Deloitte.

Essential 8 Maturity Uplift with Splunk

Organisations have made **significant commitments** to the Splunk platform for Cyber and IT resilience. This presents an opportunity to leverage existing **Splunk investments** to support the uplift of **Essential 8 maturity** through continuous monitoring of controls and an integrated, holistic approach to the Essential 8 maturity journey.

Deloitte Essential 8 Continuous Monitoring Solution

Essential 8 compliance can be complex. IT environments are **continually evolving** requiring solutions that support ongoing risk-based insights into current state maturity. At Deloitte we **help organisations** on their Essential 8 maturity journey through our continuous visibility solution that delivers real-time insights to enable the uplift and ongoing monitoring of **Essential 8 controls**. Built on the Splunk platform, our app **integrates self-assessment** with monitoring of key systems and applications alongside expert consulting to help implement ongoing **compliance monitoring.**

Real-time Awareness

Transition away from point in time, manual assessments to understanding current state of **maturity in real-time** for improved management of risks, through well defined mitigation strategies. Incorporate a risk-based approach to conducting assessments and mitigate the **impact of non-compliance** proactively to **drive maturity uplift**.

Level Up

Combine **active monitoring** with integrated self-assessment to gain comprehensive understanding of both the effectiveness and the level of **success of mitigation** strategies such as back up, patching and application whitelisting.

Cluster-wide Insights

Enable Agency clusters to measure **Essential 8 maturity** across the portfolio through delivery of an aggregate view of the cluster to help support unified and **consistent approaches** for addressing **security challenges**.

splunk>
turn data into doing™

Essential 8 Recipe for Success

Avoid Tick-box Compliance

Avoid compliance for compliance sake and shift to a "culture" of risk management that helps to reduce the compliance burden and add insights and value.

Threat & Risk Landscape

The threat and risk landscape changes impacting ongoing E8 compliance. Real-time monitoring and alerting help identify challenges and prompt action.

Risk-based Approach

Prioritise areas for uplift based on proportional risk and establish target maturities that address organizational requirements.

Compliance Visibility Gaps

Projects typically address initial compliance. Organisational change is a common cause of visibility drift and so continuous monitoring and asset detection is key.

Self-assessment Gaps

Adopting a tried and tested approach to assessments can help avoid inconsistent results, drive accurate, evidence-based and repeatable maturity reviews.

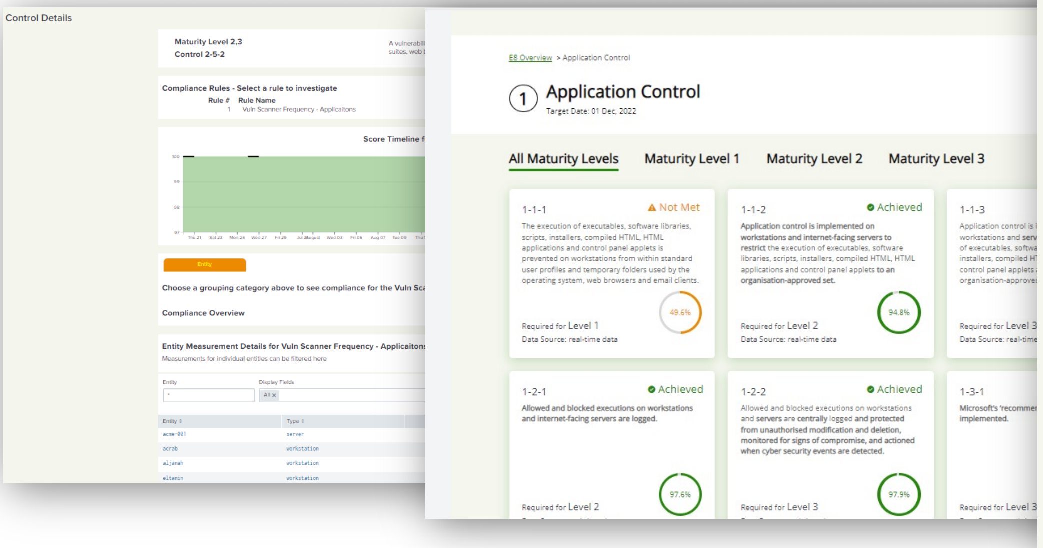
Why Deloitte?

- We have proven experience in advising Clients to effectively mitigate risks and uplift their security maturity.
- We have in-depth experience in delivering business outcomes on the Splunk platform.
- We invest significantly in the development of new and the optimization of existing Splunk apps to drive Splunk maturity.
- In-depth Splunk capability delivering Splunk solutions across both State and Federal Government.

Engagement Approach

Our expert consulting team will guide and apply Essential 8 mitigation strategies to help achieve the identified target state. We will optimize the existing Splunk environment to support maturity uplift and enable continuous monitoring of key systems and applications.

