The Inevitable Cyber Attack: From Observation to Remedial Action and Minimizing Dwell Time”
In-between

Presenter
Jon Hamlet – Senior Country Manager
Gareth Hawkins – Pre-Sales Manager

Date
22 September 2017
Organizational Security Maturity

Reactive  Proactive

BASICS  STRATEGY / CULTURE  RISK BASED
EXCLUSIVE  OVERLAPPING CONTROLS  INCLUSIVE

What is required to mature?

VISIBILITY

PROGRESS NOT PERFECTION

BUSINESS INCLUSION

Insights
“Dwell Time”
The amount of time between initial compromise and final remediation”
A Security Operations Center is a Highly Skilled team following Well-Defined Definitions and Processes to Manage Threats and Reduce Security Risk

Haider Pasha, CISSP, C|EH
Chief Technology Officer
Emerging Markets
Key Security Challenges

Security Operations Center

CONCERNS
- Scaling for Growth
- Data Protection & Compliance
- Limited Cyber Security Threat Intelligence & Analytics
- SOC Implementation Methodology

REQUIREMENTS
- Outsource vs. Co-Source of Security Operations
- Enhancing Visibility
- Governance & Control
- Proactive Threat Detection, Prevention, & Response

SOC FOCUS
- Threat Protection
- Threat Monitoring and Operations
- Intelligence & Incident Response
- Security Analytics
SOC Vision

- People
- Processes
- Technology
- Cyber Security Services
- Security Monitoring Services
- SOC Maturity
- Threat Protection
- Intelligence
- Managed Security Service
- SIEM
- Big Data Analytics
- IT-GRC
- Threat Intelligence
- Vulnerability Assessments
- Simulation Services
- Network Protection
- Proactive Protection
- Incident Response
- Incident Management
- Enhanced Visibility
- Security Advisory
- Reporting and SLAs
## Security Management Consideration

### Insourcing

<table>
<thead>
<tr>
<th>Cost</th>
<th>High CAPEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>Internal Team Knows Environment</td>
</tr>
<tr>
<td></td>
<td>Potentially Most Efficient</td>
</tr>
<tr>
<td></td>
<td>Complex to Manage</td>
</tr>
<tr>
<td>Time</td>
<td>People Recruitment, Tools Procurement &amp; Configuration</td>
</tr>
<tr>
<td>Staff</td>
<td>Hard to Acquire, Retain, Train</td>
</tr>
<tr>
<td>Risk</td>
<td>High Risk – Mitigated with Augmentation</td>
</tr>
<tr>
<td></td>
<td>Assigned to End-User</td>
</tr>
</tbody>
</table>

### Outsourcing

<table>
<thead>
<tr>
<th>Cost</th>
<th>Low CAPEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>Lack of Environment Knowledge by 3\textsuperscript{rd} Party</td>
</tr>
<tr>
<td></td>
<td>SLA Based Services</td>
</tr>
<tr>
<td></td>
<td>Difficult to Terminate / Change</td>
</tr>
<tr>
<td>Time</td>
<td>Handover, Service Definition and SLA Measurement</td>
</tr>
<tr>
<td>Staff</td>
<td>3\textsuperscript{rd} Party Responsibility</td>
</tr>
<tr>
<td>Risk</td>
<td>Medium Risk</td>
</tr>
<tr>
<td></td>
<td>Assigned to the Provider</td>
</tr>
</tbody>
</table>

### Co-sourcing

<table>
<thead>
<tr>
<th>Cost</th>
<th>Moderate CAPEX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>Benefits of Local Knowledge and 3\textsuperscript{rd} Party</td>
</tr>
<tr>
<td></td>
<td>Expertise</td>
</tr>
<tr>
<td></td>
<td>Partial SLA Service</td>
</tr>
<tr>
<td></td>
<td>Flexible Future Change</td>
</tr>
<tr>
<td>Time</td>
<td>Blended Approach</td>
</tr>
<tr>
<td>Staff</td>
<td>Staff Augmentation</td>
</tr>
<tr>
<td>Risk</td>
<td>Lowest Risk;</td>
</tr>
<tr>
<td></td>
<td>Shared Between Companies</td>
</tr>
</tbody>
</table>
Process
SOC Methodology

- **Conduct health-check and preventive maintenance for all security systems**
  - Implement new Security Policy on the managed devices following the agreed process
  - Perform Change & Configuration Management through RFC&MDT process

- **Analyze Security Systems logs for any security threats and take proper action accordingly**
  - Provide 1st & 2nd level of support for the security incidents
  - Supporting other Security departments during the incident handling process

