RSA® ADVANCED SOC SERVICES

Consulting services to improve threat detection and response

EXECUTIVE SUMMARY

A holistic approach to enhanced cyber-security operations

This service is for organizations needing to improve their defenses against targeted attacks. It provides them with consulting services to design and implement an Advanced Security Operations Center ("Advanced SOC").

Targeted attack defense requires a combination of synchronized capabilities across people, processes and technology. Given the sophistication of today's attacker, compromise can happen in minutes, thus incident detection and response must be accelerated. RSA recommends consolidating all threat detection and response efforts for an organization under a centralized Advanced SOC program.

THE NEED FOR SOC RESILIENCE

Be prepared for the unexpected

The sophisticated nature of recent attacks has increased the awareness that even well defended organizations can be compromised. While an adversary may be able to establish an initial foothold, it is possible to detect and remediate the attack before harm is done.

This makes it a race against time between the attacker and the SOC team. How effective is the organization at detecting and responding to attack activity before the adversary can meet his objectives? Despite the difficulties in dealing with the unpredictable nature of the threat environment, the SOC must be resilient. It must be capable of responding to unexpected stresses and strains if it is to protect the business from disruption.

RSA's® Advanced SOC Design & Implementation Services helps organizations better protect their critical assets by improving their detection and response capabilities. This includes the design, development and implementation of the SOC components including systems architecture, incident response and organizational structure.

EVOLVING SOC TECHNOLOGY

Four key components

Organizations have been investing in security since viruses and malware first appeared. Yet, almost continuous reports of security breaches are clear testimony that despite continued investments in traditional security systems, the countermeasures have been inadequate.

To address today's threat environment the SOC team must possess some key capabilities:

- Network visibility: Provides deep and broad visibility, accelerating detection and investigations
- Host visibility: Extending detection, investigations and response to endpoints, including both servers and clients
- Workflow automation: Automated incident response management for more rapid analysis, triage and remediation
- Centralized alerting: Centralized alert and data aggregation to help prioritize incidents for investigation and improve the efficiency and effectiveness of incident response.

These key technologies can be leveraged to integrate with broader data sets including cyber threat intelligence and business context, to help prioritize remediation efforts relating to critical assets.

People and procedures are equally as important as the security architecture and systems model. They need to complement one another and work seamlessly together.

By putting the right systems architecture in place, combined with an appropriate organizational model and incident response program, the SOC can tilt the balance in favor of the defenders and better position itself to protect the business against a difficult and unpredictable threat environment.

THE ADVANCED SOC ENGAGEMENT

Approach and deliverables

Key activities for SOC Design include:

- Interactive and business-focused interviews and workshops addressing people, policy and process
- Documentation and technology review as key components of content, analytic and threat intelligence

The final deliverable is a SOC Design Report, which is tailored to each organization's unique requirements. This typically includes multiple tools and technologies, supported with recommended technical and operational design improvements.

Large SOCs can also include secondary sites to facilitate twenty four hour and "follow-the-sun" global coverage. This may require additional planning to include shift handover and business continuity planning. Outsourcing to managed service providers may need to be accommodated in the overall SOC design.

Proactive anomaly hunting is required for targeted attack defense. This can be achieved by knowing what sources of information to capture, what to look for and what to do when issues are found. The SOC design has to address "the needle in the haystack" but also how to make the haystack smaller:

- At the network level, dropping non-relevant packets
- At the host level, whitelisting of authorized modules and processes

