BLUE LANCE

LT Auditor+

Best Practice Panels

BLUE LANCE

Table of Contents

BLUE LANCE

Overview

The LT Auditor+ Best Practices Panels are a set of panels that highlight network activity captured with LT Auditor+, encapsulated into intelligent, easy to use portals that assist organizations with improving Cybersecurity practices and hygiene.

LT Auditor+ Best Practices Panels consists of the following categories each with panels or tabs containing specific visuals that display and disseminate valuable information required to improve an organization's security posture.

1. Logon Activity
2. Active Directory Hygiene
3. Active Directory Activity
4. Group Membership
5. LT Auditor+ Status

The data source for information in these panels is the production LT Auditor+ database. The LT Auditor+ database is populated using the following products:

1. LT Auditor+ Suite that collects information on Active Directory, Group Policies, Logons, File Activity from Windows servers, SANs and NAS devices, USB devices and Workstations.
2. LT Auditor+ Assessment that scans Active Directory and File Systems for data on Users, Groups, Organizational Units, Computers, Permissions and Trustees.
3. LT Auditor+ Syslog Server that receives data from any Syslog Enabled Device.

LT Auditor+ Best Practices Panels are created in Power BI and a Power BI Pro or Premium license is required to view and share this information. Licensing and additional information on configuring Power BI with the LT Auditor+ database is provided in the LT Auditor+ Power BI Configuration guide.

The following sections describe the purpose of each panel and provides information on all the visuals.

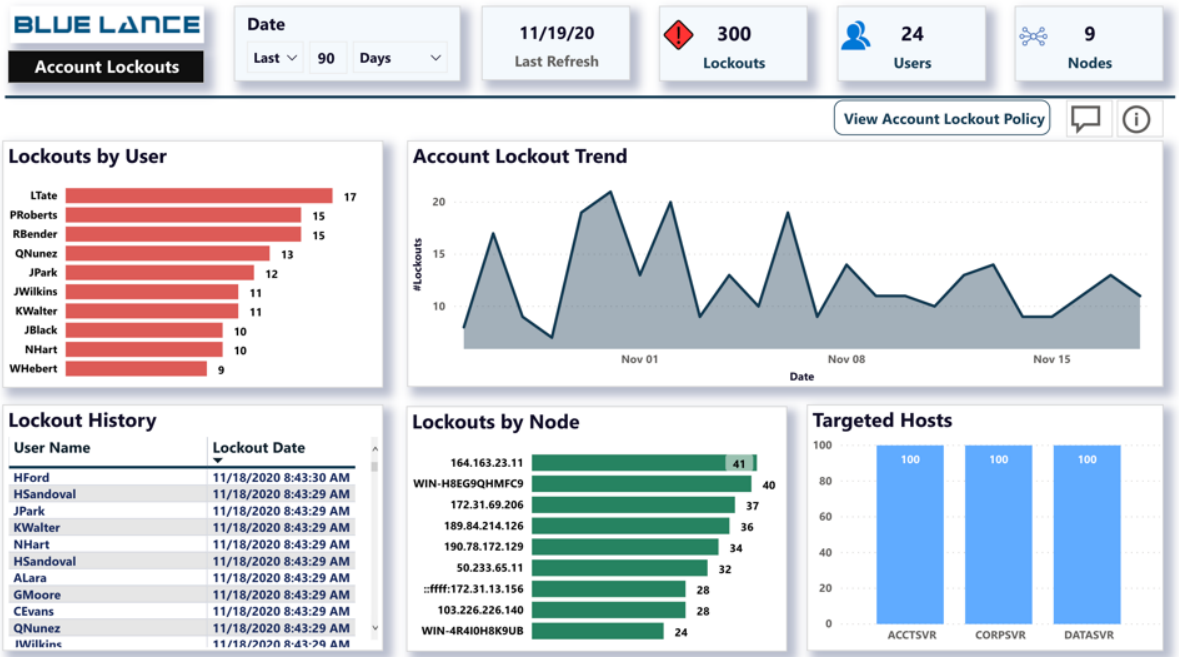
Logon Activity

Logon Activity displays data that tracks logon activity in the organization. Details of each of the panels and visuals in this category are described below:

