GE
Grid Solutions

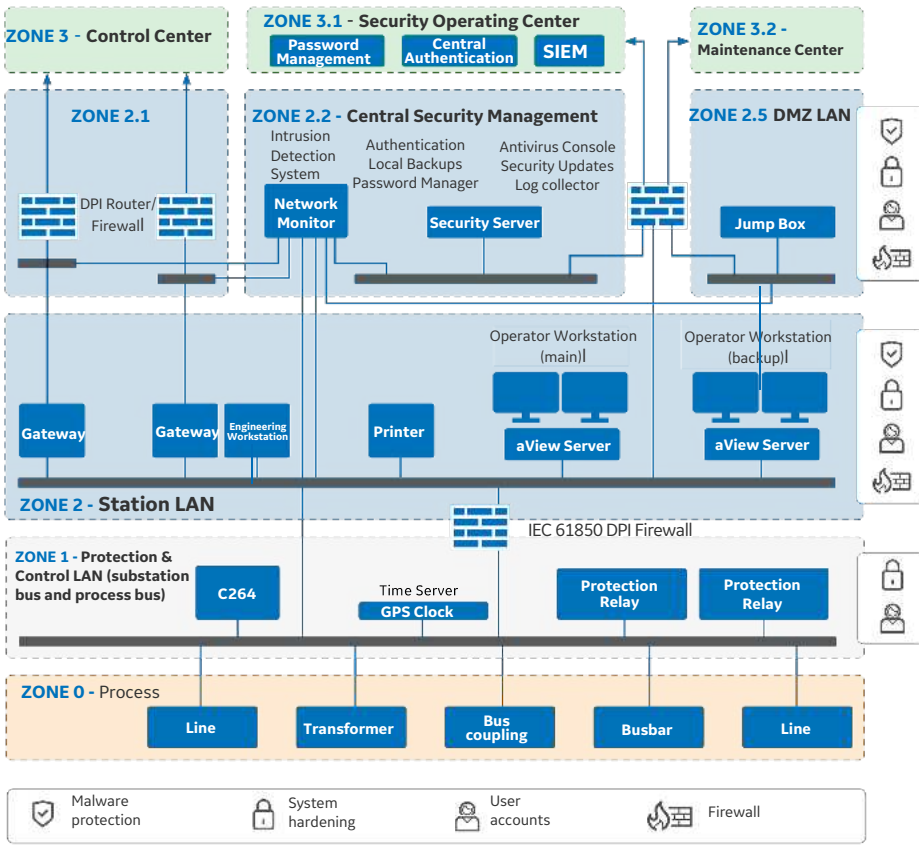
CyberSentry™ for DS Agile Substation Cyber Security

Defence In-depth Applied to Substation Automation

To mitigate the impact of deliberate or inadvertent cyber security events, substation operators need to deploy an in-depth, multi-layer defensive strategy. CyberSentry™ enables GE's DS Agile digital substation control system to provide this cyber security, working as an integrated component of an operator IT system and infrastructure.

In line with the latest in industry cyber security standards such as NERC, IEC and IEEE, the DS Agile system employs the same type of multi-layer strategy to mitigate risks or unplanned downtime associated with cyber-attacks.

DS Agile Security Architecture



Multiple Layers of Security

- Secure by design
- Network security
- Host hardening
- Malware prevention
- Authentication, RBAC
- Security event logging

Security Services

- Risk assessment, audit
- User training
- System upgrades
- Consulting
- Security updates

Applications

- Power generation, transmission and distribution utilities
- Oil & Gas
- Industrial
- Greenfield, brownfield

Figure 1: Secure Architecture
The Electronic Security Perimeter (as defined by NERC) is the DCS LANs, defined by zones 1 to 2.5 in the diagram

Imagination at work

DS Agile Cyber Security Strategy

The different technical countermeasures used to ensure cyber threat detection, prevention and protection in DS Agile are highlighted hereafter. On top of these different security layers, operational and emergency procedures combined with user training are also needed to achieve proper security implementation.

