White Paper

Essential Eight ASD Security Controls

The Missing Ninth Step

Huntsman®
Defence-Grade Security Intelligence

Essential Eight ASD Security Controls

The Missing Ninth Step

The Australian Signals Directorate's (ASD's) publication of the Essential Eight shows organisations how to defend against most cyber threats. These are the key controls ASD encourage organisations to employ to help protect against cyber-attack.

Yet there's one critical security control that's missing that provides the visibility and measurement of the status and efficacy of the other eight – and it's called **Protective Monitoring**.

The Australian Signals Directorate (ASD) has, for some time, extoled the virtues of four critical security controls that serve to defend businesses throughout Australia. With proper implementation of these four security controls, organisations can successfully defend against 85% of cyber-attacks. Recently, ASD's doctrine has been updated to augment the Top 4 with four additional controls, now pitched as the 'Essential Eight'.

https://www.asd.gov.au/publications/protect/Essential_Eight_Explained.pdf

> "The advantage of this guidance is that it is customisable to each organisation based on their risk profile and the threats they are most concerned about."

The Necessary Nine

Huntsman®

Protective Monitoring

This is a term that was initially coined by the UK government's cyber security division, CESG (now NCSC) which was part of GCHQ, an organisation in many ways equivalent to Australia's ASD.

CESG published a good practice guide called GPG 13 (now superseded) which details how organisations should establish protective monitoring at the heart of their security operations for the purposes of ICT system oversight. Protective monitoring solutions require investment in a Security Information & Event Management Solution (SIEM), the most effective of which act as a central log storage and indexing system, with advanced analytics capabilities that can mine and correlate the data looking for threats across the ICT environment.

Read more about the UK Government's latest guidance at:
https://www.ncsc.gov.uk/topics/monitoring
https://www.ncsc.gov.uk/guidance/introduction-security-monitoring
https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide

Ask any seasoned security professional and they'll tell you that it doesn't matter how many controls you throw at the problem, there will always be gaps in your defences. That's because too many controls can be so restrictive as to disrupt the business and hinder users getting their jobs done, so there needs to be a balance. The Essential Eight introduces four new security controls into the fundamental cyber strategies for mitigating modern cyber-attacks. These eight controls are a subset of a wider set of controls provided by ASD for the Australian Government. ASD's publication, "Strategies to Mitigate Cyber Security Incidents" https://www.asd.gov.au/publications/Mitigation_Strategies_2017.pdf, includes a complete list of the security controls to help build a resilient defence against cyber attackers.

Protective Monitoring – Plugging the Ninth Hole

Even when implemented in the suggested order the Essential Eight mitigation strategies are no guarantee of cyber incident prevention. ASD's recommendations do, however, provide a sound baseline for organisations to implement a good foundation that should help prevent cyber-attacks.

Protective monitoring provides the metrics and enterprise-wide oversight necessary to establish and maintain good cyber defences across your business. Implemented properly, protective monitoring provides continuous cyber security situational awareness and is equally important in detecting cyber-attacks that may have circumvented your other defences.

Situational Awareness

The United States Army defines situational awareness as, "Knowledge and understanding of the current situation which promotes timely, relevant and accurate assessment of friendly, enemy and other operations within the battle space in order to facilitate decision making."

Taking this definition and applying it to modern businesses, cyber security situational awareness is the capability of continually knowing what your systems are doing, who is accessing what, which information assets are being communicated over your network and what systems are being accessed and by whom. Security operations teams can achieve this level of awareness by monitoring system event logs and collecting log feeds from directories, network devices and security devices which, when aggregated together, allow operations analysts to make sense of the data, to look for indicators of compromise and to act to mitigate threats.

Protective monitoring gives security analysts the visibility they need to deal with security events and control statuses, while continually updating risk and compliance reporting as part of the threat detection, investigation and response process. The latest generation of monitoring and response technologies can significantly impact operational workflows to reduce the time between detecting a threat and response. Through the use of machine learning and automation technologies, protective monitoring now helps shortens the time at risk for any organisation.

Furthermore, in addition to threat identification, a properly implemented protective monitoring service helps the security operations team hunt for unusual activities that could indicate misuse; monitoring to compare current events with a dynamic baseline of recent activity or retrospectively look across a previous time interval increases analysts' detection sensitivity to anomalous activity. These current and historical investigations can deliver critical intelligence about the persistence and severity of the threat and how best to manage and contain it.

Is Protective Monitoring Right for your Business?

Implementing a cyber security strategy based on ASD's Essential Eight should include protective monitoring. This will ensure that you can develop metrics, interpret the controls, and refine your governance to better support the operational needs of your enterprise.

