• Create Centralized Logging System (Monitoring Team)

<https://www.digitalocean.com/community/tutorial_series/centralized-logging-with-elk-stack-elasticsearch-logstash-and-kibana-on-ubuntu-14-04>

• Lock Down the Wireless Network (Networking Team)

Resources → Wireless Assessment

• OS/Runtime Vulnerability Scanning (Monitoring Team)

See resources → linux/windows intrusion cheatsheets

• Create Bastion (Jump Host) Infrastructure (Systems Team?)

‘’’A **bastion host** is a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer’’’

• Develop Incident Response Procedures (Monitoring Team)

See resources → incident handling start to finish

• Implement Privileged Account Management (Systems Team)

<https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services>

• Track Elevation of Privileges (Systems Team)

/var/log/auth.log

Grep for FAILED, fail, sudo, su

Event Viewer

• Install an Outbound Proxy (Systems Team)

<https://docs.microsoft.com/en-us/iis/extensions/configuring-application-request-routing-arr/creating-a-forward-proxy-using-application-request-routing>

• Create Incident Report Template (Monitoring Team)

<http://farmerresume.com/wp-content/uploads/2017/04/cyber-security-incident-report-template_0.png>

• Provide Recommendations for System Monitoring (Monitoring Team)

<https://www.beyondtrust.com/resources/webinar/a-security-experts-guide-the-windows-events-you-should-be-tracking-and-why/>

<https://www.eurovps.com/blog/important-linux-log-files-you-must-be-monitoring>

• Harden Network Cryptography (Networking Team)

Applied Crypto Hardening - BetterCrypto.org

• Provide Recommendations for Alerts (Monitoring Team)

Wire Shark

Packet Sniffers

Automated alerts every 15 minutes via slack?

• Implement Alerts (Monitoring Team)

<http://www.ics.uci.edu/~projects/dissemination/Trinet/Goltz.Task2.Report.pdf>

• Implement Security Event Tracking (Strike/Monitoring Team)

Actionable Security Intelligence ( <https://www.eventtracker.com/>)

• Implement Incident Response Tooling (Strike/Monitoring Team)

<http://searchdisasterrecovery.techtarget.com/Free-incident-response-plan-template-for-disaster-recovery-planners> - Inciedent Response Template

<https://www.alienvault.com/resource-center/ebook/insider-guide-to-incident-response/incident-response-tools> - Specific Incident Response tools

• Implement a network packet capturing system (Monitoring Team)

tcpdump

• Manage Windows Admin Account Alerts (Systems Team)

<https://community.spiceworks.com/topic/1425763-is-it-possible-to-get-an-alert-every-time-an-administrator-account-is-used>

• Create Dashboards (Monitoring Team)

There should be a some central resource for managing and monitoring. Ideally a browser-based UI that presents the overall health, highlights issues and alerts for all the systems across the network, along with the ability to view the specifics.

• Implement an API Gateway / Application Firewall (Systems/Networking Team)

<http://microservices.io/patterns/apigateway.html> - single entry API Gateway

<http://www.comentum.com/unix-linux-ip-firewall.html> - UNIX CMDs for firewall

<https://technet.microsoft.com/en-us/library/cc771920(v=ws.10).aspx> - NETSH CMDs for Windows firewall

• Provide Situation Reports (Monitoring Team)

Within 5 minutes → something’s going wrong

10-15 minutes → what happened/what are we doing

When corrected → back to normal

30+ minutes → everything is still normal

• Provide Forensic Investigations (Strike Team)

Volatile Memory

Volatility

Rekall

Linux Memory Extractor

Memoryze

Network Analysis

Network Miner

Wireshark

Xplico

Malware Analysis/Detection/RE

CFF Explorer Suite

Chkrootkit

IDA Pro

Regshot

Process Monitor

File Carving/Parsing/Metadata

AnalyzeMFT

Exiftool

Foremost

RegRipper