SOC of the Future - Leveraging Automation, Orchestration & Machine Learning

Asset Transparency + ML-based Threat Management (UEBA) + SIEM + SOAR - Leveraging Machine Learning (ML) and automation to pro-actively address risk and employ machine-speed incident response for a majority of traditional Tier 1 events.

1 - SOC Analyst leverages a unified UX to monitor instrumentation & cybersecurity posture, as tools become more automated, ML-driven & self-directing. They collaborate with broader business teams, and focus more on strategy and business risk mitigation.

2 - Analyst has insight into ALL assets on the network, and would be alerted to a rogue device. However, quicker than the analyst can determine whether this is a problem, the SIEM is informed.

3 - While a device has been compromised, things happen so quickly that the analyst likely won’t need to respond to an alert before automated security measures have mitigated the risk...

4 - Analyst is alerted to activities that are outside of “normal,” and in this case, could see a network scanning alert as picked up by a UEBA & ML tool. At the same time, the SIEM is already integrating alert data.

5 - Before the analyst has time to process the alerts they are seeing, the SIEM has begun correlating alert data from the UBAE and rogue device tools. This is much faster than the analyst could do on their own.

6 - Quickly after the initial incidents occur (appearing as lesser, isolated alerts) in yesterday’s SOC, the system leverages the SOAR to piece together the disparate data points to establish an entire attack model.

7 - Again, in a matter of minutes, and likely without any SOC analyst intervention, the attack is identified, response actions initiated, and damage prevented.

8 - The SOC analyst will mostly see...