Technology Taxonomy

Who Am I?

I Know Some Stuff, and I Do Some Things

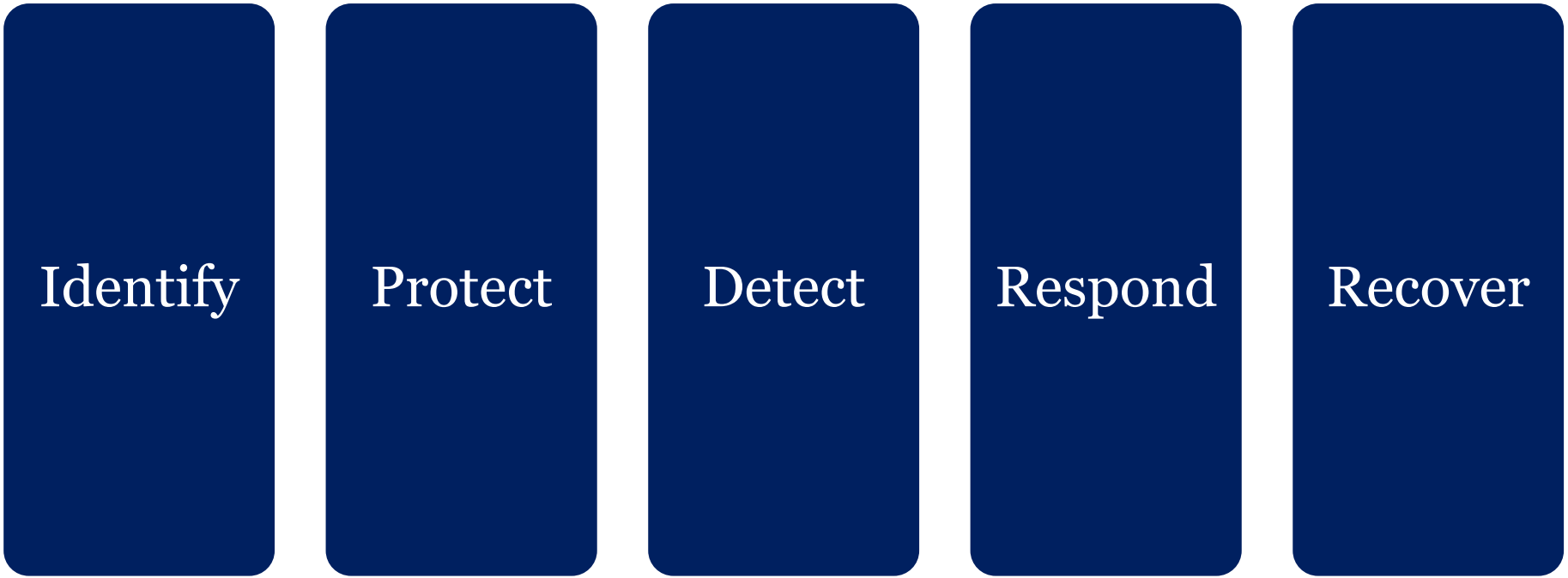
Enterprise Technology Selection

- There's no such thing as "SOC software"
- You have to make many tools work together, the tools weren't necessarily designed to play nicely with others
- No authoritative reference for technology taxonomy
- It's a marketing-vendor and analyst-research-industry driven treadmill

Technology Taxonomy

Pass 1 – NIST CSF

Cyber Security Framework



Identify

- Asset discovery and inventory
- Log management
- Risk analysis and assessment SIEM (security information and event manager)

Protect

- Access protection and control/VPN
- Application whitelisting
- Deception technologies such as honeypotting
- Data loss prevention
- Egress filtering
- Ingress filtering
- Malware detonation device (inline malware destruction)
- Malware protection system (MPS)
- Network Access Control (NAC)
- Next-generation firewall (NGF)
- SSL/TLS traffic inspection
- Web application firewall (WAF)
- Web proxy

NIST CSF – SOC Survey Mapping

Detect

- Application log monitoring
- Continuous monitoring and assessment
- Behavioral analysis and detection
- Endpoint monitoring and logging
- DNS log monitoring
- Customized or tailored SIEM use-case monitoring
- AI or machine learning
- eDiscovery (support legal requests for specific information collection)
- External threat intelligence (for online precursors)
- Frequency analysis for network connections
- Full packet capture
- Netflow analysis
- Network intrusion detection system (IDS)/Intrusion prevention system (IPS)
- Network traffic monitoring
- Packet analysis (other than full PCAP)
- Threat hunting
- Threat intelligence (open source, vendor provided)
- User behavior and entity monitoring

