Welcome to ciss316, a fast track to get a good job FASTER!!

Ciss316 will train you to be Tier 1 Cyber Security Analyst

In the Security Operations Center (SOC)

########## VDO on Cyber Security JOBS ##########

Another Link

Cyber Security Analyst Salaries in the United States - details

What is the average salary for jobs related to "cyber security analyst"?

The average salary for "cyber security analyst" ranges from approximately $41,744 per year for Intelligence Analyst to $106,256 per year for IT Security Specialist.

Average Base Pay-details:glassdoor.com

$76,410 / yr	**$53K Low**	**$76K Average**	**$116K High**

##########

Not all Security Operations Centers (SOC) are the Same.

- **Tier** 1 – Triage. This level of SOC services focuses on reviewing and assigning urgency to potential threats. ...
- **Tier** 2 – Incident Response. ...
- **Tier 3** – Proactive Cyber Defense. ...
- **Tier** 4 – **Operations**, Controls, and Management.

Apr 18, 2018

https://www.cyberhat.com/uncategorized/not-all-security-operations-centers-soc-are-the-same/

In general, there are four tiers of SOC services each having vital functions. However, as a rule, they all have two common foundations with security monitoring tools to receive contextually relevant information from both inside and outside the network (e.g., persistent outbound data

transfers, login/logoff, firewall activity, etc.). Also, these systems monitor cloud and on premise infrastructure services like DNS, email, web, domain controllers, and active directory services. Each sends information to log analysis, endpoint detection and response (EDR) or security information and event management (SIEM) tools. The second foundation of a SOC is leveraging these tools to find, identify and report suspicious or malicious activity from alerts. Below is an overview of the four tiers of SOC services.

Tier 1 – Triage.

This level of SOC services focuses on reviewing and assigning urgency to potential threats. They are the front line when reporting security incidents. Tier 1 SOC analysts run vulnerability and security assessment reports and manage security monitoring tools.

Tier 2 – Incident Response.

As trouble tickets or help desk alerts generated by tier 1 analysts, tier 2 leverages security controls, policies, and intelligence (indicators of compromise (IOC), rules, and procedures) to determine the scope and origin of the attack. Tier 2 SOCs focus on mitigation, recovery, and remediation once an attack has occurred.

Tier 3 – Proactive Cyber Defense.

This tier requires a combination of methods, technologies, and experience to hunt and kill cyber attacks. In addition to reviewing and developing a defensive posture from Tier 1 data, Tier 3 SOCs consistently look for vulnerabilities and access points into a network – hopefully without detection. Many organizations, especially in highly regulated industries like financial services, are turning to tier 3 and 4 level SOCs to ensure regulatory compliance, governance, and auditing the auditors.

Tier 4 – Operations, Controls, and Management.