Lockouts

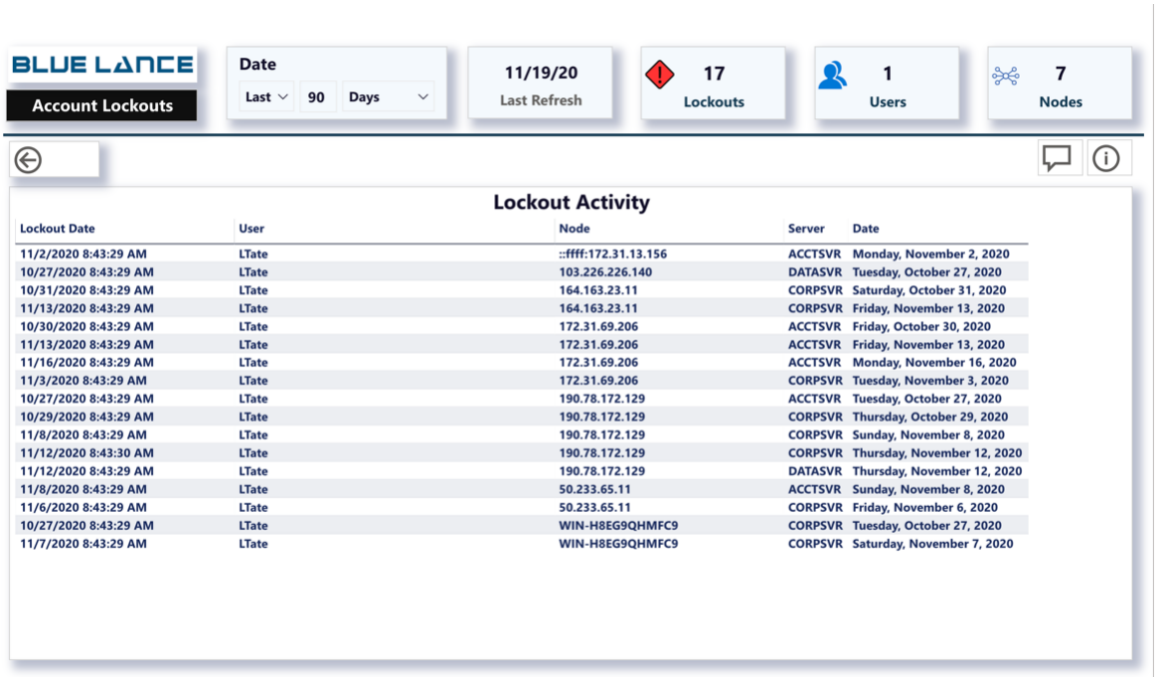
Account Lockouts can happen for a variety reasons, however from an organizational standpoint they are disruptive and costly. With the Lockouts Panel administrators or security personnel can quickly analyze lockout activity by:

- Identifying the source machine where lockouts are occurring for quick remediation.
- Finding users with the most lockout activity and facilitate training to reduce downtime.
- Investigating suspicious lockout activity based on number of incidents and location.
- Providing data to discuss review of the organization's Account Lockout policy based on the patterns of lockout activity.



Lockout Panel Visuals

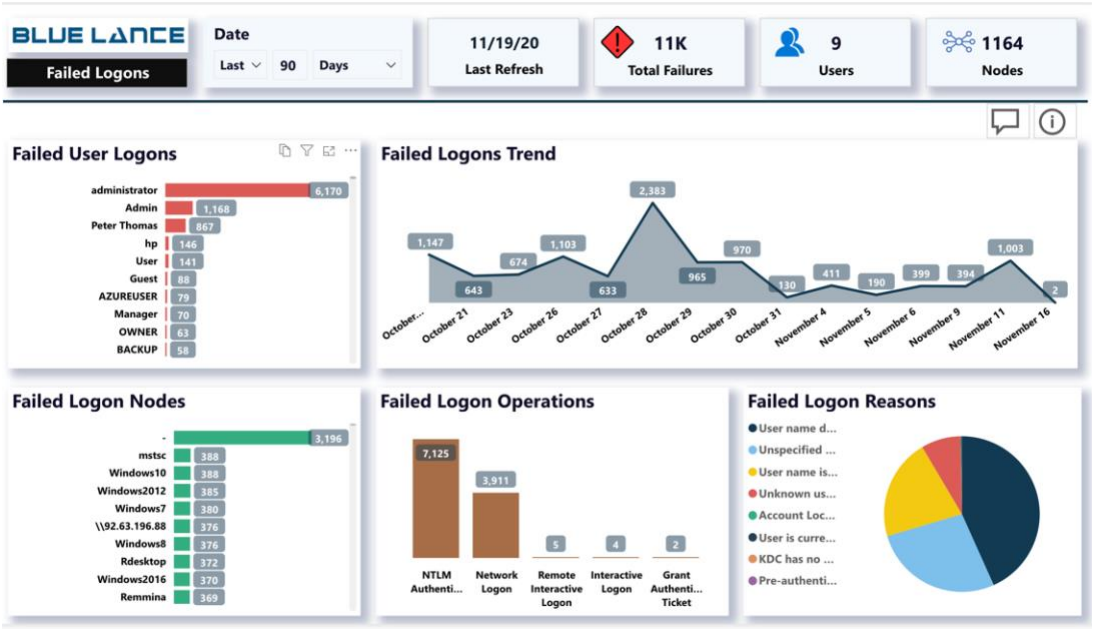
Panel	Description
Lockouts by User	Bar chart of users locked out for specified time frame. Click on a user to view history and IP addresses where lockouts occurred. Right-click on user and drill down to 'Lockout Activity' to view a report that can be downloaded or emailed as shown below.
Account Lockout trend	Graph indicating trend of lockout incidents for specified time frame. Click on a peak to view what caused the peak.
Lockout History	Table of accounts that have had lockouts with dates of each lockout.
Lockouts by Node	Number of lockouts from a given source IP address.
Targeted Hosts	Hosts where lockouts have occurred.



Failed Logons

A large number of failed logon attempts occurring within a certain period of time could be an indication of a security threat. The Failed Logons Panel provides critical information identifying all logon failures and provides important information to:

- Identify users and nodes where very large number of failures occurred.
- Show trendlines over time to help investigate security incidents if a pattern of attack is identified.
- Displays clear reasons for logon failures.