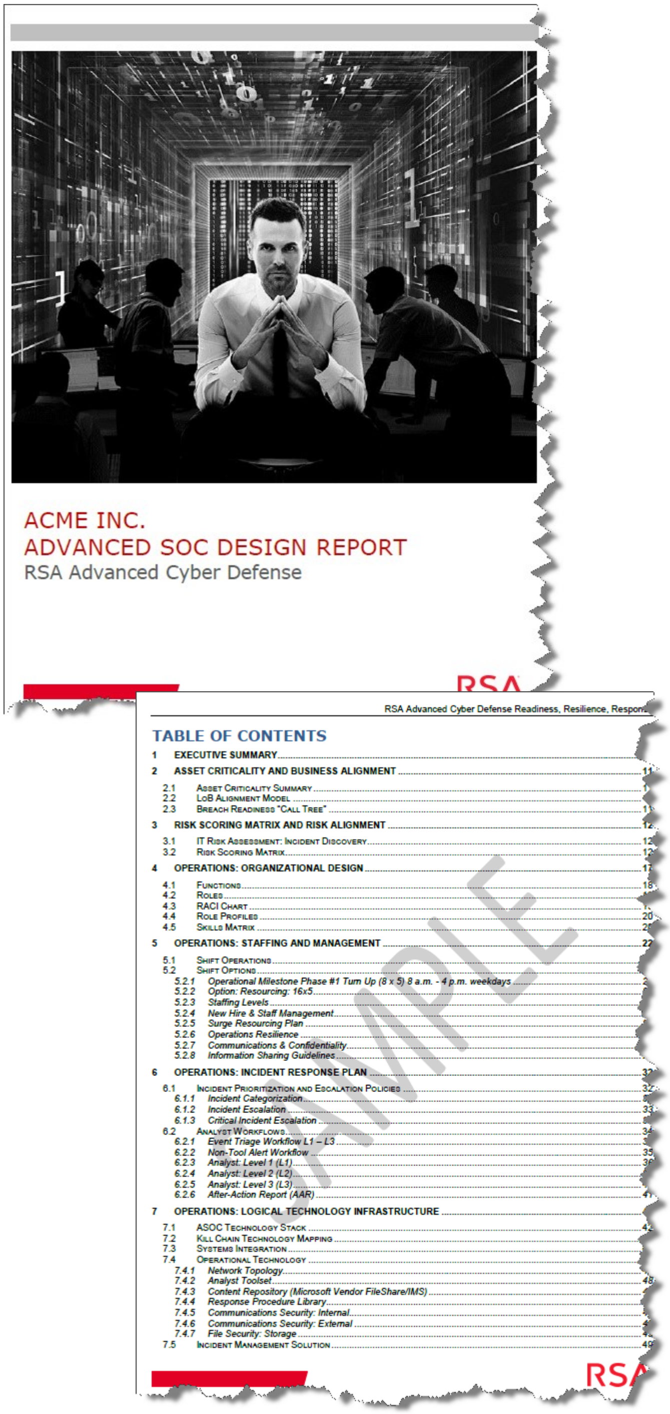
This reduces the volume, variety and velocity of data to a more relevant and manageable set and eliminates redundant data which can impede analysis and response.

By further categorizing data based on criteria such as directionality (e.g. outbound to Internet), internal address space, port and protocol usage and by generating meta data at the time of capture, the SOC team can establish a basis by which the tools and technologies can be combined with processes and procedures to facilitate early detection and rapid response.

At a high level, a SOC Design can be segmented into three broad topics:

- Systems Architecture Model
- Incident Response Program
- Organizational Model

These categories are reviewed in greater detail below.



ACME INC.
ADVANCED SOC DESIGN REPORT
RSA Advanced Cyber Defense

RSA Advanced Cyber Defense Readiness, Resilience, Respon

TABLE OF CONTENTS

Advanced SOC Design Report

SYSTEMS ARCHITECTURE MODEL

Integrated tools and technologies

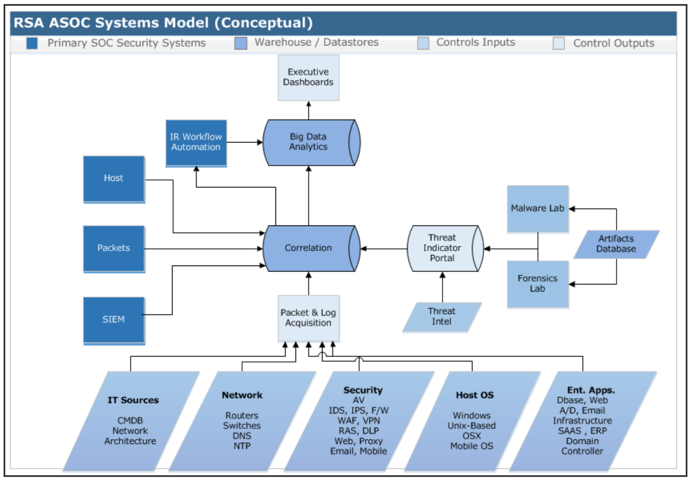
A SOC design can include several layers of technologies beyond components for packet capture, host analytics and threat intelligence. Deployment usually spans a period of time, with duration depending on the size and complexity of the environment and the number of sites involved.