Respond

- Endpoint or host-based detection and response (EDR)
- DoS and DDoS protection
- Deception technologies

NIST CSF – SOC Survey Mapping

Recover

- Ransomware prevention
- Vulnerability remediation

Pass 2 – Crowley Categories

SOC Systems - Overall

Visibility – External Awareness

Visibility (External Awareness)

- Threat Intel Portals
- Operational Status information
- News information
- Weather
- Internet Weather

SOC Systems

Communication

- Phone
- Encryption for Communication
- Websites
- Portals: Status, Metrics, Incident, Ticketing

SOC Systems - Overall

Operations

Automation & Orchestration

Ticketing

Dev,QA,Stage of Production/Operational tools

SOC Systems

Detection & Prevention

Endpoint: EDR, App whitelisting, DLP, Behavioral Analytics, e-Discovery, logs, containment / response tools

Network: NIDS, PCAP, taps, logs, containment / response tools, detonation devices

Infrastructure: Switch, Firewall configuration, logs, containment / response tools, WiFi

Extrastructure: Cloud, Social analysis (not threat intel, but compromise and data), Cellular, ISP dependency, partner capability, tertiary DNS, CDN, connectors / APIs, logs, containment / response tools

Correlation: SIEM, LCE, etc.

SOC Systems

Storage

Data Aggregation: Data lakes, Federation, Separation/Compartmentalization

Retention: disks, discovery requirements,

Physical Controls: backups, safes,

Destruction

SOC Systems

Deception

Internet connectivity

Models

Honeytokens: files, folders, accounts,

Honeypots: endpoints, servers, networks

SOC Systems

Analysis

- Modeling and Testing Equipment
- Baseline systems
- Correlation, Mapping
- Forensics: Endpoint, Network,
- Scanners
- Code manipulation: disassembler, debugger
- Simulators

Portfolio Options

Typical Open Source

Visibility (External Awareness)	Twitter, news sites, Threat connect, OTX, Maltego CE, MRTG, RRD tool, MITRE ATT&CK
Communication	GPG, Skype, Slack, Linux servers
Ops	The Hive, RTIR
Detection & Prevention	SIFT, GRR, Winpmem/Volatility, OSSEC, syslog, SecurityOnion, ELK, Wireshark, Kismet, Cuckoo
Storage	MySQL, Postgresql, syslog, ELK
Deception	Tor, public access, Remnux, ADHD, Canary tokens, Kippo
Analysis	Virtualbox, GDB, Immunity, Metasploit, radare2, STIGs, Timesketch, Maltego CE, Yara, SIFT, Burp, Arachni, JaD-X

Portfolio Options

Typical Moderate

Visibility (External Awareness)	Threat Connect, OTX, Maltego, What's Up, MITRE ATT&CK
Communication	Vonage Cloud, Exchange PKI, Microsoft Teams, AWS EC2,
Ops	CyberCPR, Jira+Confluence, Demisto, ZenDesk
Detection & Prevention	SafeBack, FTK, F-response, Tripwire, Windows Defender, AppLocker, Bitlocker, Fortinet, NetWitness, LogRhythm, ProofPoint, Tripwire, AirDefense, AlienVault
Storage	AWS EC2, Azure, Dropbox, Shredding / IronMountain
Deception	Cable / DSL connection, VMWare Workstation, Honeybot, Authentic8
Analysis	VMWare Workstation, CobaltStrike, Trackwise Change Management, Tripwire, PowerShell DSC, CaseFile, Maltego, FRED workstation, Burp Professional, Hopper, JEB

Portfolio Options

Typical Open Source

Visibility (External Awareness)	RecordedFuture, Crowdstrike, CarbonBlack, Tivoli, Cisco NetFlow, iSIGHT
Communication	Avaya, Silent Circle, iOS phones, PKI signed user certs
Ops	Service Now, Phantom(Splunk), Remedy
Detection & Prevention	Tableau, Fireeye HX, CarbonBlack Protect, Encase eDiscovery, Cylance Protect, McAfee FDE, Cellebrite UFED, Cisco FirePOWER, Splunk (logging), Solera, Arbor Network, Cisco wIPS, Palo Alto, Fireeye AX, McAfee Skyhigh, Splunk Enterprise Security
Storage	Tenable LCE, data lake from SIEM, SAN LUNs, Safe with logging and per user access control, Commercial degausser
Deception	Authentic8, VMWare vSphere, redundant non-attributable network, Javelin Networks, Cymmetria MazeRunner, Joe Sandbox
Analysis	VMWare Workstation, CobaltStrike, CaseFile, Maltego, FRED workstation, Burp Professional, IDA Pro, CoreImpact, Rapid7 Nexpose, ServiceNow (change control), McAfee ePolicy Auditor, Chef/Puppet, Crowstrike Falcon X, Cisco AMP, Cellebrite UFED 4PC, Encase Enterprise, Tenable SC

