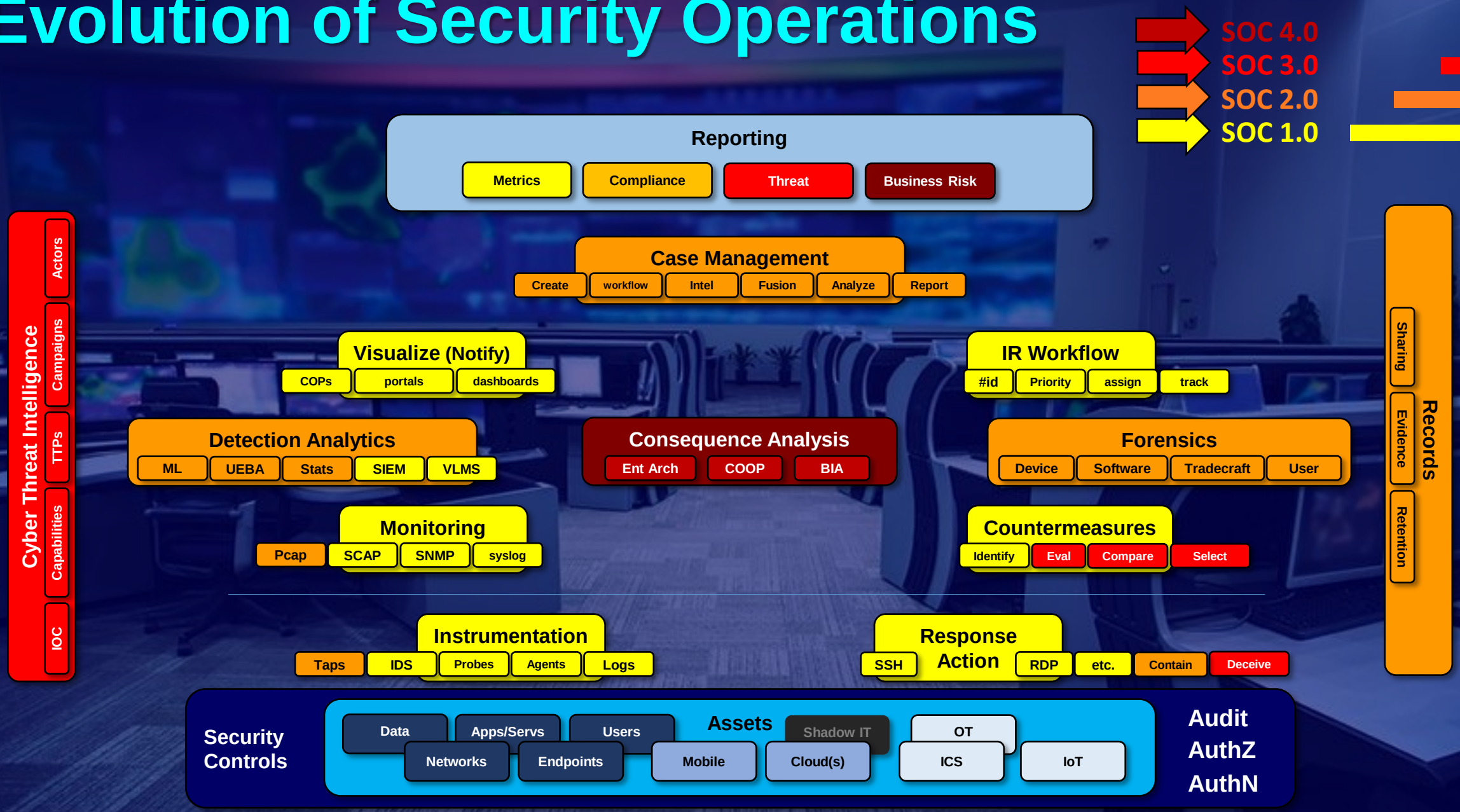
Response

- Most organizations have established dashboards and reporting procedures
  - e.g., Monthly Compliance reporting (to the CRO, and historically recorded)
  - e.g., Quarterly Risk Posture reporting (to the board)

Caveats

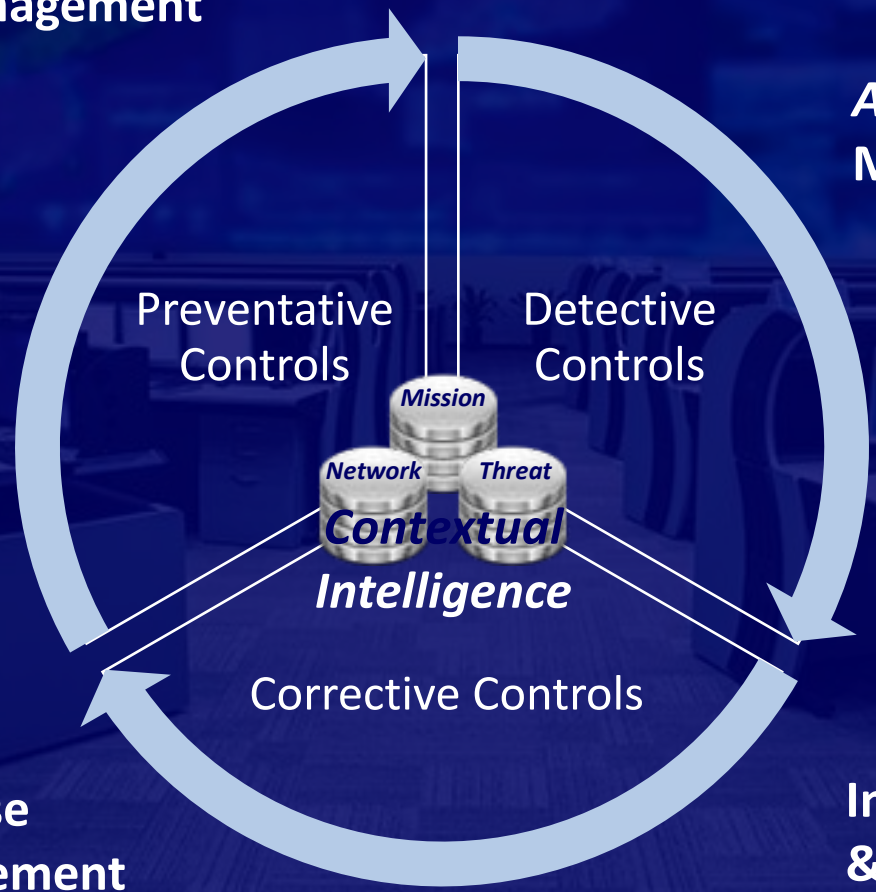
- Metrics without Context often confuse and frustrate stakeholders
- Compliance ≠ Security; a Threat Landscape needs to be *Relevant*
- Risk is always in terms of Consequences, Impact to the business

Evolution of Security Operations



Lifecycle of Security Operations

Lifecycle of Security Operations



Risk Management

Instrumentation

Pen Testing

Automated Monitoring & Analytics

Vulnerability Management

Manual Monitoring & Analytics

IdAM & PAM

Event / Complex Event Triage

Case Management

Incident Response & Management

Digital Forensics

Recovery Management