Additionally the SOC must continuously evolve, constantly adapting to new adversary tools, tactics and procedures.

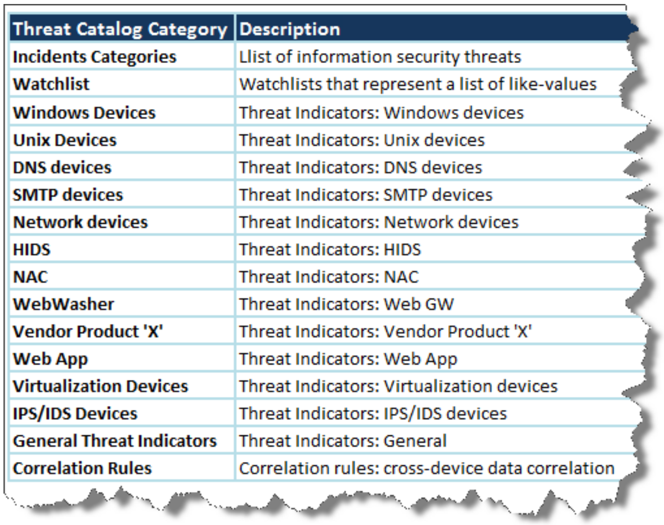
Systems need ongoing tuning and optimization to eliminate false positives. Tight integration is required to enrich data with threat and business context and to meet the use cases prescribed to counteract new and emerging adversary tools and tactics.

RSA's Use Case Framework is an approach to ensure that risks to the business are identified along with the controls required for threat mitigation. It prescribes key elements to maximize the return on technology investments:

- Objective: purpose and goal of the control
- Risk: the threat which the logic seeks to mitigate
- Stakeholder: responsibility for control monitoring
- Data Requirement: information sources for the control
- Logic: the technical rules and filters required for the control
- Testing: confirmation that controls meets requirements
- Priority: classification category and level for the threat based on the potential impact to the business
- Response Procedure: the process, procedures and workflow when responding to the threat. (This is typically addressed as an element of "runbook development" during the SOC Implementation).

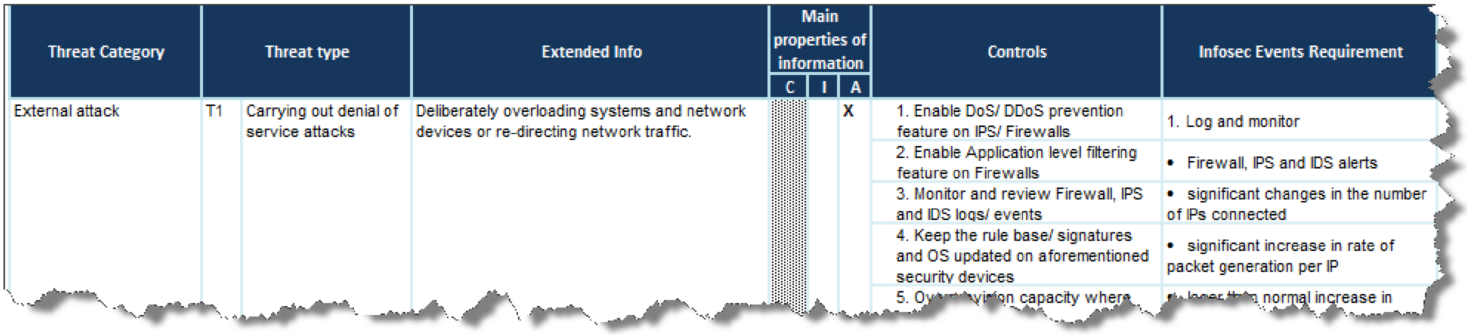


Advanced SOC Systems Model



Threat Catalog Category	Description
Incidents Categories	Llist of information security threats
Watchlist	Watchlists that represent a list of like-values
Windows Devices	Threat Indicators: Windows devices
Unix Devices	Threat Indicators: Unix devices
DNS devices	Threat Indicators: DNS devices
SMTP devices	Threat Indicators: SMTP devices
Network devices	Threat Indicators: Network devices
HIDS	Threat Indicators: HIDS
NAC	Threat Indicators: NAC
WebWasher	Threat Indicators: Web GW
Vendor Product 'X'	Threat Indicators: Vendor Product 'X'
Web App	Threat Indicators: Web App
Virtualization Devices	Threat Indicators: Virtualization devices
IPS/IDS Devices	Threat Indicators: IPS/IDS devices
General Threat Indicators	Threat Indicators: General
Correlation Rules	Correlation rules: cross-device data correlation