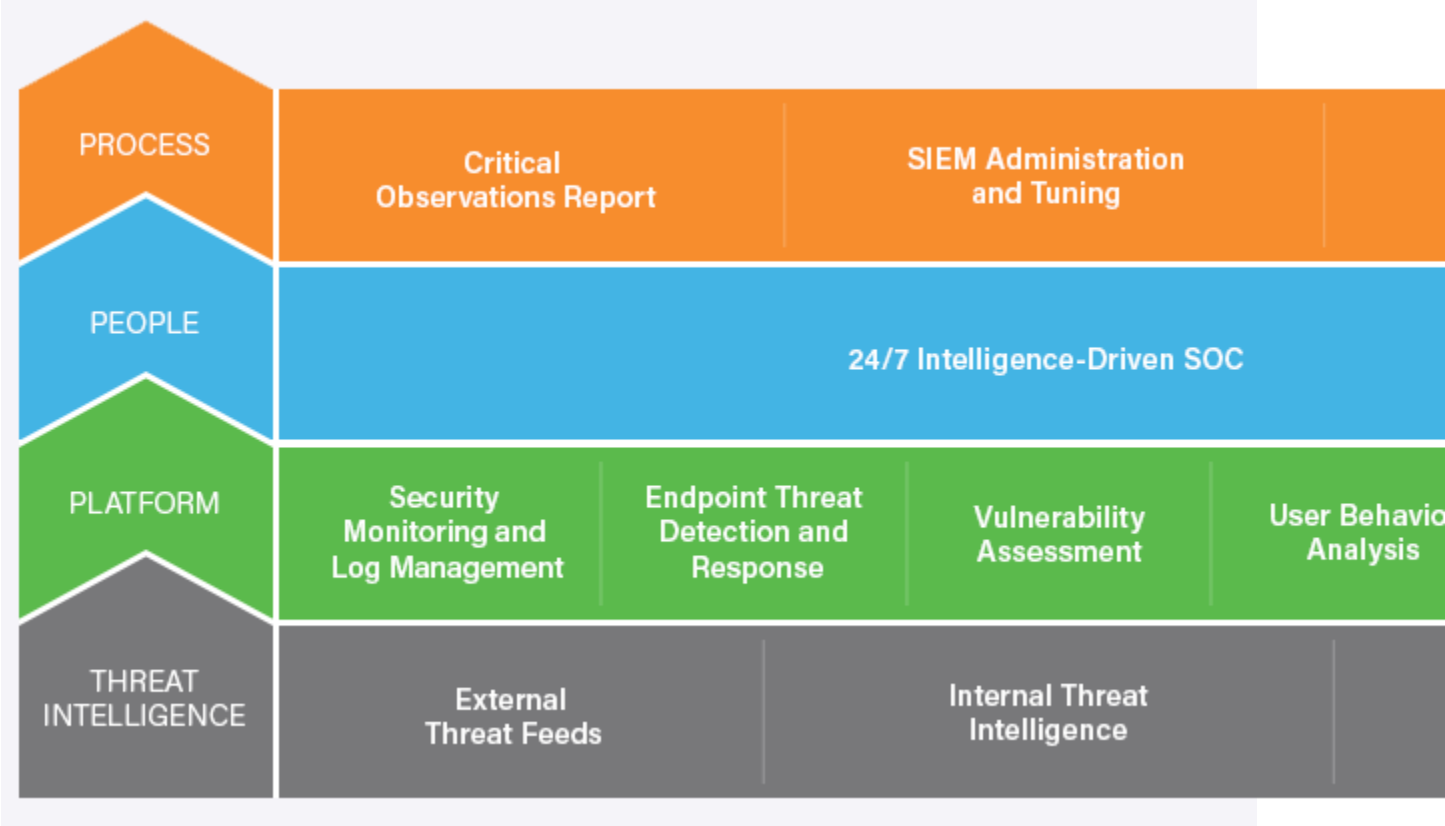
Tier 1-3 SOCs focus on the tactical activities of managing a SOC either defensively (tier 1-2) or proactively hunting threats (tier 3). At this level, the service provider typically oversees all aspects of a proactive – threat hunter – SOC operation including managing incident response programs, escalation processes, and developing the crisis communications plan across the organization. Tier 4 SOCs produce, report, and maintain performance metrics to protect their customer's executives, brands, and reputations.

While many SOC providers claim end-to-end security services, most fall woefully short and are only able to perform at tier 1 – 2 level. Moreover, most end-user organizations do not have the confidence, talent, or skills to contain and respond to a data breach. Research by an insurance service organization suggests companies can save over 65% (over a three year period) of the costs by outsourcing SOC services over building in-house, especially from an

operational and personal perspective. When determining which route to go from building vs. outsourcing a SOC, each tier and service provider has their strengths and weaknesses. It is important to do your homework, understand the limitations of each provider, and choose the right SOC as a Service provider based on your goals, internal skill-sets, and risk tolerance.

Critical SOC Components: Platform + People + Process

A good SOC must have three key interrelated components: platform, people, and process. The requirements and costs related to each of those components will change depending upon the approach you take to attaining our SOC. Understanding the advantages, disadvantages, and costs associated with each approach is critical for SOC success.


PROCESS
Critical Observations Report
SIEM Administration and Tuning
PEOPLE
24/7 Intelligence-Driven SOC
PLATFORM
Security Monitoring and Log Management
Endpoint Threat Detection and Response
Vulnerability Assessment
User Behavio Analysis
THREAT INTELLIGENCE
External Threat Feeds
Internal Threat Intelligence