- **Log Monitoring**
  - Event Detection
  - Incident Response
  - Predictive Protection
  - Proactive Prevention
  - Security Management
<table>
<thead>
<tr>
<th>Reactive Services</th>
<th>Proactive Services</th>
<th>Security Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitoring</strong></td>
<td><strong>Vulnerability Management</strong></td>
<td><strong>Business Impact Analysis</strong></td>
</tr>
<tr>
<td>Security Monitoring</td>
<td>Real-Time Device Monitoring</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Event Monitoring</td>
<td>VA/PT &amp; Threat Model Simulations</td>
<td>Threat Assessment</td>
</tr>
<tr>
<td>Event Correlation</td>
<td>Security &amp; Compliance Audit</td>
<td>Technology Watch</td>
</tr>
<tr>
<td>Incident Management</td>
<td>Performance &amp; Fault Monitoring</td>
<td></td>
</tr>
<tr>
<td><strong>Advisory</strong></td>
<td><strong>Cyber Threat Intelligence</strong></td>
<td><strong>Inventory Scanning</strong></td>
</tr>
<tr>
<td>Incident Notification</td>
<td>Threat Hunting &amp; Analysis</td>
<td></td>
</tr>
<tr>
<td><strong>Managing</strong></td>
<td>Incident Hotline</td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td>Operational &amp; Strategic Threat Reports</td>
<td></td>
</tr>
<tr>
<td>Threat &amp; Vulnerability Triage</td>
<td>Technical Reports</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Security Consulting</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alerting &amp; Warning</td>
<td>Awareness</td>
</tr>
<tr>
<td></td>
<td>Trending</td>
<td>Countermeasure Selection</td>
</tr>
<tr>
<td></td>
<td>Technical Reports</td>
<td>Executive Reporting</td>
</tr>
<tr>
<td><strong>Policy &amp; Device Management</strong></td>
<td><strong>Security Governance</strong></td>
<td><strong>Risk Management</strong></td>
</tr>
<tr>
<td>Incident Triage</td>
<td>Secure Device Configuration</td>
<td>Business Continuity</td>
</tr>
<tr>
<td>Malware &amp; Forensics Analysis</td>
<td>Policy Enforcement</td>
<td>Asset Inventory</td>
</tr>
<tr>
<td>Incident Recovery &amp; Post Mortem</td>
<td>Patch Management</td>
<td>Policy Planning</td>
</tr>
<tr>
<td></td>
<td>Events Data Retention</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Personnel &amp; Supplier Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hardening</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Events Data Retention</td>
<td></td>
</tr>
</tbody>
</table>
First SOC function: Monitoring

Bring visibility to current security issues
Real-time Device Monitoring
Incident Detection
Incident Classification
A Simplified View

Second SOC function: Managing

- Policy Management
- Policy Enforcement
- Incident Remediation
- Managed Network Security
- Managed Endpoint
- Managed Messaging
- Advanced Threat Protection
- Risk Management
- Cyber Resilience
A Simplified View

Security Operations Center

Third SOC function: Advisory
Alerting and Warning
Technical and executive reporting
Compliance Reporting
Cyber Insurance

IT
Executive
Executive

Alert and warning
Reporting
Cyber Insurance

DLP
Identity
Cloud
Mail Security
Apps
Mail Security
Endpoints
Endpoint Security
Network
Data Center
Data
FW
NDIS
Proxy
WAF
HIDS
DLP
Endpoints
DLP
Security

Copyright © 2017 Symantec Corporation
Incident Handling Methodology

- Preparation
- Detection
- Assessment (Triage)
- Analysis
- Notification
- Response
- Closure
REDUCING DWELL TIME?

Preparation

Assessment (Triage)

Notification

Closure

Detection

Analysis

Response

Threats

Events

Infrastructure

Vulnerabilities

Cloud

Changes

Workbench

Response Efficacy

Audit

GRC

Response Efficacy

Audit

GRC

Reduced Noise

Shared Threat Intelligence

Orchestration

Automated Remediation

Bidirectional

Closed Loop

GLOBAL

WELL DEFINED PROCESS – RESPONSES ACROSS THE BOARD

INTEGRATED TECHNOLOGY (OPEN SYSTEMS)

VISIBILITY

Closed Loop

Remediation

Repositioning

Copyright © 2017 Symantec Corporation
Incident Response Process Framework

Process Stages

Preparation
- IR Plan & Program Development
- Penetration Testing
- Risk Assessments
- Security Monitoring Health Checks
- IR Retainer Services

Detection & Analysis
- APT Discovery Services
- Malicious Activity Assessments
- Incident Response Services

Containment, Eradication, & Recovery
- System Forensics
- Network Forensics
- Log Analysis / MSS
- Memory Forensics
- Advanced Malware Analysis
- Intelligence Services
- Advanced Threat Protection Solutions

