WHAT DO I NEED TO ASK ABOUT MY SECURITY OPERATIONS
PREVENT MORE

PREVENTION ADAPTED FOR TOMORROWS ATTACKS;
AUTOMATICALLY STOP AND REMEDIATE THREATS IN THEIR TRACKS

SEE MORE

END POINT PLATFORM POWERED BY CROSS MACHINE CORRELATION TO UNDERSTAND THE DIFFERENCE BETWEEN APT AND IT

DO MORE

A PLATFORM MADE TO BE USED BY ALL AND BACKED BY MDR AND PROFESSIONAL SERVICES
AGENDA

» What do we define as SecOps
» Methodology for reviewing

» Processes
» People
» Technology
# Review Methodology

<table>
<thead>
<tr>
<th>1</th>
<th>Scope</th>
<th>• Scope of Work and Expectations</th>
</tr>
</thead>
</table>
| 2 | Business Review | • Compliance  
|   |             | • Revenue Gen.  
|   |             | • Risk Matrix  
|   |             | • Cyber Risk by BU |
| 3 | Process Inventory | • Existing Risk Mgt Process  
|   |             | • Maturity of Processes  
|   |             | • Gaps |
| 4 | Tech Review | • Existing Security Tech  
|   |             | • Spend  
|   |             | • Tech aligned to risk  
|   |             | • Gaps |
| 5 | Personal Interviews | • Skill Inventory  
|   |             | • Perceived Gaps  
|   |             | • Successes  
|   |             | • Team Functionality |

- RoadMap
- Report
- Design
- Build
- Run
Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes.

Define a service strategy, create work plans, and monitor and control the work to ensure the service is delivered as planned. The service provider establishes agreements with customers and develops and manages customer and contractual requirements.

These processes are well characterized and understood and are described in standards, procedures, tools, and methods. Well integrated with the overall business.

At maturity level 4, service providers establish quantitative objectives for quality and process performance and use them as criteria in managing processes. Quantitative objectives are based on the needs of the customer, end users, organization, and process implementers.

At maturity level 5, an organization continually improves its processes based on a quantitative understanding of its business objectives and performance needs. The organization uses a quantitative approach to understand the variation inherent in the process and the causes of process outcomes.

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9665
Driving an Effective Security Program

- Ad-hoc
- Managed
- Continuous Improvement

Number of customers vs. Security Program Maturity
TEAM EFFICIENCY

FOUNDATIONS

» Human centric design
» Remove waste
» Real people doing work
» Get close to the business
» Stream-line use cases
» Don’t bayonet the wounded
» Choose the right metrics
» People *efficiency*
» Use case *effectiveness*

GETTING IT RIGHT

» *Build KPIs* that make *Cyber* sense...
» E.g. Straight MTTK rewards detection
» E.g. Straight MTTR (no weighting) rewards finding the easy stuff
» Ensure...
» *Meaning* - all green is bad
» *Actionability* - results encourage corrections
» *Longevity* - value as you grow
<table>
<thead>
<tr>
<th>ITEM</th>
<th>SOC 1.0</th>
<th>SIEM-DOMINATED SOC</th>
<th>RECOMMENDED SOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPEX</td>
<td>SIEM</td>
<td>SIEM</td>
<td>NTA</td>
</tr>
<tr>
<td></td>
<td>$250K</td>
<td>$2.5M</td>
<td>$250K</td>
</tr>
<tr>
<td>OPEX</td>
<td>8 L1 Analysts 8 L1 Analysts 8 L1 Analysts</td>
<td>8 L1 Analysts 4 L2 Analysts 2 L3 Analysts 2 L3 Analysts IT Support 8 L1 Analysts</td>
<td>$800K $600K $400K $100K $800K $600K $400K $400K $800K $800K $800K $100K</td>
</tr>
<tr>
<td>EFFICIENCY</td>
<td>3 Incidents/Day/Analyst</td>
<td>6 Incidents/Day/Analyst</td>
<td>5 Incidents/Hour/Analyst</td>
</tr>
<tr>
<td>RESULTS</td>
<td>•High False Positive •High False Negative •Low True Negative •Emp: Rare, High Burnout</td>
<td>•High False Positive •Moderate False Negative •Moderate True Negative •Emp: Rare, Moderate Burnout</td>
<td>•Moderate False Positive •Low False Negative •Low True Negative •Emp: Common, Low Burnout</td>
</tr>
<tr>
<td>TOTAL COST</td>
<td>CapEx: 250K / yr OpEx: 1.9M / yr</td>
<td>CapEx: 2.75M / yr OpEx: 3.9M / yr</td>
<td>CapEx: 650K / yr OpEx: 1.9M / yr</td>
</tr>
</tbody>
</table>

20,000 EP
12,000 Employees
TECHNOLOGY
Cybereason Recommend SecOps: Foundations

Foundational Data
- EDR / EPP
- NTA
- Email Gateway

Orchestration Layer
- TI
- SOAR
<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
<th>Why</th>
</tr>
</thead>
</table>
| SOAR         | Security Orchestration and Automation (RPA for Security) | • Automate case management and analysis workflows.  
                |                                                                  | • MDR / MSSP can be a substitute  
                |                                                                  | • Create workflows that reduce human effort and decrease response time metrics..  |
| EPP & EDR    | End Point Protection, Detection, and Response     | • Protect against endpoint threats  
                |                                                                  | • Detect Compromises at the endpoint  
                |                                                                  | • Investigation tool to understand and corroborate other alerts  
                |                                                                  | • Threat Hunting on endpoint data  
                |                                                                  | • The Endpoint always is the ground zero  
                |                                                                  | • Ability to stop and isolate actors  |
| NTA          | Network Traffic Analytics                        | • Identify Rouge devices.  
                |                                                                  | • Understand undermanaged data flows.  |
| Email Gateway| Protect against email threats                    | • Email is a critical attack vector.  
                |                                                                  | • Logs and protection is a must.  |
Cybereason Recommend SecOps: High Maturity

Foundational Data
- EDR / EPP
- NTA
- Email Gateway

Orchestration Layer
- TI
- SOAR
- SIEM / Log Mgt.

Secondary Data Sources
- Critical Asset Logs
  - AD
  - Revenue Crit. Applications
  - External Facing apps
  - Regulated Assets
- Critical Infrastructure Logs
  - FW
  - IPS
  - IAM
  - CASB
  - MDM
» Log Management needs to be strategic.

» Traditional security controls can be noisy.

» Pre-requests:
  » Controls implemented
  » Known inventory of critical assets
  » Risk Matrix

» Understanding of log value to response and detection workflows aligned to business.
# Cybereason Recommend SecOps: Best In Class

## Foundational Data
- EDR / EPP
- NTA
- Email Gateway

## Orchestration Layer
- TI
- SOAR
- SIEM / Log Mgt.
- eGRC

## Secondary Data Sources

<table>
<thead>
<tr>
<th>Critical Asset Logs</th>
<th>Critical Infrastructure Logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>FW</td>
</tr>
<tr>
<td>Revenue Crit. Apps</td>
<td>IPS</td>
</tr>
<tr>
<td>External Facing Apps</td>
<td>IAM</td>
</tr>
<tr>
<td>Regulated Assets</td>
<td>CASB</td>
</tr>
<tr>
<td></td>
<td>MDM</td>
</tr>
<tr>
<td></td>
<td>DLP</td>
</tr>
</tbody>
</table>
CYBEREASON
RECOMMEND SECOPS:
BEST IN CLASS_

» Integration with enterprise risk governance.

» Detection and response is viewed as a business critical risk management strategy.

» Well run data governance and management program.