Use Case Development: Threat Indicator Catalog



Threat Category	Threat type		Extended Info	Main properties of information			Controls	Infosec Events Requirement
				C	I	A		
External attack	T1	Carrying out denial of service attacks	Deliberately overloading systems and network devices or re-directing network traffic.	▨		X	1. Enable DoS/ DDoS prevention feature on IPS/ Firewalls	1. Log and monitor
							2. Enable Application level filtering feature on Firewalls	• Firewall, IPS and IDS alerts
							3. Monitor and review Firewall, IPS and IDS logs/ events	• significant changes in the number of IPs connected
							4. Keep the rule base/ signatures and OS updated on aforementioned security devices	• significant increase in rate of packet generation per IP
							5. Ov[illegible] capacity where	• [illegible] normal increase in

Use Case Development: Threat Controls

INCIDENT RESPONSE PROGRAM

Incident Lifecycle Management

Incident response requirements can be met by mapping decision points, inputs and outputs throughout the lifecycle of the incident.

The National Institute for Standards and Technology prescribes a process which includes the following steps:

- Preparation
- Detection and Analysis
- Containment, Eradication and Recovery
- Post-Incident Activity

Proper preparation ensures that incidents can be managed more efficiently and effectively, for example by defining incident priority and criticality levels along with response and remediation timelines.

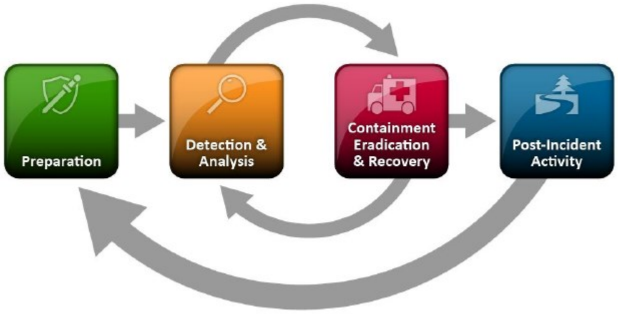
Incident response should address the incident triage process, clarifying the roles and responsibilities of different stakeholders. This typically includes a tiered escalation path and confidentiality for potentially sensitive communications.

Detailed documentation of workflows helps to clarify the incident response process. Response efficiencies can be greatly enhanced through automation. This is key to reducing the breach exposure time and preventing an attacker from turning an initial compromise into a breach.

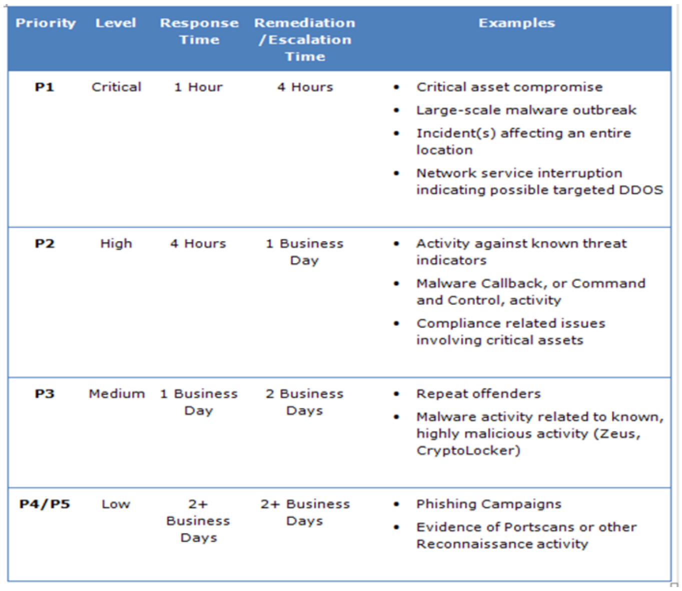
The incident response program clarifies SOC interdependencies with other stakeholders such as IT Network Operations. For example, the Systems Architecture Model may address the need to integrate the Incident Management and Ticketing systems to facilitate seamless handoffs between the SOC and IT teams. This would enable, for example, the security analyst to generate tickets for IT to clean a host system which has been infected by a virus.