For example, say a user starts sending many emails to their private email address from the corporate email system. This kind of usage may be allowed, but by correlating this behaviour with other internally (or externally) sourced information about the user and the transactions, the protective monitoring solution can flag inappropriate activity – sensitive information being exfiltrated. None of the Essential Eight controls would have prevented this sort of insider misuse, but carefully implemented protective monitoring capabilities can help spot the anomaly, raise an alert and improve governance going forward.

Data Breach Notification – A Compelling Case for Protective Monitoring?

With the introduction of data breach notification into Australian law in February 2018, there will now be compliance obligations on most organisations, in line with the Australian Privacy Principles (APPs), to protect personal information. The implementation of the Essential Eight will become increasingly important as a means protecting that data. In reviewing the principles it becomes clear that it's not so much about how you protect the information, but knowing how it's being used:

- The open and transparent management of personal information including having a privacy policy
- An individual having the option of transacting anonymously or using a pseudonym where practicable
- The collection of solicited personal information and receipt of unsolicited personal information including giving notice about collection
- How personal information can be used and disclosed (including overseas)
- Maintaining the quality of personal information
- Keeping personal information secure
- Right for individuals to access and correct their personal information

Again, protective monitoring will help you keep tabs at all times on how your information is being accessed and to whom it is being disseminated. It will enable the quick identification, investigation and resolution of unsatisfactory system/user activity and reduce the prospect of heavy financial penalties as a result of a data breach and uncontrolled compliance.

Implementing Security Controls

Even in the absence of regulatory "must haves", how do you know when your systems and information are as safe as they can be? How do you decide which controls are most important and working for you?

How do you decide which controls are most important and working for you? It's best to consider each control as a separate risk mitigation strategy. That way you make sure you have assessed the value of the assets you are protecting (based on the impact of compromise), determined the competency of the threat actors you are defending against and uncovered the vulnerabilities you are trying to patch with the controls. Like any risk calculation, it is only when the value of your security investment exceeds the risks of not putting them in that you see the overall benefit to your business.

Expert advice is recommended to truly assist in any cyber risk assessment, but organisations should consider several attributes when putting cyber defences in context:

- **Categorise Information** – Especially important, sensitive or information that is time sensitive, highly personal, financially attractive and frequently accessed;
- **Establish likely threats** – This can include cyber criminals and fraudsters, nation states with a political or economic motive, activists, adversaries as well as malicious insiders; and
- **Implement appropriate protection levels** – The effective deployment and management of the Essential Eight forms a baseline upon which additional controls can be added depending on your risk assessment. These might include, amongst others, fraud prevention, encryption of sensitive data or the filtering of network traffic.

Conclusion

The Essential Eight is an important source of information about security strategies and controls. ASD publishes some of the best cyber security advice available on the Internet.

Importantly however, both the Centre for Internet Security (CIS) Critical Security Controls in the US and the CESG Top 10 prioritise the importance of protective monitoring as a critical component of measuring and managing security controls.

Irrespective whether it's the top 20, 10 or 8 controls, CIOs need to recognise that a properly implemented protective monitoring strategy will enable continuous visibility of the security controls, measurement of their performance and ultimately the management of their improvement.

Author: Jason Legge

Head of Security Consulting, Huntsman Security

Jason works directly with customers, Huntsman's channel partners and internal teams to provide solutions to cutting-edge cyber security challenges. Jason's extensive experience in the areas of security threat analytics and incident response means he is well aware of the demands faced by analysts in quickly and accurately resolving cyber threats. Before joining Huntsman, Jason headed up the High Security Operations Centre for a UK government agency for six years. During that time, he advised business leaders, security accreditors and IT operations managers and analysts at a national level on IT and cyber defence threat mitigation strategies and SOC design and operation.

Jason may be contacted at
jlegge@huntsmansecurity.com

Please visit the Huntsman Resources page at
https://www.huntsmansecurity.com/resources/
for White Papers, Compliance Guides, Solution Briefs and Product Brochures.

Huntsman®

HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC
t: **+61 2 9419 3200**
e: **info@huntsmansecurity.com**
Level 2, 11 Help Street
Chatswood NSW 2067

EMEA
t: **+44 845 222 2010**
e: **ukinfo@huntsmansecurity.com**
7-10 Adam Street, Strand
London WC2N 6AA

NORTH ASIA
t: **+81 3 5809 3188**
e: **info@huntsmansecurity.com**
TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

AMERICAS
toll free: **1-415-655-6807**
e: **usinfo@huntsmansecurity.com**
Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman