Seven Strategies for Defending Industrial Controls:

PARTNER WITH BAKER HUGHES, A GE COMPANY (BHGE) TO HELP PROTECT YOUR CONTROL SYSTEM

As the industrial world becomes more digitally connected, cyber security vulnerabilities are on the rise. Industrial Control Systems are a frequent target and need to be protected.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published Seven Strategies to Effectively Defend Industrial Control Systems. These strategies can be used to mitigate the top threats commonly aimed at industrial control systems.

BHGE's SecurityST solution support all seven strategies recommended by ICS-CERT. This centralized security management platform provides a single vantage point to view and manage your cyber security posture.

SECURITYST FEATURES INCLUDE

- **Role-based Access Control**
- **Application Whitelisting**
- **Centralized and Validated Patch Management**
- **Security Information and Event Management**
- **Remote Access Security**
- **Network Intrusion Detection and Prevention System**
- **Backup and Recovery**
- **Endpoint Protection**

SecurityST addresses **ALL 7 STRATEGIES**

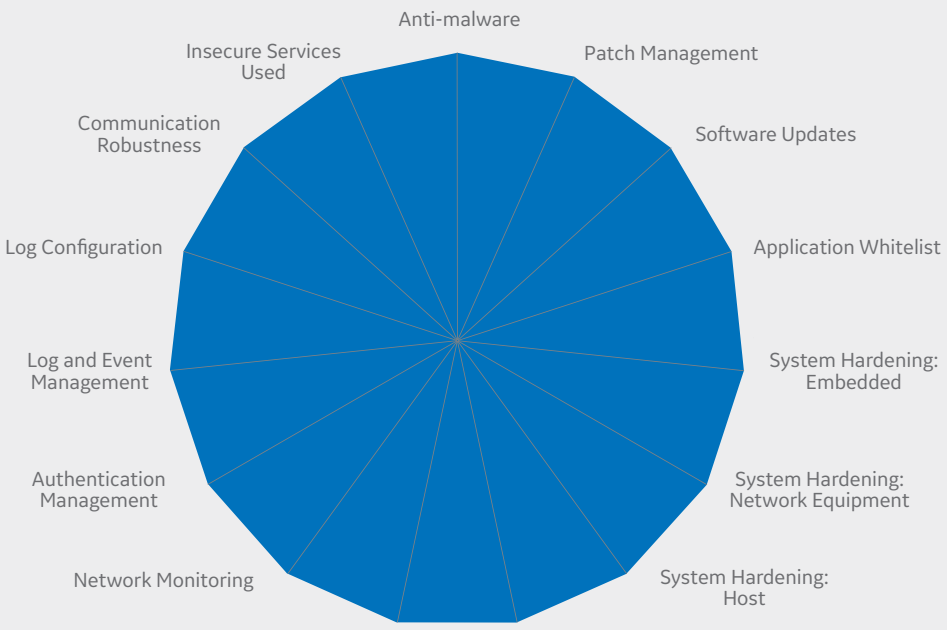
Percentages represent the number of ICS-CERT reported incidents in 2014 and 2015 that would have been prevented using that specific strategy.

- 38% APPLICATION WHITELISTING
- 29% PROPER CONFIGURATION/ PATCH MANAGEMENT
- 17% REDUCE YOUR ATTACK SURFACE
- 9% BUILD A DEFENDABLE ENVIRONMENT
- 4% MANAGE AUTHENTICATION
- 2% MONITOR AND RESPOND
- 1% SECURE REMOTE ACCESS