Detailed response procedures can be compiled to clarify the tasks and activities associated with various incident categories and types. This is sometimes referred to as a "runbook," and is typically associated with SOC Implementation.

It is highly beneficial for an organization to identify the top threats it is likely to contend with. This may include alignment with other standards such as VERIS and the development of response procedures for incident categories such as malware, hacking, social, misuse, physical, error and environmental.

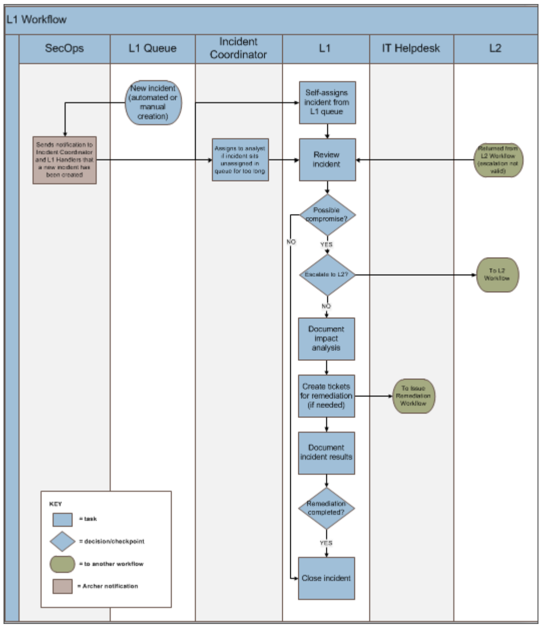


NIST 800-61: Incident Response Lifecycle



Priority	Level	Response Time	Remediation /Escalation Time	Examples
P1	Critical	1 Hour	4 Hours	• Critical asset compromise • Large-scale malware outbreak • Incident(s) affecting an entire location • Network service interruption indicating possible targeted DDOS
P2	High	4 Hours	1 Business Day	• Activity against known threat indicators • Malware Callback, or Command and Control, activity • Compliance related issues involving critical assets
P3	Medium	1 Business Day	2 Business Days	• Repeat offenders • Malware activity related to known, highly malicious activity (Zeus, CryptoLocker)
P4/P5	Low	2+ Business Days	2+ Business Days	• Phishing Campaigns • Evidence of Portscans or other Reconnaissance activity

Incident Categories and Prioritization


L1 Workflow
SecOps
L1 Queue
Incident Coordinator
L1
IT Helpdesk
L2
New incident (automated or manual creation)
Self-assigns incident from L1 queue
Sends notification to Incident Coordinator and L1 Handlers that a new incident has been created
Assigns to analyst if incident sits unassigned in queue for too long
Review incident
Returned from L2 Workflow (escalation not valid)
Possible compromise?
NO
YES
Escalate to L2?
To L2 Workflow
NO
Document impact analysis
Create tickets for remediation (if needed)
To Issue Remediation Workflow
Document incident results
Remediation completed?
YES
Close incident
KEY
= task
= decision/checkpoint
= to another workflow
= Archer notification

Level 1 SOC Analyst Workflow Model

ORGANIZATIONAL MODEL

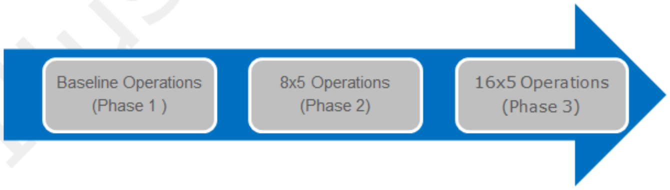
Staffing, roles & responsibilities

A SOC can be a complex and stressful environment as it requires a constant level of vigilance against persistent and determined adversaries. High levels of technical aptitude needs to be complemented with soft skills and values that include passion, persistence and resilience.

