Operationalizing the MITRE ATT&CK Framework in Security Operations

Primary security analytics and operations objectives.

As the threat and volume of attacks against businesses have grown, the demand for effective security operations has increased. Security operations teams are using security analytics and operations (SOAR) tools to improve their operations. These solutions can help you improve your organization’s security by providing visibility into security events, handling incidents more efficiently, and automating security tasks.

Security analytics and operations landscape grows increasingly complex.

Unfortunately, meeting these objectives won’t be easy. The complexity of modern threats, the diversity of data sources, and the increasing volume of data make it difficult to capture, correlate, analyze, and act upon security events. The volume of security data needed for analysis, and the overwhelming number of factors like the increasingly dangerous threat landscape, makes it difficult to understand what threats your organization is facing, and what steps you should take to mitigate them.

Plans for security analytics and operations automation.

To scale security operations, many organizations are implementing SOA technologies to help them automate security operations processes. More organizations are already using these technologies, while others are piloting the technology to gain experience. SOA technologies can help organizations improve their efficiency and effectiveness by automating tasks, reducing response times, and improving decision-making.

Priorities for security analytics and operations automation.

SOC teams have ambitious goals for security automation and orchestration. They are striving to integrate security and IT operations, automate tasks and orchestrate workflows, and increase visibility into security events. These priorities are driven by the increasing complexity of security threats, the need for more efficient operations, and the desire to improve the overall security posture of the organization.

The Bigger Truth

Servicenow provides a platform that enables SOAR to drive automation and orchestration in your environment. Servicenow’s automation capabilities, like the MITRE ATT&CK Framework, can help you improve your security operations by automating tasks, reducing response times, and improving decision-making. This can help you improve your organization’s security posture and increase visibility into security events.