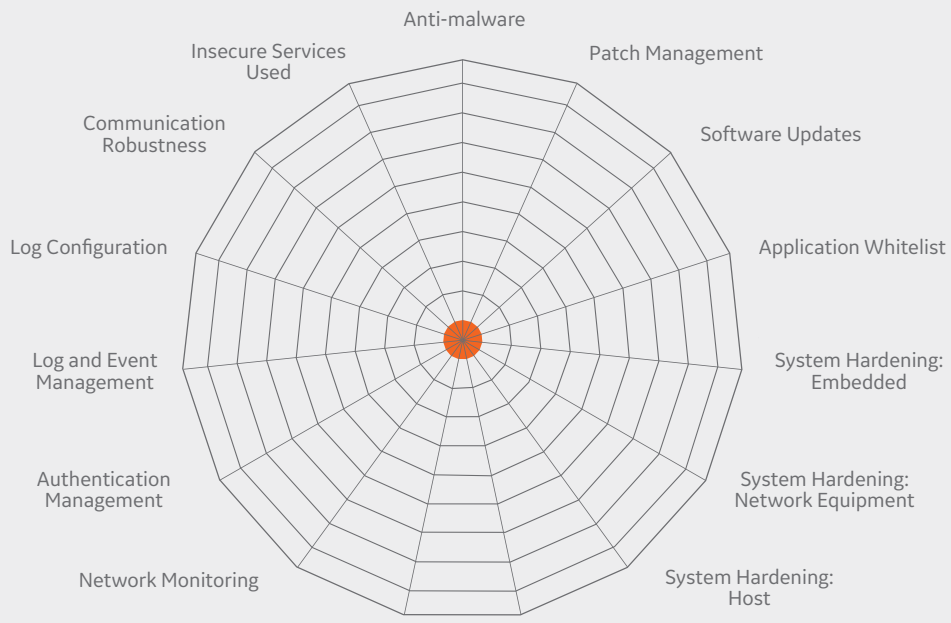
REDUCING YOUR ATTACK SURFACE

When attack surfaces are uniformly and consistently addressed, technical controls can be implemented or corrected to provide suitable protection and improve security posture. SecurityST can reduce your attack surface and help to mitigate overall security risks.

As-Is Security Posture:
Large Attack Surface

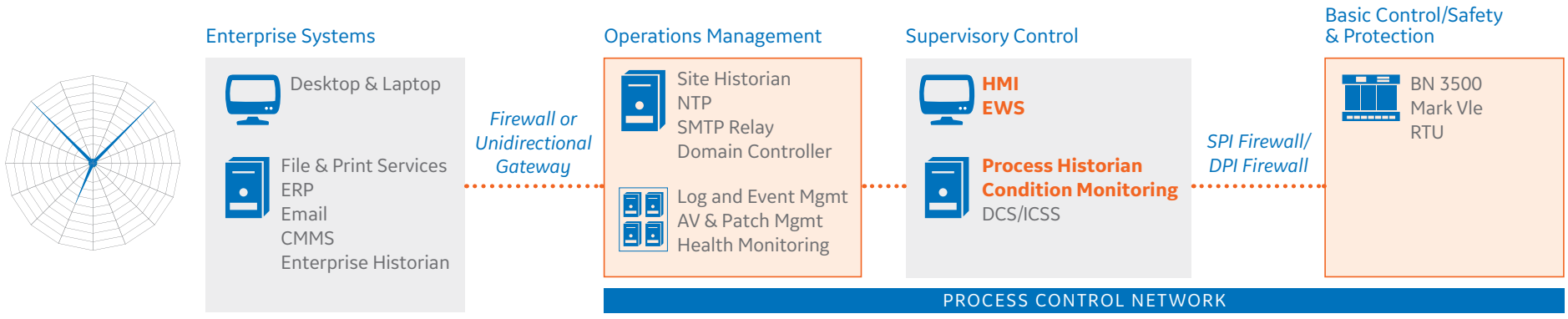


Objective Security Posture:
Small Attack Surface



■ High Risk: Large Attack Service
■ Low Risk: Small Attack Service

USING TECHNICAL CONTROLS TO MITIGATE THREATS: **SECURITYST**



CYBER SECURITY BY THE NUMBERS

7
NUMBER OF STRATEGIES
recommend by ICS-CERT to mitigate top cyber threats.

243
AVERAGE NUMBER OF DAYS
before detection that a system is compromised.

10/12
THE NUMBER OF SOFTWARE PATCHES TESTED MONTHLY
in the BHGE Validation Lab that require modifications to ensure no negative effect on operations.

26%
OF INCIDENTS
investigated by ICS-CERT were spear phishing, making it the leading threat for 2016.

74%
OF EXPLOITS
are targeted at applications, with more than 40% of those being Microsoft & Adobe.

98%
NUMBER OF INCIDENTS
ICS-CERT responded to in FY2014 and FY2015 that would have been prevented using the Seven Strategies.

BAKER HUGHES
a GE company

CS16051-01 08/2017