Evolution of the SOC Analyst

**SOC Analyst**

*How they spend their day*

- managing low fidelity alerts (80%)
- reporting, shift ops, tool maintenance (20%)

*How they are measured*

- Reduction in alert investigation time
- Reduction in alert volume

*Job satisfaction*

- 73% of SOC analysts say that 25%-75% of alerts are false positives
- More than 70% of SOC analysts are overwhelmed investigating over 10 alerts per day
- Job satisfaction falls to less than 50% after just a few years in the role
- 28% of SOC analysts say they have never stopped an intrusion and don’t feel they are making a difference
- Over half of SOC analysts teams have a turnover of more than 25% 

**Threat Hunter**

*How they spend their day*

- investigating high fidelity alert (05%)
- strategic project work playbooks for threat analysis (20%)
- monitoring and investigating audit and new activity alerts (20%)
- maintenance and configuration of security tools (20%)
- reviewing threat intelligence and apply to environment (35%)

*How they are measured*

- Number of artifacts processed with ATT&CK tags
- Number of alerts and defensive measures created
- Amount of threat intelligence cases
- Number of continuous monitoring capabilities

*Job satisfaction*

- "Our days are much more exciting. We are more proactive instead of waiting for things to happen."
- "I love being able to investigate a problem, solve it, then stop it from happening again."
- "We are much more strategic now. Alerts are tuned so we only see things that make the most impact."

**Why the Role is Changing**

1. Learning the environment and what is “normal” so alerts can be tuned
2. Alert tuning and automation improved in security tools
3. More and better training available for SOC Analysts to tune and create high fidelity alerts
4. Threat research and intelligence more frequent and available
5. Less overall alerts gives Analysts more time to process threat research

---

**Graph Key**

- Low fidelity alerts
- High fidelity alerts

---

**VMware, Inc.**

---

**VMware, Inc.**

---

**VMware, Inc.**

---

**VMware, Inc.**

---