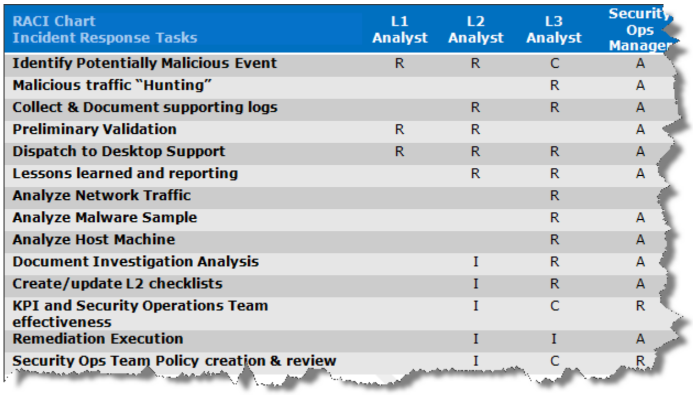
It takes time to build out a SOC organization's structure, staff it with the right people and retain such a highly specialized team. This can be addressed in part by planning a phased implementation model where capabilities are enhanced over time. For example, the SOC Design can stagger the rollout by beginning with interim coverage before progressing to full time coverage and by providing services on call during off-hours and weekends. In large organizations this may include a secondary SOC site. Procedures need to be implemented to ensure that a seamless shift-handoff process eliminates the potential for SOC downtime, which could result in a window of opportunity for attackers.

The shortage of cybersecurity staff and skills is a continuing reality, often topping the list of security concerns and challenges. RSA can help organizations bridge this gap by carefully identifying skills and certification requirements to ensure that qualified candidates with broader expertise are not omitted from the potential pool of eligible candidates.

As the organization ramps-up its staffing RSA can also provide residency services, complementing in-house resources with RSA Advanced Cyber Defense consultants for extended periods of time. This provides an excellent model for skills enhancement and knowledge transfer and can be particularly beneficial for accelerating the development of other capabilities such as a catalog of use cases, threat indicators and response procedures.

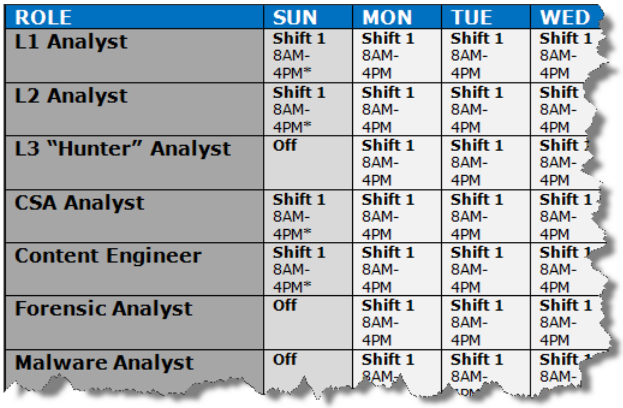


SOC Implementation: Phased Buildout



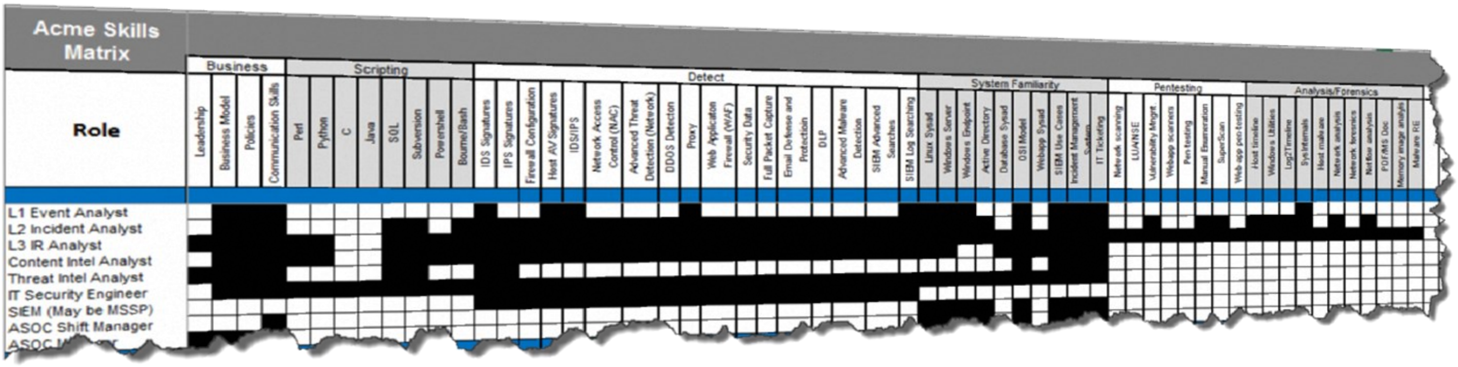
RACI Chart Incident Response Tasks	L1 Analyst	L2 Analyst	L3 Analyst	Securit Ops Manager
Identify Potentially Malicious Event	R	R	C	A
Malicious traffic "Hunting"			R	A
Collect & Document supporting logs		R	R	A
Preliminary Validation	R	R		A
Dispatch to Desktop Support	R	R	R	A
Lessons learned and reporting		R	R	A
Analyze Network Traffic			R	
Analyze Malware Sample			R	A
Analyze Host Machine			R	A
Document Investigation Analysis		I	R	A
Create/update L2 checklists		I	R	A
KPI and Security Operations Team effectiveness		I	C	R
Remediation Execution		I	I	A
Security Ops Team Policy creation & review		I	C	R