Additional Technology Thoughts

SOC is the Defense

- The SOC contains all information for defense of your organization
- It should be considered a critical infrastructure component
- SOC information systems receive substantial protection of:
  - Integrity
  - Availability
  - Confidentiality
- Failure represents a loss of control, or perception that the information systems are operating normally when they are not

SOC Systems – who manages them?

- Considerations in systems administration for the SOC resources
  - Separation of duties between operations and SOC activities
  - Redundant system administration staff in both SOC and IT Operations is costly
  - Available skillset to manage systems, IT Ops SysAdmins might not be capable of administrating specialized SOC systems
- Decision
  - ROM 1 and 10 will transfer basic SysAdmin duties to IT Ops, probably have one or two people with shared responsibility for SOC system
  - ROM 100 and 1,000 will have dedicated internal System Admins, with a subfunction in Command Center or NSM for this work

Interoperability

- In addition to selecting specific technologies you must assure that your tools interface with one another and your ticket and tracking systems
- Having a well-designed process makes this easier
- We'll discuss data flow tomorrow in operation. A defined operational plan enables specifying electronic information exchange requirements at Request for Proposal (RFP) from vendors

What is the Data Glue?

- Scripting
  - Challenge of long term maintenance, adequate skillset
- Professional Services
  - Expensive, can be difficult to schedule in time
- Only select compatible products
  - Lock-in, missed opportunities
- Automation / Orchestration Tool
  - Current practice (and the latest buzzy marketing word)

SOC Components

- Location – decide on centralized or distributed
  - Perhaps a follow the sun model for Global organizations
- Insulation of SOC staff
  - SOC staff generally are not available to handle direct requests and should be physically isolated
  - Have a help desk function (either part of the SOC, or your actual help desk) between technical staff and customers

Selection Factors

- You may be fortunate enough to have funding to get all of these things initially
- Important factors
  - Information transfer between systems
  - Vendor support / relationship
  - Configurability and customization
  - Adequate volume support, scalability and growth path

Detailed Selection Criteria

Part One

- Best practices and patterns – are they provided? Or is it DIY?
- Configuration – Ease of configuration
- Convention – What is the standard use?
- Horizontal scaling – Scalability within SOC framework
- Testing – Can you test it? How?
- Scaffolding – Configuration helpers, or manual coding required?

Detailed Selection Criteria

Part Two

- Monitoring – How will you track the performance and issues?
- Track record – Support offering, other customers, company survivable?
- Integration – Data portability, data integration, connectors available?
- Modularity –Data transfer capabilities based on objects or raw data?

One Use of the Taxonomy – Improving SOC Effectiveness

- There are a lot of toys to buy but very few are cheap **and** easy to use
- Real world staffing, budget and organizational constraints need to be addressed
- The first step is a realistic starting point
  - Staff skill levels
  - Acquisition and maintenance budgets
  - SOC Maturity Level
  - Pattern recognition

