bluechip infotech

ManageEngine

ASD Strategies To Mitigate Cyber Security Incidents

How ManageEngine solutions can help implement ASD strategies to mitigate Cyber Security incidents.

Distributed by:

Bluechip Infotech
ManageEngine Team

Email:
manageengine@bluechipit.com.au

Product Specialist:
Arjun Patel

Phone:
0421 908 910

How ManageEngine solutions can help implement ASD strategies to mitigate cyber security incidents

One of the most important points to understand in today's security landscape is that attack mitigation goes beyond just having preventive security solutions. Attacks can stem from many fronts, and security teams need the right set of tools to ensure their enterprise is secure. The ASD (Australian Signals Directorate) has prescribed a set of strategies to mitigate cyber security incidents. **ManageEngine** provides a suite of cutting edge tools that can help an organization implement some of the mitigation strategies as prescribed by the ASD.

ManageEngine solutions featured in this document:

- **Log360:** A comprehensive SIEM solution for mitigating both external and internal threats.
- **AD360:** The ideal integrated solution for Active Directory administrators that has different components which takes care of:
    - Active Directory management and reporting - ADManager Plus
    - End-user password management for Active Directory - ADSelfService Plus
    - Real-time Active Directory change auditing and alerting - ADAudit Plus
    - Backup and restoration of domain controllers and virtual machines – Recovery Manager Plus
    - Exchange server reporting, auditing, and monitoring - Exchange Reporter Plus

Mitigation strategies to limit the extent of cyber security incidents

1. "**Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing."

- With **ADManager Plus,** you can easily provide different levels of permissions to users to access or perform operations on any Active Directory object. You can also ensure that there is no privilege misuse by validating privileges using the predefined report for group membership.
- With **ADAudit Plus**, you can monitor the user activity of privileged accounts with real time reports for security groups.

2. "**Disable local administrator accounts** or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials."

- **ADManager Plus** helps administrators to easily manage and disable Active Directory accounts. Our free tool can be used for managing Windows local users.
- **ADSelfService Plus** helps administrators assign passwords 'that are random and unique for each computer's local administrator account'. With its granular password policy enforcer, the solution ensures that end-users set strong passwords,

    - With a minimum length criteria
    - That contain both upper and lower cases along with special characters and numbers
    - That are not dictionary words, or common patterns that are easy to crack.

Mitigation strategies to detect cyber security incidents and respond

1. "**Continuous incident detection and response** with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access and network activity."

- **Log360** automates the log management process for enterprises by collecting and analyzing log data from every resource in your network including servers, domain controllers, network perimeter devices such as routers, switches, firewalls, IDS/IPS, and business critical applications such as databases and web servers. The solution provides in-depth auditing and alerting for security threats and file/folder access. With its built-in incident management console, every incident can be automatically raised as a ticket in a centralized ticketing tool (ManageEngine ServiceDesk Plus or ServiceNow) to ensure accountability to incident detection and response.

2. "**Hunt to discover incidents** based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analyzed threat data with context enabling mitigation action, not just indicators of compromise."

- **Log360** has an augmented threat intelligence platform that comes with a built-in STIX/TAXII feeds processor and global IP threat database which includes 600+ million blacklisted IP addresses identified from trusted open sources).The solution correlates

the log data from within the network with these threat feeds to instantly detect and alert in real time for any malicious traffic interacting with your network and for outbound connections to malicious domains and callback servers.

Mitigation strategies to recover data and system availability

1. **"System recovery capabilities** e.g. virtualisation with snapshot backups, remotely installing operating
systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts.“

- **Recovery Manager Plus** is the ideal enterprise backup tool for easy backup and restoration of Active Directory, domain controllers and virtual machines. In the event of downtime, you will be in a position to perform a granular restoration to get your domain controllers and virtual machines up and running again.

Mitigation strategy specific to preventing malicious insiders

1. "**Personnel management** e.g. ongoing vetting especially for users with privileged access, immediately disable all accounts of departing users, and remind users of their security obligations and penalties.“

- **ADAudit Plus** can help with the ongoing vetting for users with privileged access. You can comprehensively track privileged accesses, monitor actions performed by privileged users and be alerted in real time for ones that can jeopardize your security with predefined reports and alert profiles for administrative user actions.

- **ADManager Plus** can be used to easily disable accounts (including mailbox, O365 accounts etc.) for departing users. The tool has in-depth features to perform administrative tasks related to a user departing or changing department. You can perform a thorough clean up of your Active Directory accounts by easily identifying user and computer accounts that have not logged on for a certain number of days and carry out operations such as deleting account permanently, moving the user into a different OU, or disabling the user account.