→ INSIGHT THROUGH AUTOMATION

KEEPING YOUR SYSTEMS SECURE WITH LIONGARD

WHEN IT COMES TO MANAGING YOUR IT, NOBODY DOES IT BETTER.

We leverage a platform called Liongard to secure your IT infrastructure. Liongard takes our capabilities to the next level by providing unified visibility into your entire IT environment—from endpoints and cloud services to firewalls and networks—so we can proactively secure and protect your critical systems and data.

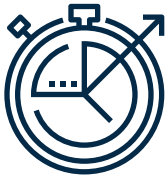
WE USE LIONGARD TO:

SECURE SYSTEMS

- → Alert on critical systems to keep them up and running, so you can focus on your business
- → Monitor your systems, including firewall and antivirus, to make sure they're actively mitigating threats
- → Detect and prevent vulnerabilities that could lead to a security breach or public data leak

SOLVE PROBLEMS

- → Track and discover systems (including hidden ones you may not have known about)
- → Resolve issues faster by rewinding time to see system history and changes
- → Monitor permissions to ensure compliance with security best practices such as Role-based Permissions and Least Privilege



OPERATE EFFICIENTLY

- → Track licenses across systems or environments to avoid paying for unused or duplicate accounts
- → Get alerted before certificates and domains expire to reduce outages and downtime
- → Identify when required password policies and authentication methods such as multi-factor authentication are not being followed

MONITORING & INSIGHT INTO YOUR CRITICAL SYSTEMS

Automation that enables insight. Visibility into your systems is just the first step. Liongard's automation ensures our documentation is always up-to-date, accurate and provides the data we need to take action. This lets us secure systems, avoid costly errors and quickly troubleshoot when issues come up. These are some of the systems Liongard helps us manage:

DOMAIN & TLS/SSL

- → Monitor upcoming expirations to proactively renew them before they expire
- → Get notified about DNS changes for web sites and email records and track previous configuration
- → Audit your domain registrant and other contact info, verify they're accurately updated, and understand the registrar details for each domain that you own
- → Know where your email is hosted and whether it's behind a spam filter
- → Identify if your domain name reputation is protected via SPF and DNSSEC records
- → Detect security vulnerabilities due to out-of-date and misconfigured certs
- → Discern and track the certificate Issuer

ANTI-VIRUS

- → Detect which devices are protected and which have been infected and require action
- → Confirm we've purchased enough seats to protect all your devices
- → Ensure your anti-virus policy is properly configured and applied

BACKUP

- → Ensure backups have been running successfully
- → Know agents are active and healthy

MICROSOFT 365

- → Confirm you've got the right quantity and types of licenses
- → Keep track of former staff members and other stale accounts
- → Determine whether you're being targeted for malware or are experiencing brute force attacks
- → Check policies to ensure security best practices with passwords are applied and properly enforced
- → Know your SharePoint sites and their storage usage

FIREWALLS

- → Track changes to firewall rules and other critical network security configurations
- → Renew licenses and track expirations for features enabled on the device
- → Detect unsaved configurations that may cause unexpected outages
- → Track firmware versions to improve maintenance and security processes
- → Know your critical network services e.g. DHCP detail and ranges & DNS
- → Know remote access details such as VPN users

ID MONITORING

- → Monitor users to see if their information has been compromised as part of a known data breach
- → Provide details including what information has been compromised and the source of the breach, when applicable

WINDOWS SERVER & ACTIVE DIRECTORY

- → Gather deep server data such as domain controllers, OS version, file share, and the computer details
- → Monitor privileged users and get notified if password policies are changed
- → Audit installed software to make sure you're running the latest version
- → Track and identify current, former, and stale staff members and stale accounts
- → Provide rapid review of users, group memberships and policies
- → Track device counts, listing of servers and domain controllers
- → Audit password policies, Active Directory Domain and Forest details, e.g. role holders, LDAP details, policies, and more

NETWORK DISCOVERY

- → Discover network devices via IP scan automatically
- → Surface public IP and DNS
- → Auto-discover the following network devices: SonicWall firewall, Synology NAS, Watchguard firewall, HP Procurve switch, and Fortinet Fortigate

SQL SERVER

- → Track database quantity, names, types, and sizes
- → Track and alert on critical health metrics like transaction log size and last backup
- → Track and audit maintenance plans, recovery model, and other database administration tasks