Security Development Lifecycle (SDL)

Our SDL process identifies threats to the products, ensures that product security requirements are included in the design and tested, and verifies software and firmware code for potential weaknesses to ensure a high quality of design and coding in all releases.

Network Security

Virtual Private Network

Communication between the substation and other remote systems (remote centers or other substations) are tunneled in a virtual private network (VPN) - a secure encrypted point-to-point communication channel.

Network Segregation

Global protection of the ESP is ensured by a firewall that denies all communications by default, and allows only required communication protocols between specific zones, typically forwarding all inbound traffic to the DMZ.

Intrusion Detection System (IDS)

The network IDS is configured to detect and report malicious traffic allowing an authorized operator to react quickly upon threat detection to block the threat and minimize its impact.

Jump Box

Remote maintenance is done by connecting to a “jump box” (a standard PC with Ethernet access) in the DMZ zone, and from there accessing a restricted list of devices and applications on the private zone. This allows controlling the traffic to the substation IEDs.

Switches

Switches are configured to reduce threat impact on the network by organizing the LAN traffic (broadcast storm limitation, QoS to prioritize IEC-61850 traffic, VLANs to segregate traffic, MAC address filtering, etc.).

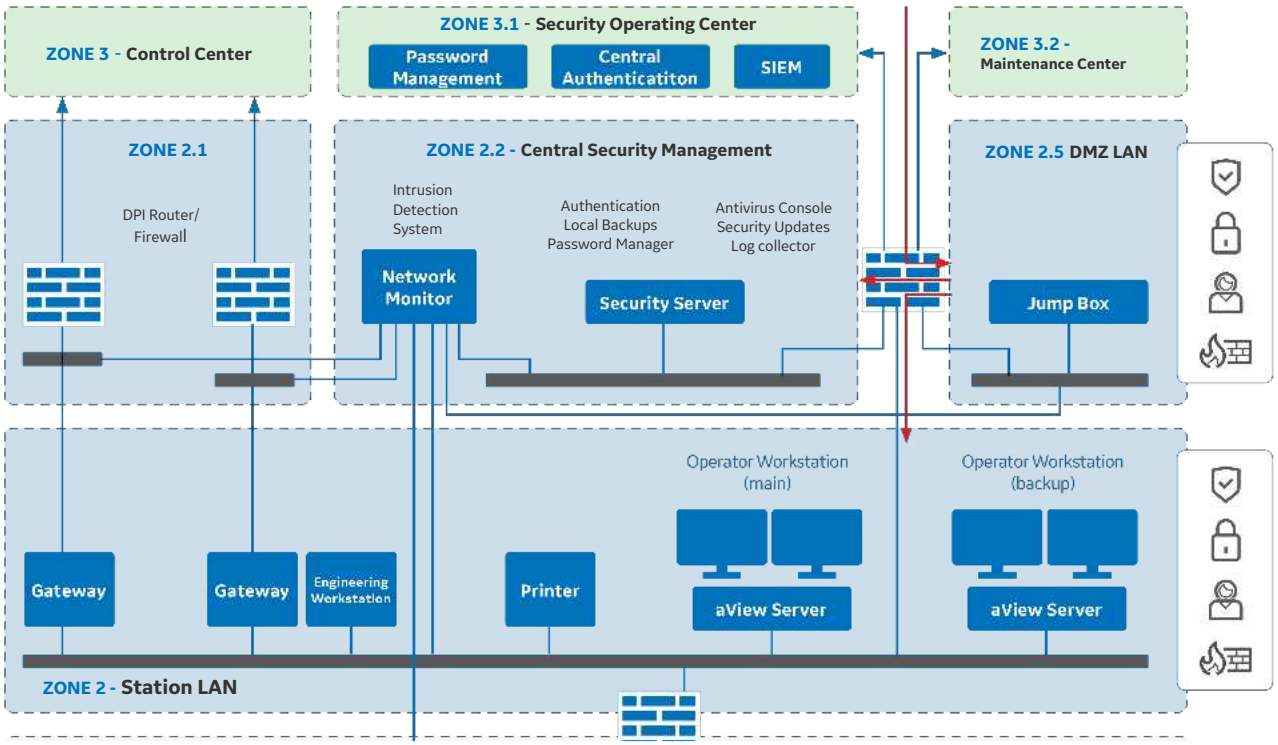


Figure 2: Router forwarding external communications to DMZ

Host Security

System Hardening

Hardening aiming at improving security by reducing the number of possibilities a threat has to disrupt or take control of the operating system on which DS Agile software is installed.

- Network services and TCP/IP ports are enabled on a per-need basis
- Physical communication ports are disabled, where possible
- Unnecessary user accounts are disabled
- Audit and password policies are set
- User sessions are automatically terminated after a configurable time out
- Users are locked out after password verification failed for a configurable number of times
- DS Agile C264 is certified Achilles© ACC Level 1

Host Firewall

As a complement to the LAN firewall, software firewalls on PCs are configured to allow only the required communication flows between authorized devices.

Malware Prevention

- Application Control (Whitelist)

  All PC in the DS Agile system come with whitelisting software installed and configured.
  Whitelisting software will not allow a program execution unless it is present in the whitelist ("deny by default" policy) and will not allow software installation or update unless it is digitally signed by a trusted party. This guarantees the binary file integrity and authenticity on the PC and effectively blocks unknown malware.

- Anti-virus

  Optionally, as a complement to the application whitelist, an antivirus scanner can be installed for on-demand scans.

Software Integrity

All GE software and firmware are digitally signed to guarantee authenticity and integrity at installation time.

Application Security

Authentication

All users are required to authenticate to interact with any IED. Users have individual accounts and passwords (no shared accounts).

There are no backdoors or hardcoded user accounts.

It is possible to enable a password policy to configure the minimum password length and character content which provides the complexity looked for.

All passwords are securely stored using a one-way secure hash algorithm with a unique salt which mathematically ensures that clear text passwords cannot be extracted from the system.

DS Agile can authenticate users to a central authentication service using the LDAP over TLS secure protocol, such as a Microsoft Active Directory server. Users can then be managed centrally.

Authorization

DS Agile implements Role Based Access Control (RBAC) to tightly manage the authorized users. Each user account is assigned one or more roles and associated rights.

The main roles are according to IEC62351-8.

In addition to these roles, it is possible to configure additional custom roles in the aView operator interface to meet the "least privilege" concept.

Secure Communications

IEC62351-3 on SCADA link

The IEC69870-5-104 SCADA link is secured according to the IEC62351-3 standard.

When the SCADA does not support encryption, link is secured using the VPN feature of the router/firewall.

The VPN can transport IEC-60870-5-104 as well as serial protocols.

Maintenance protocols
Configuration protocols are secured either with TLS or SSH.

Remote Access
Authentication can be required to access the substation LAN remotely by configuring the firewall as a proxy authentication, as mentioned in the network security section.

Network and System Security Guide

DS Agile is delivered with its Network and System Security Guide which documents all system's cyber security related information:

- Installation sequential steps, including hardening, application control, default password changes
- List of protocols and ports that are used in the installed system
- Deviations from the standard installation (to allow for later auditing)
- Good practices for a secure system

This guide allows the engineering teams to properly configure the cyber security of the system and is a baseline for future audit to ensure security continuity.

Security Event Logging

All basic security events are logged on each device:

- Successful and failed login attempts
- User management actions including password changes and role assignment
- Configuration database changes

