Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

Network Security Playbook Guide

You've seen the headlines: cyber breaches at major corporations jeopardizing confidential information for millions of users; highly targeted spear phishing campaigns delivering malware deep into networks; and DDoS attacks at e-Commerce companies causing loss of revenue and brand damage.

What you possibly haven't seen are the network security playbooks that organizations rely on during these events. By recognizing that a faster response leads to a better outcome, these plans mitigate business disruption and protect valuable information.

Don't make the mistake of thinking it won't happen to you. If you don't have a network security playbook already, it's time to start planning.

Making A Plan

Your network is unique. And so is every attack. A playbook that's tailored to your circumstances will help you orchestrate a swift response when you need it most.

Think of it as a playbook for threat game day that outlines your responses to diverse security scenarios. From threat detection and monitoring to response capabilities, this guide will walk you through some of the basic elements you should consider while putting together your playbook.

Keeping It Together

One of the benefits of having a network security playbook is that it enables efficiency during an otherwise cumbersome process. Yet, if your playbook isn't organized to suit your network and your security teams, you face the potential of providing your attackers with valuable time. And the longer an attacker has access to your network and systems, the more your security infrastructure suffers.

When establishing the structure of your playbook, consider organizing it along the timeline of a threat: detection, monitoring and response.

Incident Detection

This section of your playbook should help you make the transition from vigilantly watching over your network to identifying and preparing to take action against potentially threatening activity.

Detection Considerations:

- Keep a list of contact information for key players that are part of your incident response team. This can include internal team members, as well as individuals from network and Internet security providers.
- List protocols for identifying and responding to potential extortion or blackmail attempts.
- Have a holistic network map to serve as a visual tool during your diagnosis of the threat. This macro view map can help you perform "what-if" analyses in a model-based environment.

Incident Monitoring

Despite your cautious eye, you have detected a legitimate network attack. Your next steps will play a large role in how long it takes to recover. At this stage in your playbook, you should focus on actions that acknowledge the visibility you have into your network.

Monitoring Considerations:

- Have contact plans for network service providers. Evaluate your service level agreements with these providers so that you'll have realistic expectations of the role they can play in mitigating attacks.
- Utilize threat information sheets. Compile relevant information, such as the destination of the attack or the particular item (website, email server, database) being attacked, and input the information into a form that's easy to disseminate.
- Determine essential and non-essential devices for your organization. Depending on your needs, it might be acceptable to shut down a mail server, web server, or other non-essential ports to thwart an attack.

Response Capabilities

With clear visibility into your network, an informed team of key players and a wealth of data to rely on, you should be prepared to enact processes that will mitigate an attack. The benefit of having a playbook at this stage of a threat is that it will allow you to select a relevant response based on a strong foundation of knowledge and past experience.

Response Considerations:

- Communicate all of the information you've collected to your network provider. While your provider might not offer comprehensive mitigation services, they may provide some basic features that can help mitigate an attack.
- Use your network security partners to compile a threat-based series of responses that are centered in current industry best-practices. Whether it's a DoS, DDoS or insider-malware event, every industry has different needs when it comes to network security threat responses.
- Perform regression testing. You might have successfully mitigated the attack, but there may still be lingering issues that could come back to haunt you.

Simplify Your Threat Management

Protecting your business operations and securing valuable information are your playbook's top priorities. But why should you face increasingly complex cyber threats alone? With around-the-clock monitoring and mitigation services backed by Level 3 Communication's Security Operations Center, you can simplify threat management with a playbook that integrates the global footprint of a network provider.

Monitoring And Alerts

With proactive monitoring and alerts from Level 3, you'll benefit from:

- Continuous management of edge routers and detection of anomalies in volumetric flows
- Detection of layer 3 and 4 DDoS attacks
- Additional forensic evidence for quick DDoS attack mitigation
- Continuous management and monitoring of Firewall and Unified Threat Management (UTM) devices
- Proactive counter-measures to block threats based on SIEM alerts

DDoS Mitigation

With a total capacity of 4.5 Tbps of attack ingestion and scrubbing capacity, Level 3's footprint provides you with the bandwidth to re-route traffic to eight different regional scrubbing centers. DDoS attack traffic is filtered, and normal traffic is returned to you.

Peacetime Performance And Reporting

Even when operations are running smoothly, a provider like Level 3 has the global footprint and network depth to help you monitor and improve your network performance.

Firewall / UTM

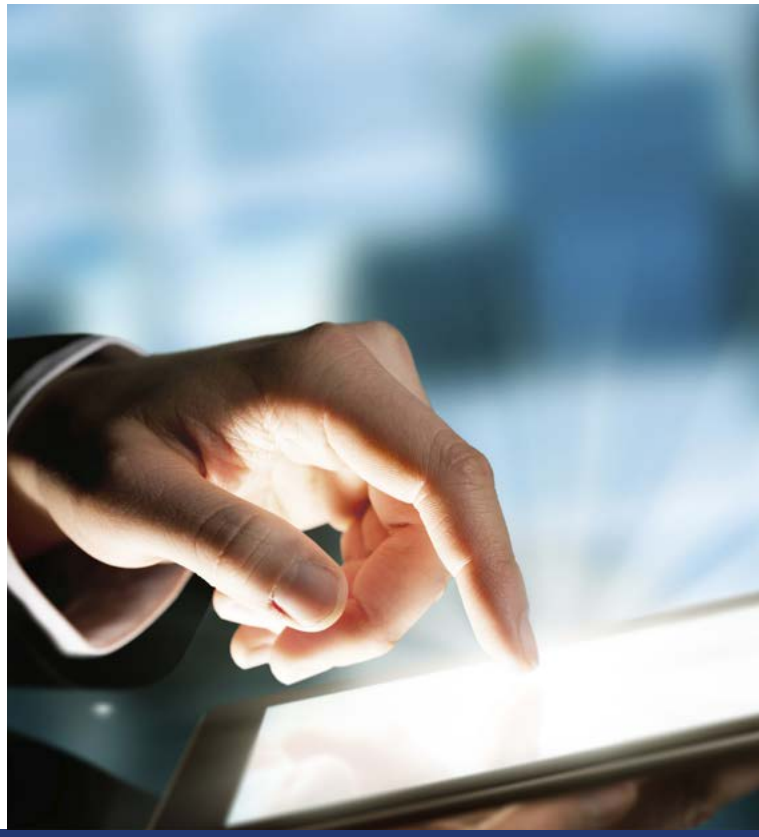
Simplifying your security infrastructure requires a commitment to innovative solutions. With Level 3℠ Managed Security Services, you'll have access to managed firewalls and Unified Threat Management (UTM). These tools can help you reduce costs, improve latency, and limit operational complexities — all of which will help your business grow.

MyLevel 3℠ Customer Portal

Visibility into attack data can make a big difference in the amount of downtime your business sees. The Level 3 Customer Portal gives you a clear overview of everything you need to know:

- IDS/IPS detections and actions
- Top IPS alerts
- Top source/destination IPs and ports denied by firewall
- Attack and clean traffic volume
- Attack duration
- Attack source IP address
- Specific reports that include: number of circuits under attack, attacks and attack-traffic volume, top historic attacks by type, and top 10 attack destinations

Many organizations expose themselves to costly business interruptions, damage to their brand image and loss of consumer trust because they aren't adequately prepared. Level 3's approach to network security addresses the complex and ever-changing threat environment that we live in. With attacks increasing in scale and complexity, it's critical to have the type of protection that a global network provider can offer.



Contact your Level 3 sales representative with questions about network security or setting up your organization's **Network Security Playbook.**