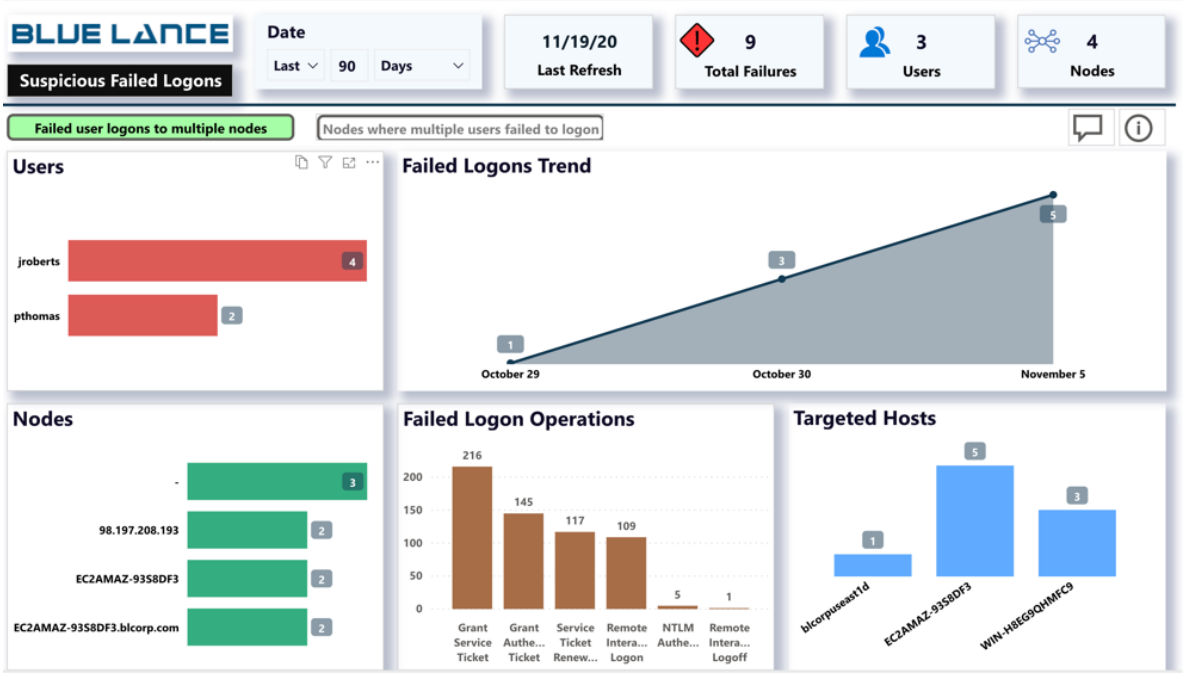
Failed Logons Panel Visuals

Panel	Description
Failed User Logons	Bar chart of failed logon users for specified time frame. Click on a user to view where failure occurred, reasons for failure and target hosts. Right-click on a user and drill down to 'Details' to view a detailed report that can be downloaded or emailed
Failed Logons Trend	Graph indicating trend of failed logon activity for specified time frame. Click on a peak to view what caused the peak.
Failed Logon Nodes	Number of logon failures from a source IP address. This is where logon failures are occurring.
Logon Operations	Displays the types of logon events that caused failures.
Logons Failure Reasons	Displays the reasons for logon failures.

Suspicious Failed Logons

Multiple failed logins from a single user to different nodes or machines is an extremely suspicious pattern of activity that might indicate a malware infection. This could be a situation where malware on an infected host machine is attempting to move laterally within an organization.

The Suspicious Failed Logons Panel displays all failed logons of valid users that have attempted access to multiple nodes in the organization allowing investigators to quickly pinpoint machines that may have malware.



Each of the visuals allows for drilling down to a detailed report.

Suspicious Failed Logons Panel Visuals

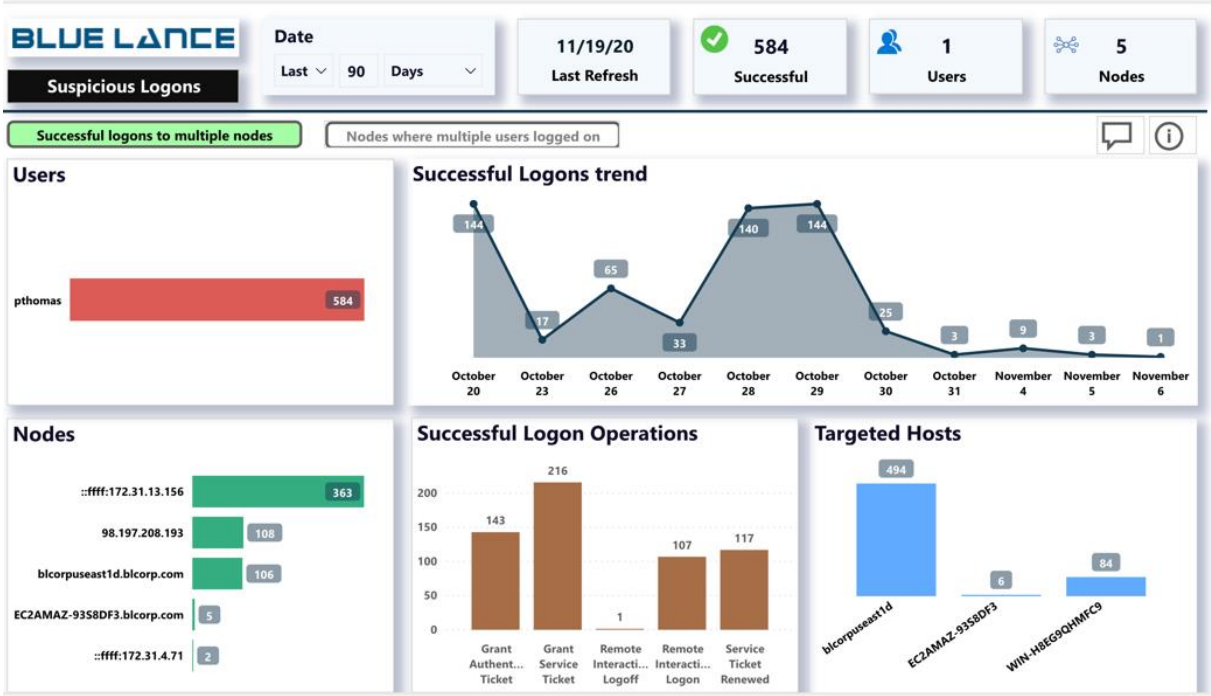
Panel	Description
Users	Bar chart of valid failed logon users that have recorded logon failures for multiple nodes within the specified time frame. Click on a user to view nodes where failure occurred and target hosts. Right-click on a user and drill down to 'Details' to view a detailed report that can be downloaded or emailed
Failed Logons Trend	Graph indicating trend of failed logon activity for specified time frame.
Nodes	Nodes where failed occurred.
Failed Logon Operations	Displays the types of logon events that caused failures.