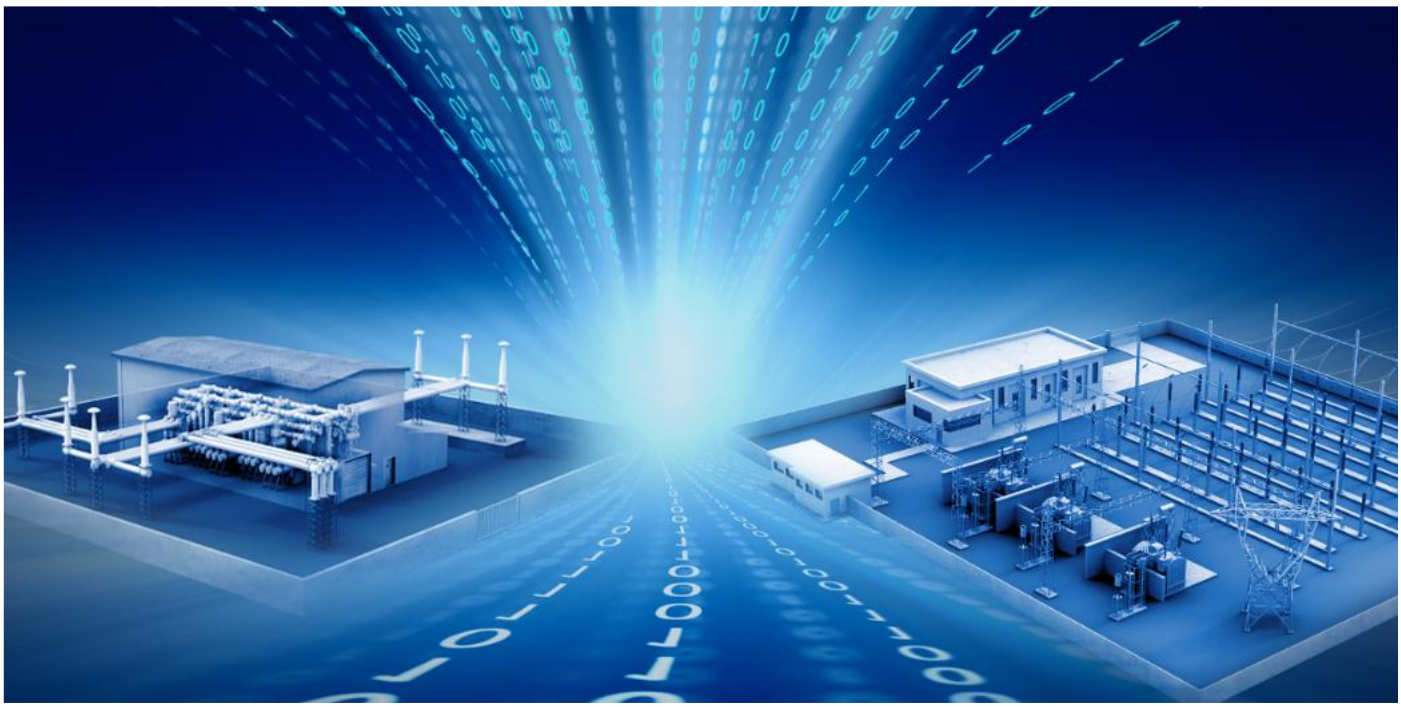
The logs include the user name, originating IP, timestamp and action description. No sensitive information (such as passwords) is logged.

Logs can be forwarded to a central logging system using the SYSLOG protocol over UDP, TCP or TLS.

Security Updates

As a service contract, GE provides:

- Monthly security bulletins informing about Microsoft Windows 10 security update availability, their applicability to and compatibility with DS Agile. Security updates are tested in a controlled, representative environment simulating a customer's typical control system in our R&D lab
- Event driven security notices of newly discovered vulnerabilities in DS Agile, including severity and possible mitigation measures
- DS Agile firmware security updates
- Security updates deployment, on site or remotely



CyberSentry™ Security Services

CyberSentry™ includes a comprehensive portfolio of services to support our customers on their cyber security journey:

- Design of a new substation with cyber security as a solid foundation
- Cyber security posture improvement of installed systems without any process change and minimizing - or eliminating - the need for an outage
- Security awareness training
- On-going support to sustain security
- Upgrade services to benefit from the state-of-art security of the latest versions
- Security update maintenance contract

