The beginning of the new financial year is a great time to analyze our biggest strengths and
threat areas that need more attention. We hope that this issue will address those questions.

Threat Intelligence Analysts

Webinar

FIRST 90 DAYS AS A CISO

Slideshare

about cybersecurity that have remained unanswered, until now.

Detecting incident security

MITIGATE SUCH RISKS?

Blog

How to become a
cybersecurity incident...

methodically responding to a
Incident response is a plan for
LIFE CYCLE? EVERYTHING YOU

collecting data through the Google Hacking Database and other
threat intelligence, and technical threat intelligence.

Must be able to form a report
Communicate with potential
Forensic
Analyst

Must be proficient when collecting data
Must be able to deal with the different types of threat

– 4 KEY CAPABILITIES

System monitoring
Since a SOC monitors everything that's
visibility is seeing exactly what devices

WHAT IS THE ROLE OF A THREAT

INDICATORS OF COMPROMISE

5 OF THE HIGHEST- PAYING

- 4 KEY CAPABILITIES

WHAT ARE THE

- 4 KEY CAPABILITIES

System monitoring
Since a SOC monitors everything that's
visibility is seeing exactly what devices

DO YOU KNOW WHAT IOT

ENVIRONMENT?

WHO CAN RESPOND TO AN INSIDER THREAT?

DO YOU KNOW HOW TO RESPOND TO AN INSIDER THREAT?

SOC Analyst Roles

Tier 1 Analyst (Response)

Tier 2 Analyst (Investigation)

Tier 3 Analyst (Decision Support)

Tier 4 Analyst (Management)

Tier 5 Analyst (Executive)

Tier 6 Analyst (Policy)

Tier 7 Analyst (Consulting)

Tier 8 Analyst (Forensics)

Tier 9 Analyst (Research)

Tier 10 Analyst (Product)

Tier 11 Analyst (Sales)

Tier 12 Analyst (Marketing)

Tier 13 Analyst (Support)

Tier 14 Analyst (Partnership)

Tier 15 Analyst (Community)

Tier 16 Analyst (Security)

Tier 17 Analyst (Data)

Tier 18 Analyst (Analytics)

Tier 19 Analyst (Automation)

Tier 20 Analyst (Automation)

Tier 21 Analyst (Automation)

Tier 22 Analyst (Automation)

Tier 23 Analyst (Automation)

Tier 24 Analyst (Automation)

Tier 25 Analyst (Automation)

Tier 26 Analyst (Automation)

Tier 27 Analyst (Automation)

Tier 28 Analyst (Automation)

Tier 29 Analyst (Automation)

Tier 30 Analyst (Automation)

Tier 31 Analyst (Automation)

Tier 32 Analyst (Automation)

Tier 33 Analyst (Automation)

Tier 34 Analyst (Automation)

Tier 35 Analyst (Automation)

Tier 36 Analyst (Automation)

Tier 37 Analyst (Automation)

Tier 38 Analyst (Automation)

Tier 39 Analyst (Automation)

Tier 40 Analyst (Automation)