Targeted Hosts	Hosts where failed logins were attempted.

Suspicious Logons

Multiple successful logons from a single user to different nodes or machines is another extremely suspicious pattern of activity that might indicate a malware infection. This could be a situation where malware on an infected host machine is successfully got the right user credentials is moving laterally within an organization.

The Suspicious Logons Panel displays all successful logons to multiple nodes in the organization allowing investigators to quickly pinpoint machines that may have been infested.



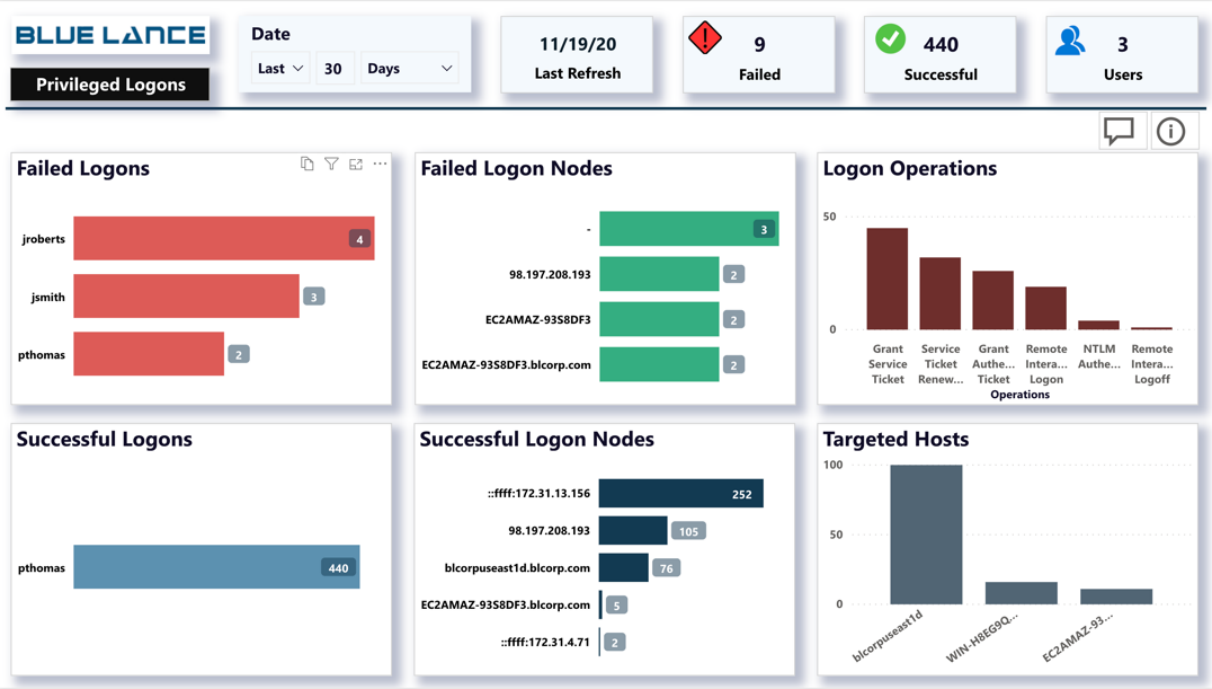
Suspicious Logons Panel Visuals

Panel	Description
Users	Bar chart of users with successful logons to multiple nodes within the specified time frame. Click on a user to view nodes where logons occurred. Right-click on a user and drill down to 'Details' to view a detailed report.
Successful Logons Trend	Graph indicating trend of successful logon activity for specified time frame. Click on a peak to view what caused the peak.
Nodes	Nodes where logons occurred.
Successful Logon Operations	Displays the types of logon events users to connect.
Targeted Hosts	Hosts where successful logons succeeded. \

Privileged User Logons

Privileged users have access to most critical resources in an organization. The prime objective of most attackers is to compromise a privileged account to either exfiltrate information or hijack an organization with ransomware demands. Tracking privileged user activity is a critical part of any organization's security footprint and important for compliance and governance.

The Privileged Users Logons Panel tracks all successful and unsuccessful logon activity for privileged users in the organization.