SOC Organization: RACI Chart



ROLE	SUN	MON	TUE	WED
L1 Analyst	Shift 1 8AM- 4PM*	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM
L2 Analyst	Shift 1 8AM- 4PM*	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM	Shift 8AM- 4PM
L3 "Hunter" Analyst	Off	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM
CSA Analyst	Shift 1 8AM- 4PM*	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM
Content Engineer	Shift 1 8AM- 4PM*	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM
Forensic Analyst	Off	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM	Shift 1 8AM- 4PM
Malware Analyst	Off	Shift 1 8AM-	Shift 1 8AM-	Shift 1 8AM-

SOC Organization: Shift Management


Acme Skills Matrix
Role
Business
Leadership
Business Model
Policies
Communication Skills
Scripting
Perl
Python
C
Java
SQL
Subversion
Powershell
Bourne/Bash
Detect
IDS Signatures
IPS Signatures
Firewall Configuration
Host AV Signatures
IDS/IPS
Network Access Control (NAC)
Advanced Threat Detection (Network)
DDOS Detection
Proxy
Web Application Firewall (WAF)
Security Data
Full Packet Capture
Email Defense and Protection
DLP
Advanced Malware Detection
SIEM Advanced Searches
SIEM Log Searching
System Familiarity
Linux Sysad
Windows Server
Windows Endpoint
Active Directory
Database Sysad
OSI Model
Webapp Sysad
SIEM Use Cases
Incident Management System
IT Ticketing
Pentesting
Network scanning
LUA/NSE
Vulnerability Mngmt.
Webapp scanners
Pen testing
Manual Enumeration
SuperScan
Web app pen-testing
Analysis/Forensics
Host timeline
Windows Utilities
Log2Timeline
SysInternals
Host malware
Network analysis
Network forensics
Netflow analysis
PDF/MS Doc
Memory image analysis
Malware RE
L1 Event Analyst
L2 Incident Analyst
L3 IR Analyst
Content Intel Analyst
Threat Intel Analyst
IT Security Engineer
SIEM (May be MSSP)
ASOC Shift Manager
ASOC M

Sample Staffing & Skills Model

RSA RESIDENCIES

SOC handover and transitioning

Due to the high level of skill and specialization needed as well as a tight labor market, it is often challenging to meet recruiting objectives. RSA provides Advanced Cyber Defense residency services to assist organizations with staffing. Through a process of shadowing and mentoring, staff can be groomed over time to take on more responsibilities.

RSA STRATEGY & ROADMAP

Setting the course for SOC Design

Along with a number of other services, RSA also offers the *RSA Strategy & Roadmap for Targeted Attack Defense* service. This service represents a compelling precursor to a SOC Design and helps organizations identify gaps and remediation requirements across their entire security program.

WHY WE ARE BETTER

Technical and Operational Expertise

RSA's ACD practice represents a team of professionals who have built and managed SOC's around the world, sharing resources and preferred practices with EMC's global Critical Incident Response Center, protecting over 60,000 employees in over 100 countries. The ACD practice includes our Incident Response team which has worked with customers across industry verticals and specializes in technical forensic analysis for targeted attack defense and remediation.

LEARN MORE

Detect Advanced Threats

RSA's portfolio of ACD services enables organizations to evolve from "being the hunted" to "be the hunter" and develop the strategies required to navigate the new terrain of targeted attacks.

For more information on the RSA's ACD capabilities, which are available on a global basis, please visit the web site: https://www.rsa.com.

ABOUT RSA

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. For more information, go to https://www.rsa.com.