Post-Incident Activities
- Incident Response Services
- Enablement Services
- Partner-led Remediation Services
- Partner-led Litigation Support

Scope

Preventative & Detective Controls
- IR Plans & Team Training

IR Technology & Partners
- Event Monitoring & Analysis
- Triage & Document Incident
- Incident Notification

Evidence Collection & Analysis
- Incident Scope & Containment Strategy
- Mitigation, Recovery, & Verification

Incident Reporting & Lessons Learned
- Remedial Actions
- Evidence Archival

Solution Areas

Specialty Areas
- Security Intelligence
- Advanced Threat Protection
- Advanced Malware Analysis
- Global Operations
People
PEOPLE: 24/7 SOC Shift Example

Security Monitoring team shift A
L2 Senior Analyst
L1 Junior Analyst

Security Monitoring team shift B
L2 Senior Analyst
L1 Junior Analyst

Security Monitoring team shift C
L2 Senior Analyst
L1 Junior Analyst

Cyber Security Team - L3 Analyst

Vuln & Threat Management Team

UAM & CR Management Team

Security Analytics Team – Admin&Op
Admin & Operation team
Senior/Junior System Admin
Senior/Junior Network Admin

Security Analytics Team – Admin&Op
Admin & Operation team
Senior/Junior System Admin
Senior/Junior Network Admin

SOC Governance and Management

SOC Service Delivery Manager
SOC Manager
SOC Quality Control Team

Shift team in rest
Security Monitoring team shift D
L2 Senior Analyst
L1 Junior Analyst

Copyright © 2023 Symantec Corporation
Typical SOC Team Structure

SOC Manager

Cyber security Intelligence team

Security monitoring team

- Security monitoring team manager
- Shift A (L1+L2+ Shift leader)
- Shift B (L1+L2+ Shift leader)
- Shift C (L1+L2+ Shift leader)
- Shift D (L1+L2+ Shift leader)

Cyber Intelligence team manager

Security Operation team

- Security Operation team manager
- Security Monitoring and operations Infrastructure
- User access management and Operational CR assessment

Vulnerability and Threat Management Team

- Threat&Vulnerability manager

Security analytics team

- Big Data Platform Management team
- Big Data Platform Analyst team

Reporting and Quality control team

SOC Service Delivery Manager

Copyright © 2017 Symantec Corporation
Technology
Integrating Threat Protection: SOC Workbench

Global Intelligence

- Remediation
- Isolation
- Investigation

Monitored Security Services

IT Helpdesk

Email Security Service/Gateway

Web Security Service/Gateway

Data Protection Connector

SOC: Incident Response Function
- Automated Incident Creation and Correlation
- Detection of Suspicious Events
- Prioritization of Incidents
- Event Enrichment

SOC: Threat Intelligence Team
- Who’s attacking us
- What TTP are used and IOC
- Campaign and Adversary Intelligence
- Enterprise Visibility

SOC Workbench

- Visibility
- Control
- Assurance

Single Console

Endpoint Protection

Sandbox

Correlation

Attribution

Network

Endpoint Protection

Email

Web

IT Helpdesk

Web Security

Email Security

Data Protection

Incident Response

Security Analytics

Integrated Threat Protection:

- Endpoint Protection
- Sandbox
- Correlation
- Attribution

Security Analytics

Single Console

Visibility

Control

Assurance

Route high severity incidents directly to the SOC

Sandbox

Correlation

Attribution

Monitoring and Control

Visibility

Control

Assurance

Security Analytics

Single Console

Visibility

Control

Assurance

SOC Workbench
Integrated Information Protection: SOC Workbench

- Data Protection: Incident Response Function
  - Automated Incident Creation
  - Universal policy deployment
  - Single enforce platform

- Single Data Protection Console
  - Visibility
  - Control
  - Assurance

- Remediation
- Investigation

- Data Protection Connector
- Corporate SaaS Apps
- Email Security Service (SMTP)
- Web Proxy
- Web & Internet
- Data at Rest
- Email
- IT Helpdesk
- CASB
- Shadow IT Visibility & Control
- Tagging & Encryption
- Identity & Authentication

Integrated Information Protection Controls
Few takeaways

- Each SOC project is a journey. Get the required buy in.
  - Projects require a considerable amount of time and money.

- Hybrid approach can massively speed up the time to service delivery.
  - Consider adopting an MSSP even as a temporary solution

- Define Service Catalog Carefully.

- Implement baby steps: do few things well.
  - Do not oversell SOC mission and implement the basics right.

- Do not ingest any data: clearly define your use cases.

- Get the right staff in place.
  - Motivate them, motivate them, motivate them.