Privileged User Logons Panel Visuals

Panel	Description
Failed Logons	Bar chart of failed privileged users' logons within the specified time frame. Click on a user to view nodes where logons occurred. Right-click on a user and drill down to 'Details' to view a detailed report that can be downloaded or emailed.
Failed Logon Nodes	Nodes where privileged failed logons occurred.
Logon Operations	Displays the types of logon events for all privileged successes and failures.
Successful Logons	Bar chart of successful privileged users' logons within the specified time frame. Click on a user to view nodes where logons occurred.

Successful Logon Nodes	Nodes where privileged successful logons occurred.
Targeted Hosts	Hosts where all privileged logon activity occurred.

Active Directory Hygiene

Active Directory is the backbone of most organizations worldwide that governs access to resources and assets. Maintaining Active Directory hygiene ensures a reduced attack surface resulting in significantly lowering the probability of security breaches, data exfiltration and exploitation.

The Active Directory Hygiene panels display a set of key metrics that an organization must monitor to keep the system healthy and resilient against Cybersecurity attacks.

User Accounts

User Accounts Panel is set of hygiene metrics for all active users on the network.

Details on the metric can be derived by clicking the report icon.

User Accounts Panel Visuals

Panel	Description
Dormant Privileged Accounts	Active privileged accounts that have been dormant is a serious security hygiene issue. An organization can be severely impacted if such accounts are compromised. Click on the report to view dormant privileged users and provide that information to an Administrator for remediation.
Password Never Expiring Accounts	These accounts do not have the requirement to change their passwords. This is a serious concern as they bypass organizational password policies. Such accounts are susceptible to password cracking since a hacker has theoretically unlimited time to do so.
Password Not Required Accounts	These accounts can be logged into without a password. This a very serious deviation from standard security practices since a compromised account gets automatic access to the organization.
Password Change Not Allowed	These accounts cannot have their password changed by the user. Passwords left unchanged gives more time to attackers to crack them.
Dormant Accounts	Active accounts that have had no logon activity for a defined stale period (Default is 90 days). These accounts must be disabled to reduce avenues of attack.
Never Logged on Accounts	Accounts with no logon activity since creation. These accounts though never used can still exist as a point of entry into the system for attackers

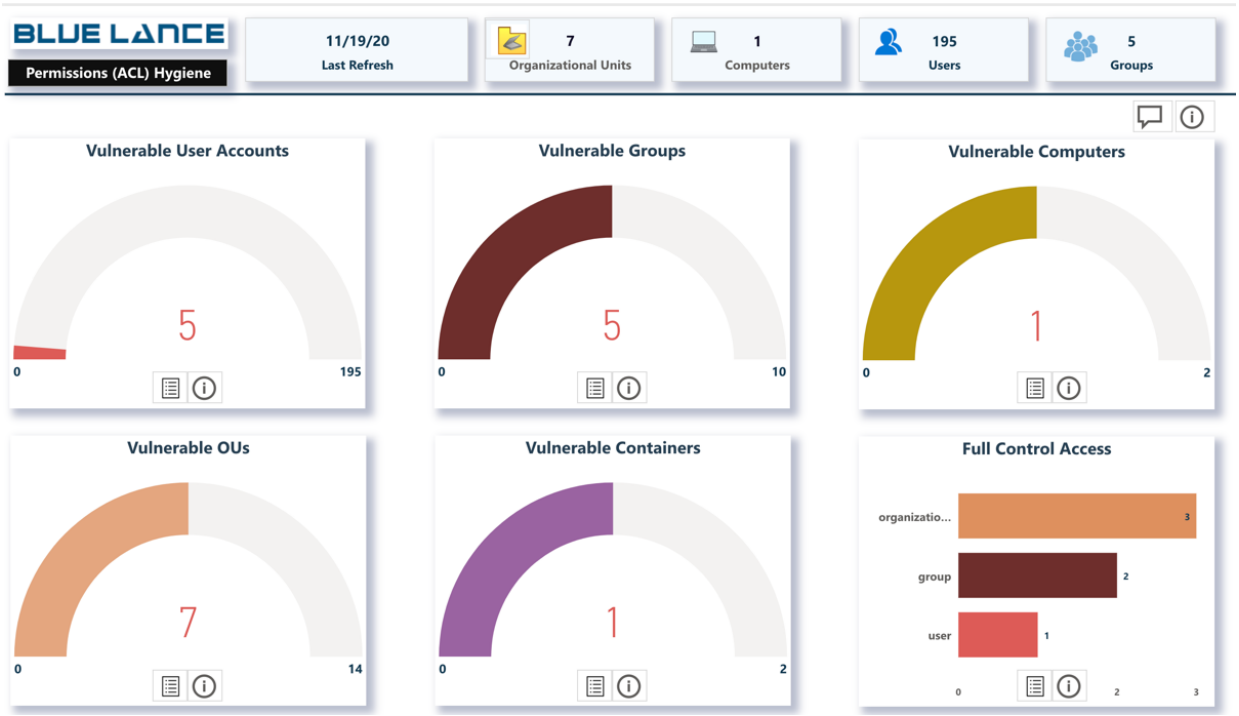
Note: The dormancy period required to classify an account as dormant defaults to 90 days. This value can be changed in the Power BI Parameter section.

Permissions (ACLs)

Active Directory ACL's (Access Control Lists) represent access control on all objects (Users, Groups, OU's, Computers) within the directory. Discretionary access control (DACLS) defines trustees or principals granted access to an object. The LT Auditor+ Best Practices Permissions (ACLs) Panel are a set metrics that identifies DACLs that could potentially be exploited by an attacker.