Four Step Process to Optimize Cyber Security Posture Improvements

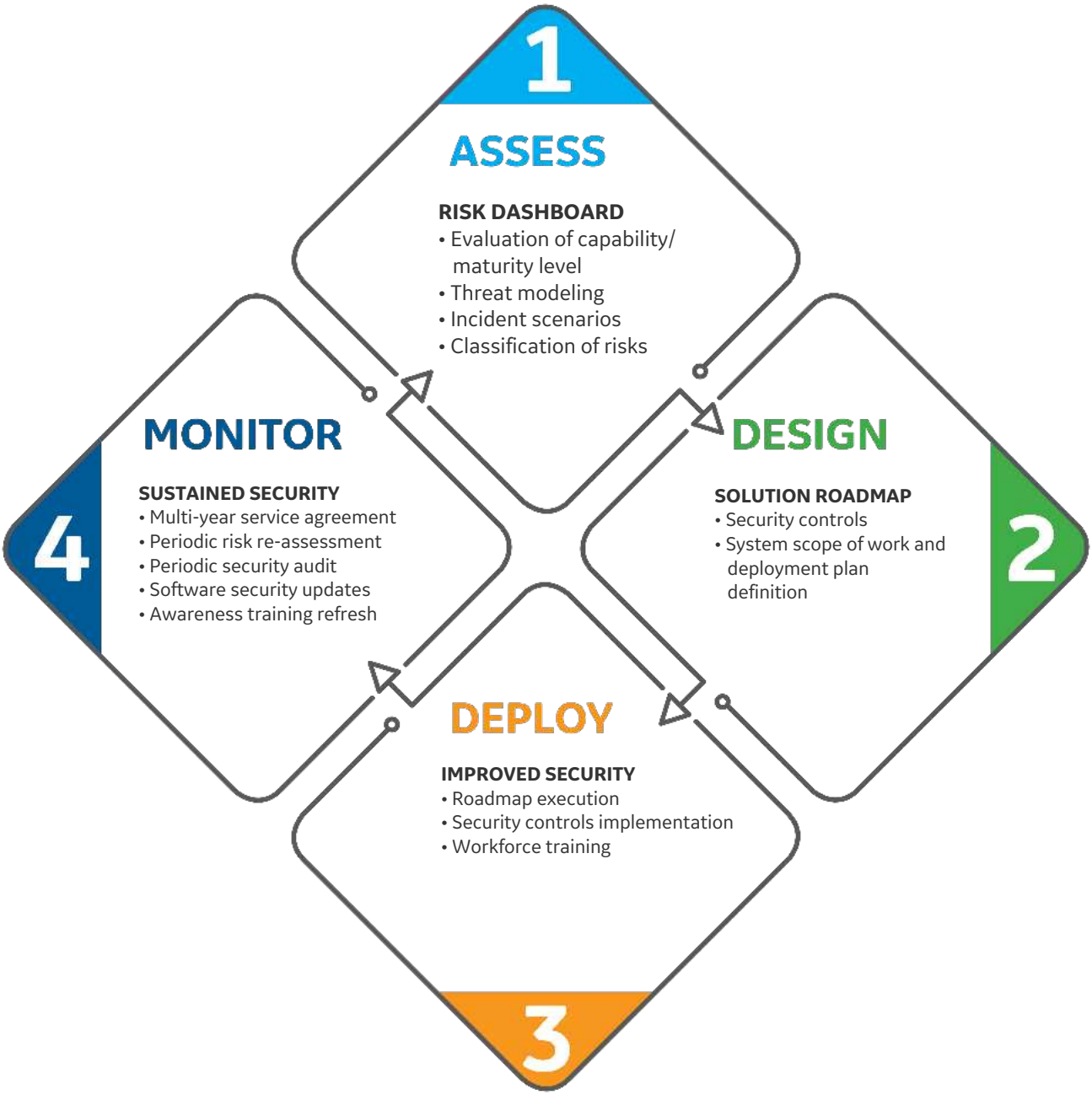


Figure 3: Security cycle

Conclusion

GE has strongly reinforced the substation cyber security by implementing in DS Agile this differentiated defense in-depth strategy with emphasis on prevention and detection at each level in DS Agile architecture.