Detailed Assessment Dashboards



Control Details

Maturity Level 2,3
Control 2-5-2

A vulnerabili
suites, web b

Compliance Rules - Select a rule to investigate

Rule #	Rule Name
1	Vuln Scanner Frequency - Applicaitons

Score Timeline f

Entity

Choose a grouping category above to see compliance for the Vuln Sca

Compliance Overview

Entity Measurement Details for Vuln Scanner Frequency - Applicaitons
Measurements for individual entities can be filtered here

Entity: *
Display Fields: All ×

Entity	Type
acme-001	server
acrab	workstation
aljanah	workstation
eltanin	workstation

E8 Overview > Application Control

1 Application Control
Target Date: 01 Dec, 2022

All Maturity Levels | Maturity Level 1 | Maturity Level 2 | Maturity Level 3

1-1-1 — Not Met
The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.
49.6%
Required for Level 1
Data Source: real-time data

1-1-2 — Achieved
Application control is implemented on workstations and internet-facing servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
94.8%
Required for Level 2
Data Source: real-time data

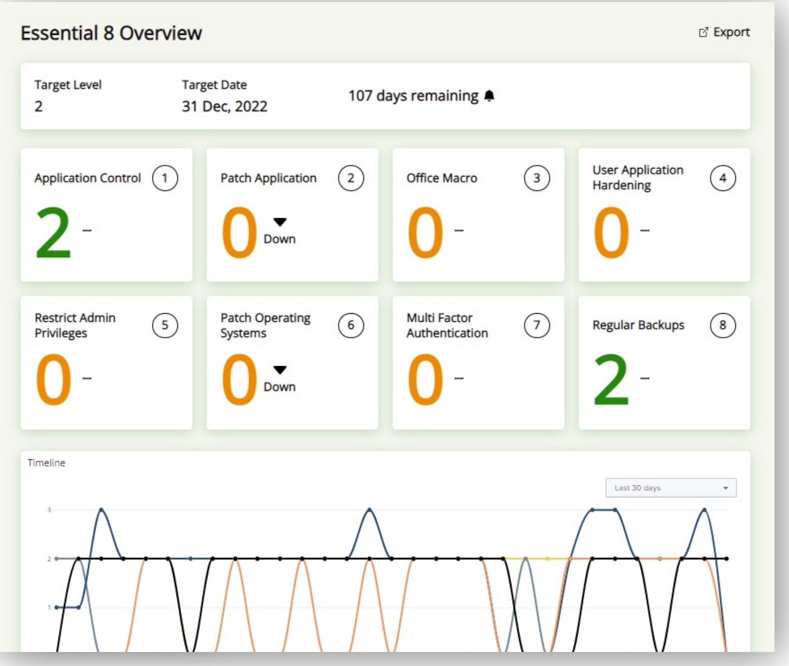
1-1-3
Application control is i
workstations and serv
of executables, softwa
installers, compiled HT
control panel applets a
organisation-approved
Required for Level 3
Data Source: real-time

1-2-1 — Achieved
Allowed and blocked executions on workstations and internet-facing servers are logged.
97.6%
Required for Level 2

1-2-2 — Achieved
Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.
97.9%
Required for Level 3

1-3-1
Microsoft's 'recommen
implemented.
Required for Level 3

Executive Scoring Dashboard



Essential 8 Overview

Export

Target Level: 2
Target Date: 31 Dec, 2022
107 days remaining

Strategy	No.	Level	Trend
Application Control	1	2	-
Patch Application	2	0	▼ Down
Office Macro	3	0	-
User Application Hardening	4	0	-
Restrict Admin Privileges	5	0	-
Patch Operating Systems	6	0	▼ Down
Multi Factor Authentication	7	0	-
Regular Backups	8	2	-

Timeline

Last 30 days

1. Environment Review & Planning

Assess existing Splunk environment and data sources based on E8 requirements. Provide recommendations on health and additional data sources to be onboarded. Provide an **Essential 8 Data Source Maturity Assessment Report** and an Implementation Plan.

2. Data Onboarding & Configuration

Onboard required data sources and map data model to existing data sources. **Deploy the Deloitte Essential 8 app** and configure dashboards. Create alerts and integrate with IT Service Management. Refine & tune solution to meet requirements.

3. Knowledge Transfer & Interpretation

Uplift organisational knowledge of Essential 8 mitigation strategies. Our expert consulting team **will interpret maturity results** and provide a roadmap on ongoing maturity uplift. Enable teams to manage the solution through **Knowledge Transfer Workshops**.

Health Check > Implementation > Handover & Support

Solution Benefits

Continuous Maturity Assessment

Deloitte's Essential 8 solution provides **ongoing assessment** of each of the 8 mitigation strategies, underpinned by real-time dashboards and reports to support organisational maturity uplift.

Alerting

In-depth alerting enables **proactive management** of changes to the environment to effectively maintain and improve Essential 8 maturity.

Leverage Existing Splunk Investment

The Deloitte app is built on your **existing Splunk environment,** with no requirements for new technology investment or additional skillset to achieve the outcome.

Reduce Manual Assessments

Integrate self assessment with continuous monitoring to effectively close the gap in existing approaches.

Optimise Splunk Platform

Essential 8 data sources will support **broader adoption** of Security and IT Operations use cases providing additional value out of the existing Splunk investment.

Key Contacts

Aby Olival
Cyber Analytics
Director, Risk Advisory
aolival@deloitte.com.au
0479 194 771

Matt Burgess
Cyber Analytics, Federal
Senior Manager, Risk Advisory
mburgess@deloitte.com.au
0473 995 168

Stuart Hirst
Cyber Analytics
Partner, Risk Advisory
shirst@deloitte.com.au
0487 471 729