Permission (ACLs) hygiene metrics look for the following DACL assignments:

- **GenericAll** - full rights to the object (add users to a group or reset user's password)
- **GenericWrite** - update object's attributes (Example: logon script)
- **WriteOwner** - change object owner to attacker-controlled user take over the object
- **WriteDACL** - modify object's ACEs and give attacker full control right over the object
- **AllExtendedRights** - ability to add user to a group or reset password
- **ForceChangePassword** - ability to change user's password
- **Self (Self-Membership)** - ability to add yourself to a group



Clicking the report icon on the visual will bring a detailed report.

Permissions (ACLs) Panel Visuals

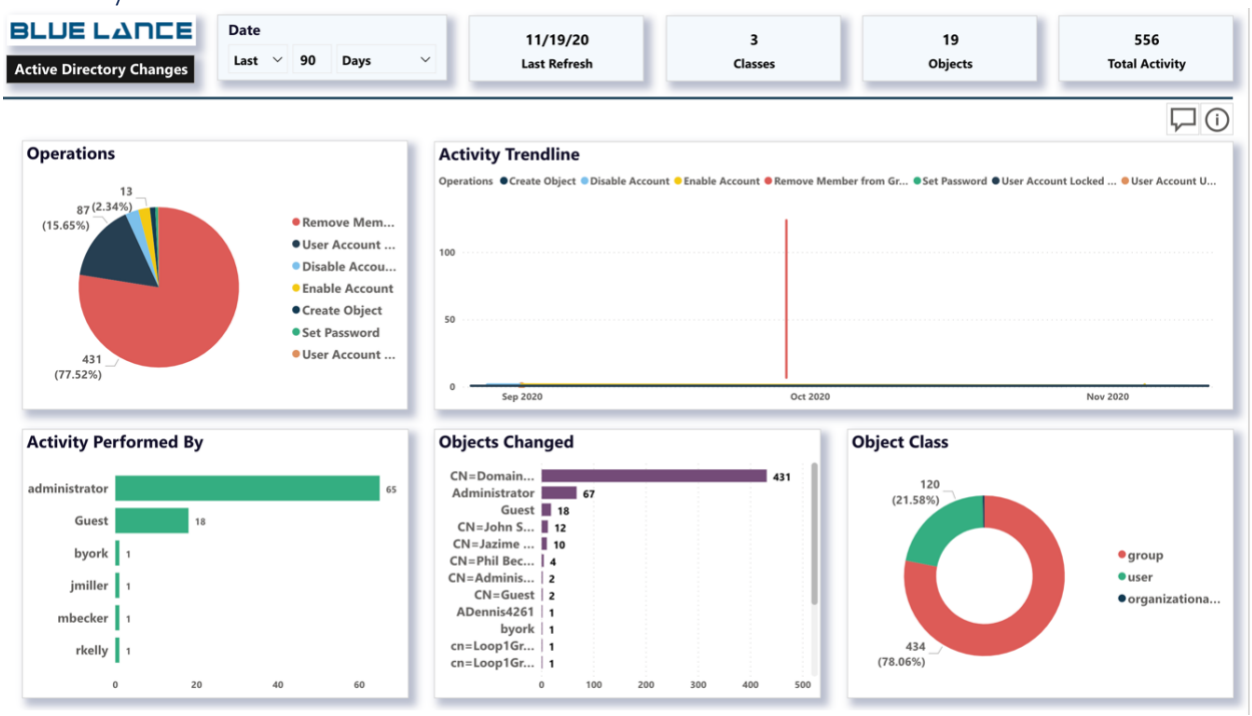
Panel	Description
Vulnerable User Accounts	Principals or Trustees of these user accounts have the ability to reset the user account password and gain access.
Vulnerable Groups	Principals or Trustees of these Groups have the ability to add members to the Group. This can be very dangerous if the Group has powerful privileges or has access to sensitive information.
Vulnerable Computers	Trustees could gain code execution with elevated privileges on a computer they have WRITE privilege on that computer's AD object. If a trustee account gets compromised the attacker could take over this computer to gain access.
Vulnerable OUs	List all Principals with full rights to the OU (Organizational Unit) and all objects contained in it. Care should be taken to ensure access rights given are needed and that there are no violations of the principal of 'Least Privileges'.
Vulnerable Containers	List all Principals with full rights to Container and all objects contained in it. Care should be taken to ensure access rights given are needed and that there are no violations of the principal of 'Least Privileges'.
Full Control Access	List all objects with Principals that have full rights to Active Directory objects. The report can be used to ensure unnecessary rights have not been granted.

Active Directory Activity

Monitoring and keep track of changes in Active Directory is another core element in reducing the probability of security breaches, data exfiltration and exploitation.