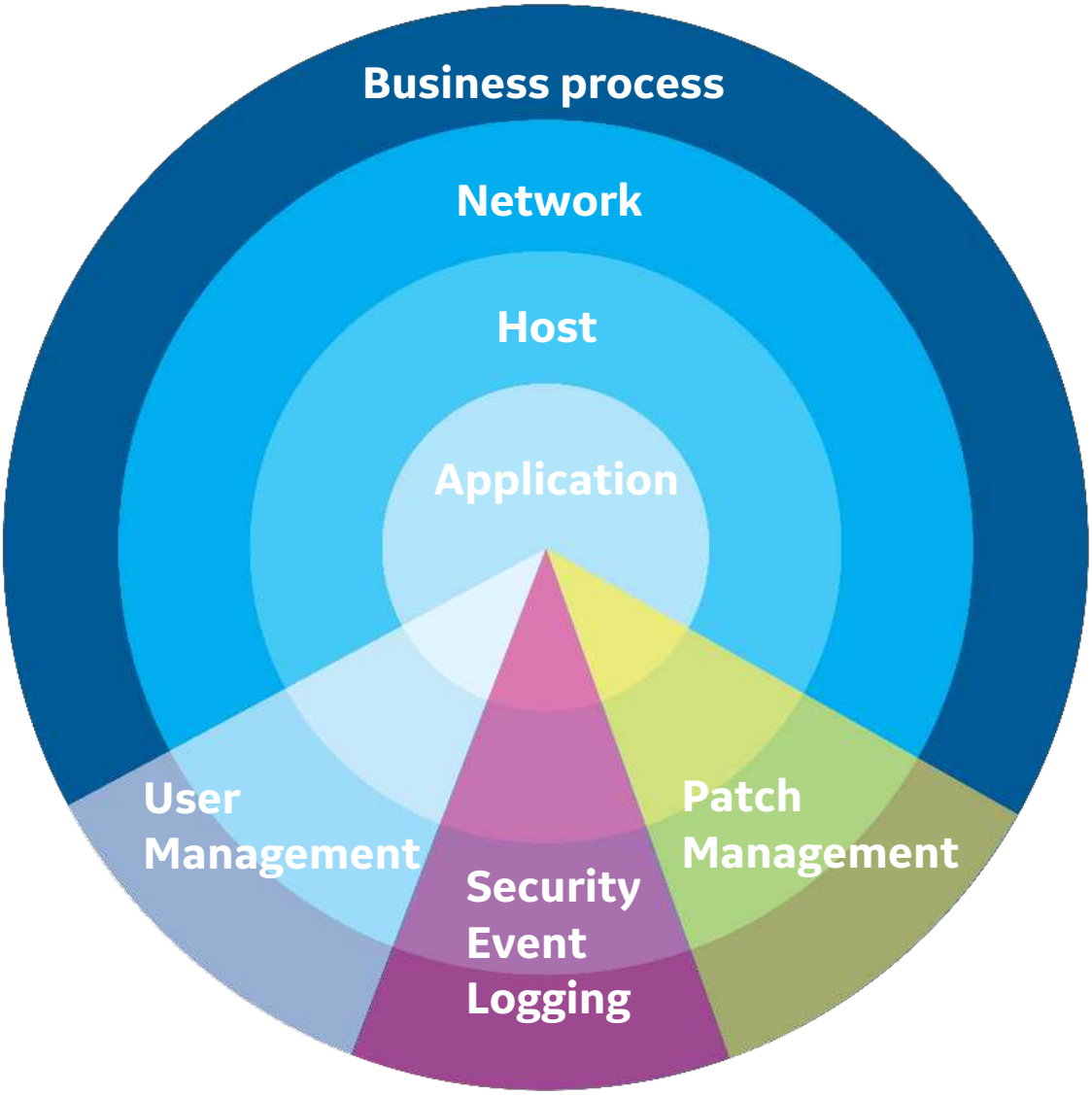


Figure 4: Defense-in-depth

For more information please contact
GE
Grid Solutions

Worldwide Contact Center

Web: www.GEGridSolutions.com/contact
Phone: +44 (0) 1785 250 070

GEGridSolutions.com

Imagination at work