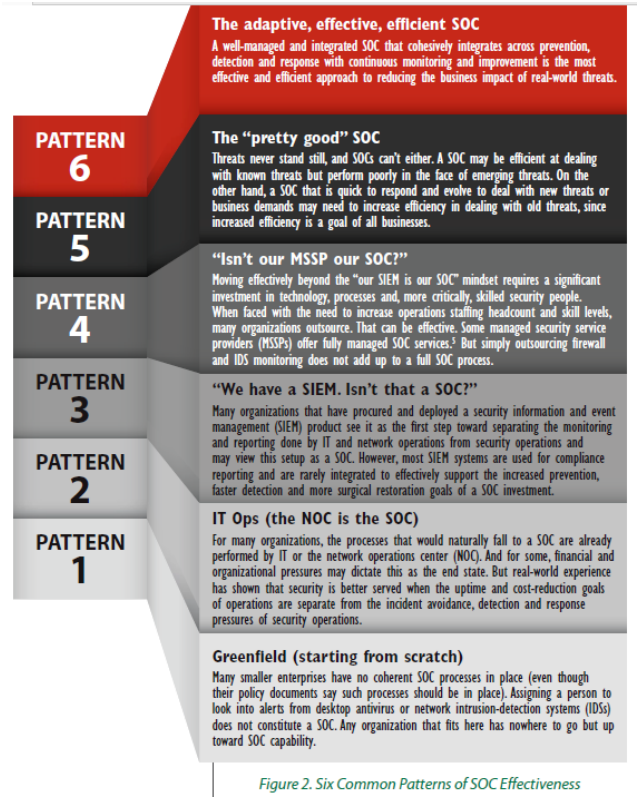
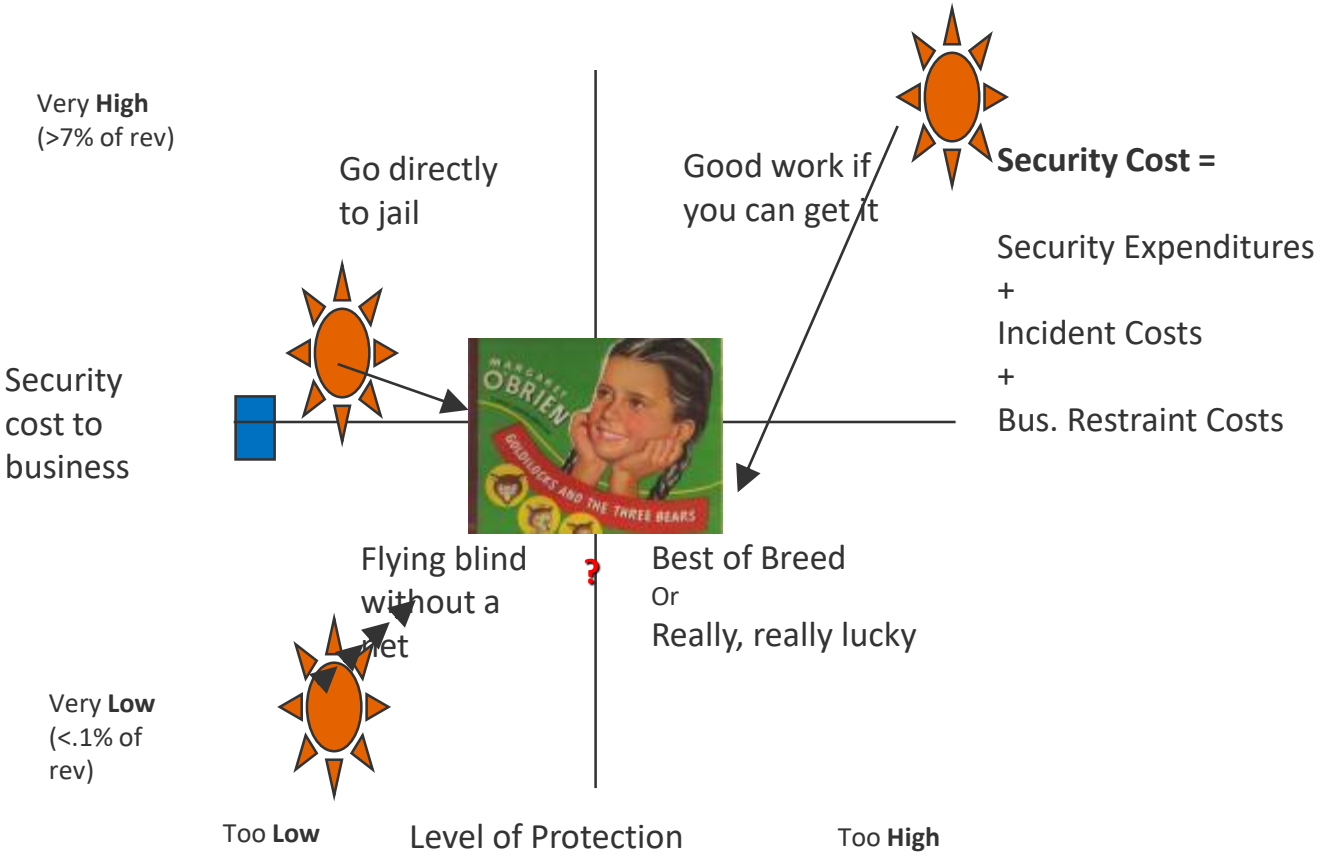


Figure 2. Six Common Patterns of SOC Effectiveness

Improving Effectiveness and Efficiency



Strategy Choices