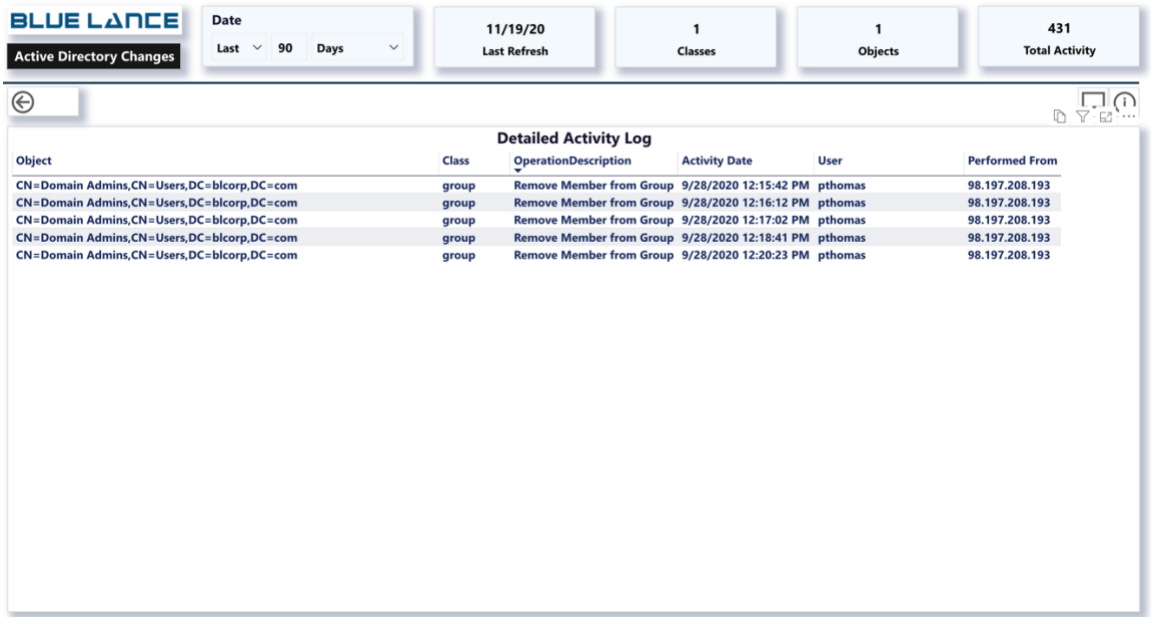
The LT Auditor+ Best Practices Active Directory Activity panel displays key Active Directory changes that have occurred allowing for quick analysis and investigation. The panel also provide a set of key metrics on Privilege Escalations. Security Administrators must investigate events associated with user privilege escalation to ensure that escalation complies with organizational security policies. Additionally, attackers always look to escalate privileges so as to gain a foothold in the organization. This panel is a vital tool to discover and validate whether such activity is legitimate.

Summary Panel Visuals



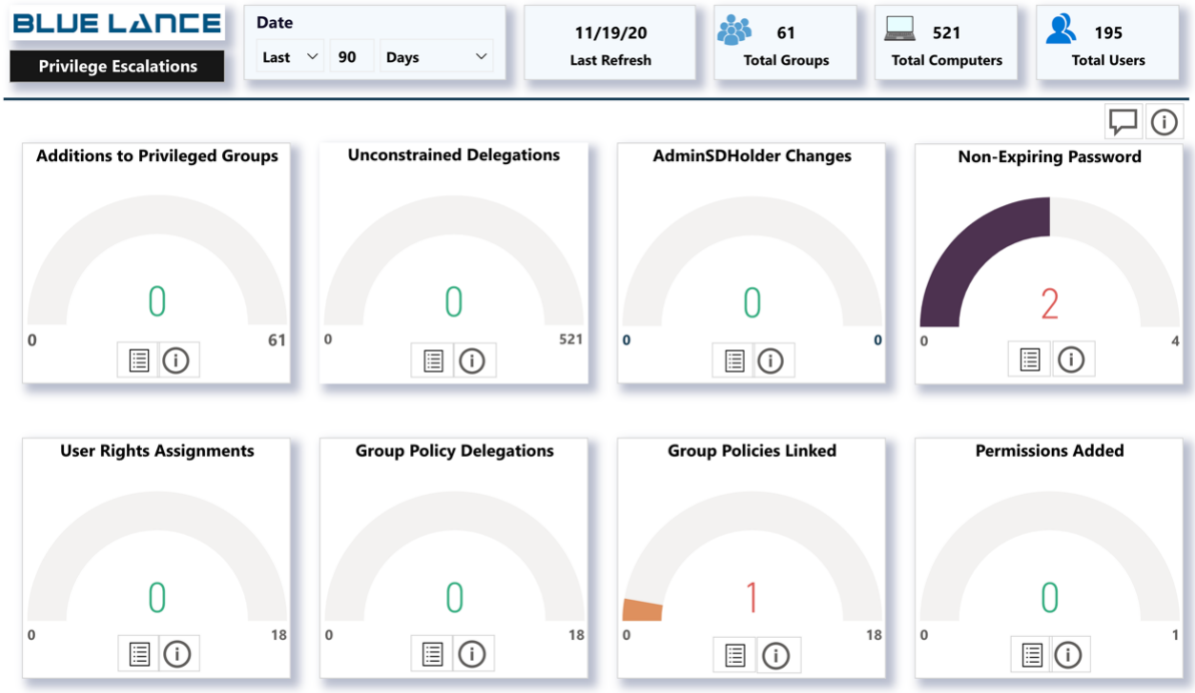
Summary Panel Visuals

Panel	Description
Operations	Pie chart of all Active Directory operations captured with LT Auditor+ for specified time period. Clicking on a specific operation will update the Panel with all activity for that specific operation. Right-click and click 'Details' to view a detailed report for specified operation as shown below.
Activity Trendline	Trend line of activity occurring over specified time frame.
Activity Performed By	Bar chart of Users performing Active Directory activity. Right-click->Details to view report on user activity.
Objects Changed	Chart of Active Directory objects changed.
Object Class	Class of objects changed.



Privilege Escalations

The Privilege Escalations sub visual contains 8 metrics that indicate enhanced rights and access within the Active Directory infrastructure. The ideal scenario would be to 0. In the event any metric displays a positive number, details of the escalation can be viewed by clicking the report icon on the metric.



