SECURITY ALERT

Computer Security

COMPUTER SECURITY ALERTS

The Security Alerts Your Analysts Should Be Following

Security alerts help organizations quickly detect advanced cyber-attacks. However, organizations are often bombarded with alerts from an array of IT devices. In fact half or more of the untuned security alerts generated by organizations end up as false positives. The sheer volume of alerts generated from an IT environment can be overwhelming for security teams.

It is important that local security analysts are focused on the right security alerts. Here are some of the important ones to start following and begin sifting out false positives.

1. Privileged User & Account Monitoring

Privileged user accounts are one of the most common security weaknesses for organizations. End users with endpoints can have administrator or root privileges which can lead to downloading malicious software, making changes to network or system settings, or inadvertently letting a hacker obtain access to sensitive data.

Local security teams should create dashboards to track privileged user activity. Hackers regularly attempt to obtain privileged user accounts and ways to escalate privileges as they are an entry to other systems and applications on your network. If a hacker has access to one of your privileged accounts, they can potentially bypass firewalls or Intrusion Detection Systems (IDS).

2. Abnormal External Communication

Security teams may be investigating lots of inbound traffic but, are they monitoring for abnormal outbound activity as well? External communication can take place on your network through an abnormal port or protocol. Your firewall can help with traffic filtering but may not catch everything. Abnormal external communication could be a hacker attempting to deploy malicious software, carry on Command-and-Control Activities, or more recently conduct hive Bot and swarm activities.

Security teams should review how external communications are filtered, monitored, and blocked. External communications toward an open resource are typically allowed, but if the communication is not for public resources, then it could be an unauthorized communication. Any traffic that gives cause for concern should be validated against your security policy and reviewed against malicious patterns. Security alerts can be generated from your IDS/IPS, firewalls, and switches to monitor these external communications.

3. Acceptable Use Policy Violations

Acceptable Use Policies (AUP) can be something that employees signed when they first onboarded but rarely follow now. Every organization should have a security briefing as part of onboarding, and an annual review and signoff thereafter. The AUP policy defines what end users can and cannot do with organizational technology. AUPs are important to protecting your organization from malicious activity on your network but are often not enforced or monitored.

Security teams should set up security alerts and dashboards to review AUP violations. Employees may browse inappropriate websites, download Torrent content, or fall for phishing schemes that leave your company susceptible to threat actors. As a result, monitoring AUP violations can help you quickly find endpoints with malware installed.

4. Data Exfiltration/Unusual Port Activity

Data exfiltration is one of the main objectives for advanced persistent threats (APTs). Threat actors can infiltrate frequently used ports to avoid firewalls and IDS and steal your company data. They can also use phishing and other social methods for infiltrating your environment.

Commonly used ports for data exfiltration include common Internet services, hoping that they will have an any/any rule for that port on firewalls:

- TCP: 80 (HTTP)
- TCP: 443 (HTTPS)
- TCP/UDP:53 (DNS)

Hackers typically use the following techniques to conduct an attack:

- Backdoors: collects files and uses ports like 80, 443, and 53 to hide traffic
- Web applications: an attacker can access data directly from web pages using ports above
- File transfer protocol (FTP): hackers use FTP as it is a standard for transferring files – use SFTP or FTPS instead, or even better, use a secure cloud provider; lookup https://thruinc.com.
- Windows Management Instrumentation: a threat actor can use this to look at files and receive emails from Microsoft Outlook

Security teams can set up alerts using your network intrusion and prevention system logs to identify any of the suspicious port activity mentioned above. Your team may find that the traffic represents malware infiltration. Your team could also consider setting up specific security alerts when data is shared externally more than normal. It could be a threat actor or insider stealing company data.

5. File Integrity Monitoring

Another area your analysts may want to look at closely is File Integrity Monitoring (FIM). Your auditing policy should include unexpected changes in a file's status and alert on it, through NG Endpoint Protection (EPP), SIEM or both. Your team could setup an alert and dashboards to find out if files have been changed recently. If file access auditing looks suspicious or like something changed that should not have, then you should investigate the event in more detail.

File access auditing can tell you which files have been viewed, what programs are executing using those files, and if any files were deleted or created. Any suspicious files should run through your antivirus tool or next-gen endpoint protection solution to identify if there are malicious executables. You may find correlations with patterns like ransomware, data compromise, and exfiltration.