

SecureX

Implementation Project Job Aid

Steven McNutt, CCIE #6945

Contents

[A. Internal Communication Example 3](#_Toc80794592)

[B. Fact Sheet Example 4](#_Toc80794593)

# A. Internal Communication Example

ACME Widget Corp.

Memo

|  |  |
| --- | --- |
| To: | Bubba Smith, CEO; Executive Leadership Team |
| From: | Steven McNutt |
| Date: | Monday, August 23, 2021 |
| Re: | Proposal For implementation of Extended Detection and Response (SecureX) |

Mr. Smith and Executive Leadership Team,

As part of our Security Enterprise agreement with Cisco, we have acquired an XDR (Extended Detection and Response) tool called SecureX. The capability provided by this tool will enable the organization to respond to security incidents more quickly and in a more cohesive fashion. Speed is everything at the onset of a security incident, so we regard this as a high impact capability.

SecureX enables operational teams within the organization to rapidly respond to and collaborate on Security incidents by tying together and correlating threat intelligence information from all available sources and packaging them into case files. Resources can be added to the response and quickly become integrated through the use of the case file, which also provides a historical record of the incident.

Because this is a tool that consumes data from a variety of sources and is intended for use by multiple teams coordinating together, there is some work required to properly operationalize the tool in ACME’s environment. If approved we would need:

* An executive sponsor
* Full-time project manger
* One team member from each department approximately 4-6 hours a week
* Three simulated incidents to test and validate

We believe the implementation time would be approximately forty-five days from start to finish. There is no product cost as ACME already owns the right to use SecureX by virtue of its Enterprise Agreement with Cisco Systems.

I appreciate your consideration in this matter and look forward to your response.

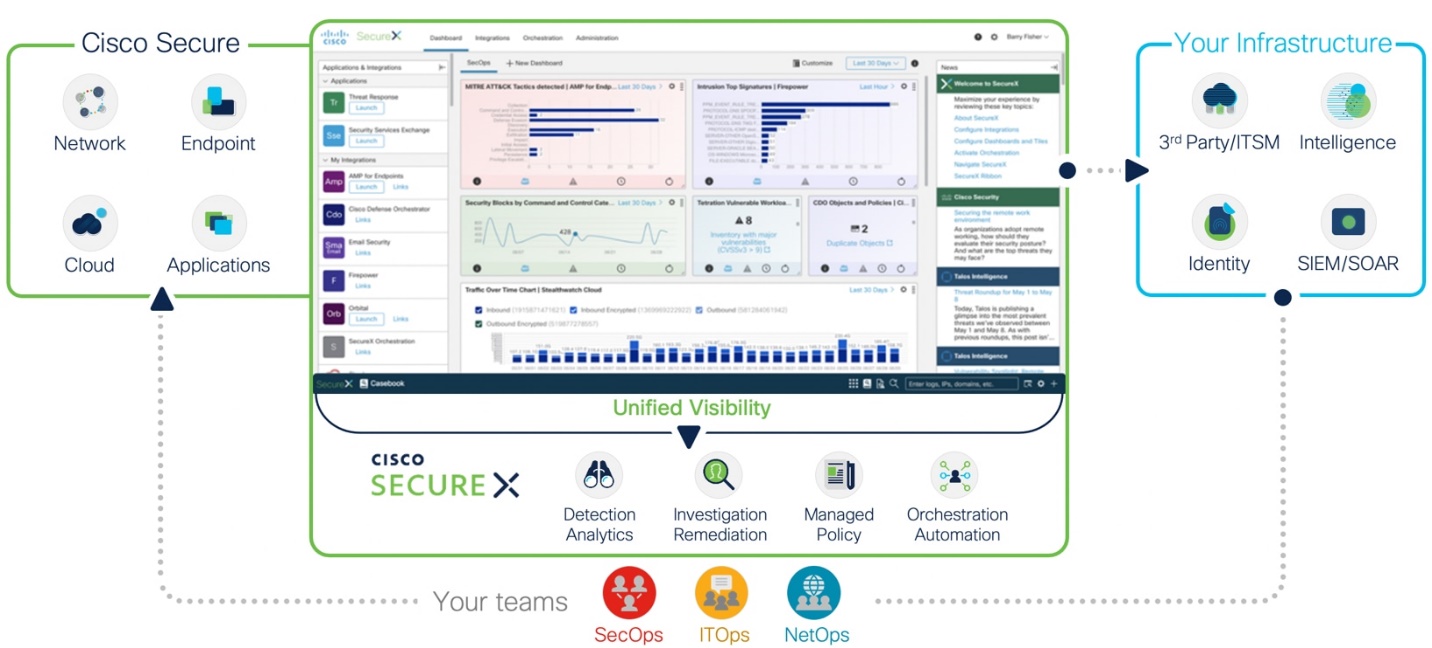
Steven McNutt

# B. Fact Sheet Example

SecureX Extended Detection & Response

**(XDR)**

**&**



**When detecting and responding to a Security incident, speed is crucial**.

Determining the Scope and severity of the breach, gathering and investigating artifacts, stopping the spread. The faster this process happens the better the outcome. It could mean the difference between a few computers being encrypted and the entire business being shut down by a ransomware attack.

SecureX accelerates this process by pulling in threat intelligence from multiple tools, correlating the data, and taking the appropriate response, all while facilitating cross-team collaboration.

**Critical to the success of SecureX is for operations teams to work together as a cohesive unit, regardless of job role or location**.

Everyone will receive basic training on SecureX. There will be three cohorts, each populated from members of different operations teams.

Once basic training has occurred there will be a series of three simulated incidents. The team that performs best will win a company catered lunch and a hundred-dollar gift certificate for each member.

Training

Implementation Phases

SecureX XDR

1. In Phase one a tiger team of representatives from each functional team will receive training on SecureX

2. In phase 2 the tiger team will integrate existing tools and products will into SecureX, and the incident response playbook will be updated to include SecureX based workflows

3. In phase three all members of all teams will receive training on SecureX

4. In Phase four there will be a series of simulated incidents to fine tune the response plan and to gain experience