Details on each of the metrics are provided in the table below.

Privilege Escalations Panel Visuals

Panel	Description
Addition to Privileged Groups	Users added to groups with enhanced privileges such as Administrators, Domain Admins or Enterprise Admins. Extreme caution must be taken when adding users to these groups as they full rights to resources in the directory.
Unconstrained Delegations	Unconstrained delegations give authority to a server allowing it to act on behalf of a client with other remote systems in an environment. This form of impersonation is a security risk because a compromised client can use an unconstrained server to get other servers or resources in the environment to perform tasks on the client's behalf.

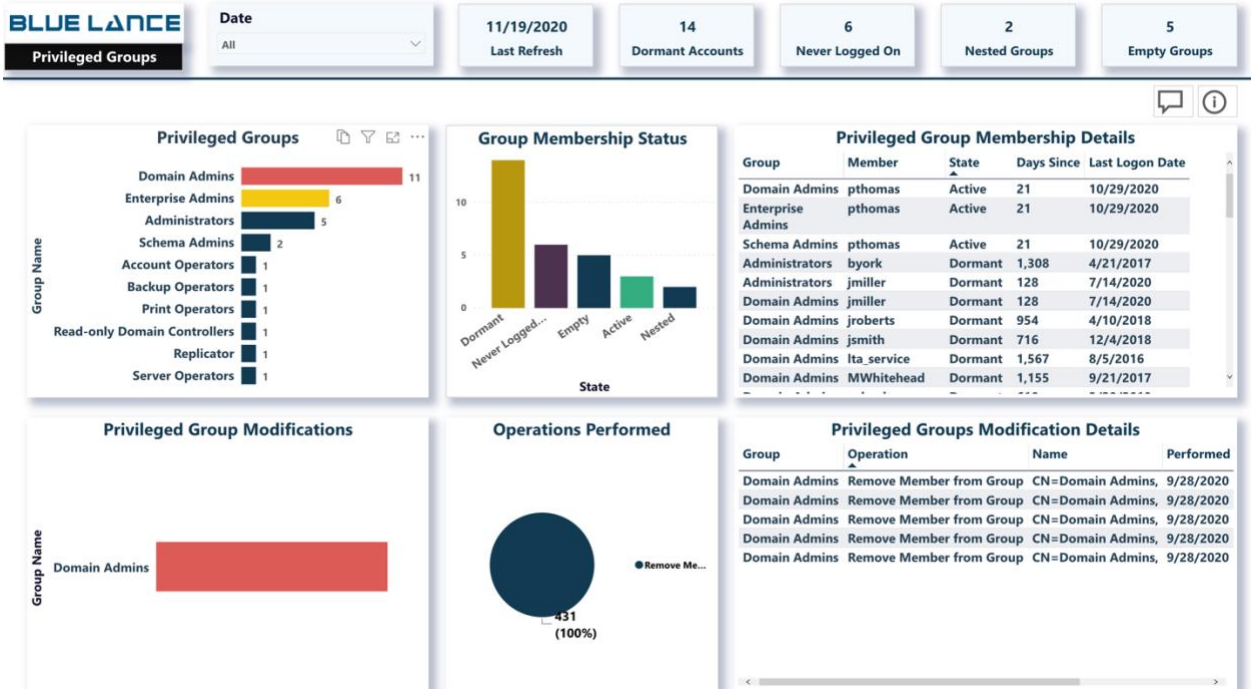
AdminSDHolder changes	The Active Directory AdminSDHolder object manages the access control lists of members of built-in privileged Active Directory groups. All changes to permissions (ACLs), on this object, must be monitored to detect manipulation. Such changes could give attackers access to privileged accounts within the domain.
Non-Expiring Password	Configuring a user account to have a password that never expires is a security risk for the organization. These accounts are not required to adhere to the organization's password policies and could have very weak passwords.
User Rights Assignment	User rights assignments are settings applied to the local devices on the network. They allow users to perform various system tasks, such as local logon, remote logon, backups, debug programs, impersonate a client etc. These rights can escalate privileges and need to be monitored.
Group Policy Delegations	Group Policy Delegations delegate rights to other users which could mean escalation of rights. These delegations must be monitored to ensure that these assignments are not a mistake or malicious.
Group Policies Linked	Linking a Group Policy to an OU activates rights to objects within the OU. This operation must be monitored to ensure that linking is not a mistake or malicious.
Permissions Added	Provides a listing of all ACL changed that occurred for specified time frame.

Group Membership

The Group Membership panel provides information on all Active Directory Groups and Group Members. This panel can be used to identify nested groups and status of members that will help administrators with Group Membership hygiene.

Privileged Groups

The Privileged Groups sub panel displays information on all privileged group members. By default, privileged members are protected groups in Active Directory, however other important groups can be included into this list if required.



Privileged Groups Panel Visuals

Panel	Description
Privileged Groups	Pie chart of all Privileged Groups. Clicking on a specific group will update the Panel with all activity for that specific group.
Group Membership Status	Provides the status on group members such as Active accounts, Dormant accounts, Never Logged On accounts, Empty and Nested groups
Privileged Group Membership Details	Detailed grid on group membership data.
Privileged Group Modifications	Privileged groups that have modified.
Operations Performed	Operations performed on privileged groups.

Privileged Group Modifications Details	Details of modifications performed on each privileged group

Regular Groups

The Regular Groups Panel displays information on all non-privileged group members. Data displayed is the same as the previous section.