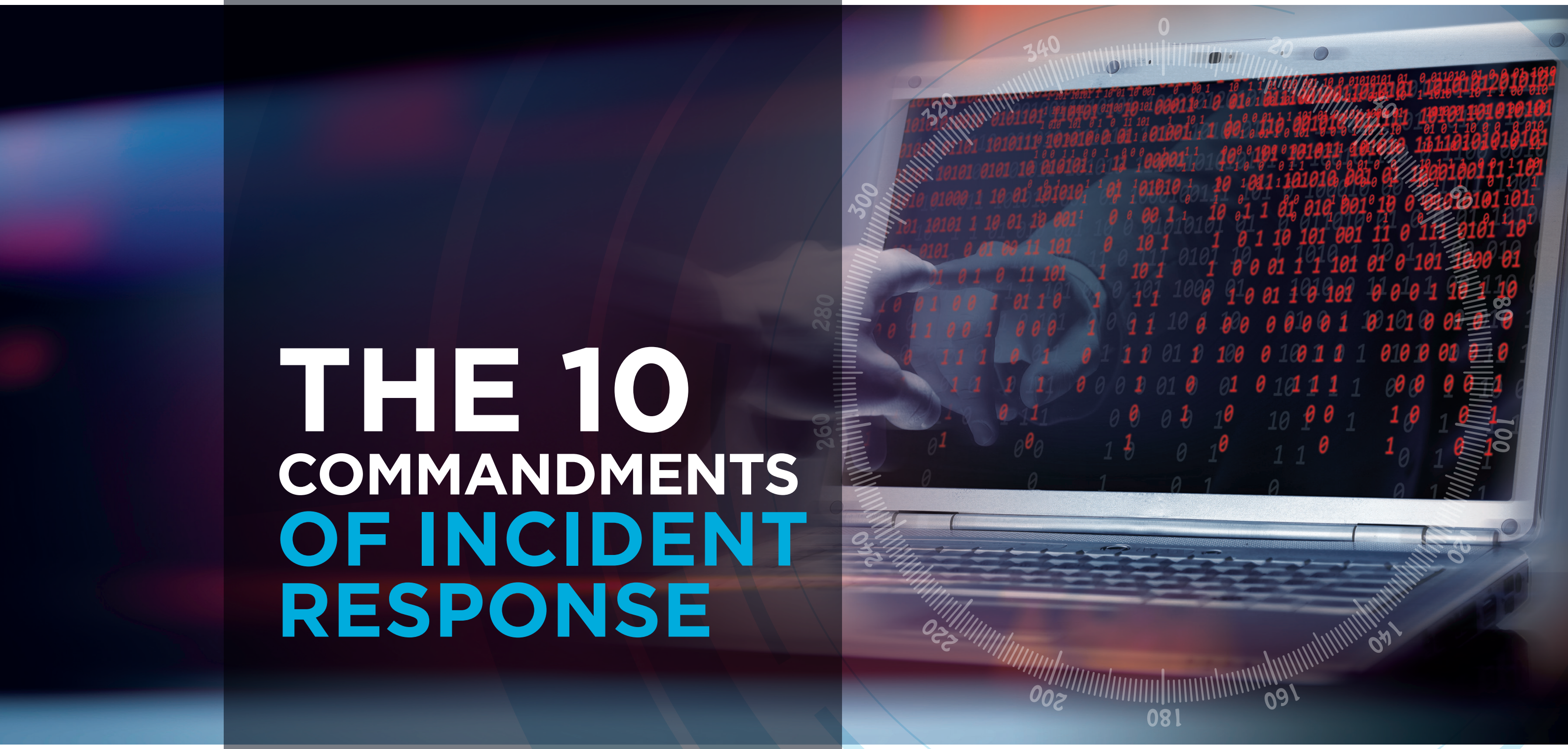
Cynet
Advanced Threat Detection & Response



THE 10 COMMANDMENTS OF INCIDENT RESPONSE

Today's increasingly sophisticated cyberattacks require rapid-response readiness on the part of an organization looking to protect its assets. Innovative cyberattacks have the potential to lock the endpoints and intelligence of the largest enterprise in minutes, bringing business to a standstill. As attacks grow in stealth and frequency, organizations are searching for better ways to defend themselves. Many utilize multiple silo solutions, in the attempt to defend every front. But attacks succeed in bypassing these defenses, and security teams are left needing to rapidly and accurately react when this occurs. This is when they turn to Incident Response. Below you will find Cynet's 10 Commandments of Incident Response.

Alerts Report
Date Range: 01/05/2017 - 31/05/2017

Alerts By Type

Alerts By Status

Summary
- 83 Total alerts
- 74 High alerts
- 5 Med alerts
- 4 Low alerts
- 82 Opened alerts
- 1 Closed alerts

26- Total open file alerts
Top 10 file alerts:
C:\windows\system32\msiexec.exe
...3de82576f6fa5d4cac344f15c0e0.exe
...2576f6fa5d4cac344f15c0e0.bin.exe
...2576f6fa5d4cac344f15c0e0.bin.exe
...e Workstation\x64\vmware-vmx.exe
...e Workstation\x64\vmware-vmx.exe
...e Workstation\x64\vmware-vmx.exe
...e Workstation\x64\vmware-vmx.exe
...e Workstation\x64\vmware-vmx.exe

0- Total open user alerts
Top 10 user alerts:

THE 10 COMMANDMENTS OF INCIDENT RESPONSE

1 **You need an Incident Response solution.**
Endpoint Detection & Response, User & Entity Behavior Analytics, Network Analytics and more. All are important, but unless they function on an integrated level, threats are missed. Multiple silo solutions means that getting the full picture of an attack process is nearly impossible.

2 **The stakes are high.**
Without an Incident Response solution in place, organizations risk facing repeat attacks; not knowing about an attack until severe damage has occurred; and experiencing financial loss.

3 **The key is visibility and preparedness.**
Incident Response is crucial because of the visibility and readiness it provides, enabling organizations to respond quickly and effectively. Organizations that are not prepared are commonly breached without their knowledge, making it difficult to respond and increasing the scope of damage.

4 **It is crucial to have a good plan in place.**
The key to attack preparedness is visibility; all data related to a specific attack needs to be presented as a cohesive picture. This includes identifying the impacted user(s), their roles and locations, the compromised host, its location and the assets impacted by the attack. This information needs to be delivered automatically, as soon as an attack occurs.

5 **Identify and remediate true attacks more quickly.**
Security teams often waste crucial time investigating leads that turn out to be false positives. With an Incident Response solution in place, true threats can be identified, confirmed and remediated quickly, without wasting crucial time and risking increased data loss.

6 **Attack analysis time must be as short as possible.**
The longer it takes for an organization to respond to a true threat, the more data and financial loss it's likely to incur. Even the largest organizations should have the ability to analyze user, file, network and machine activity quickly.

7 **Think like a hacker.**
Identifying what hackers have done or are doing requires investigation, correlation and visibility. Best practices call for first determining whether the incident was a true breach or a false alarm, then analyzing all related indicators. This information should be documented for every event, machine, file or user to prepare against future attacks.

8 **Triage and classify.**
After an attack, it's imperative to understand and document the functional and informational impact of the attack, and the recovery effort. Detailed information on every incident and element related to the attack, as well as a RACI table for each potential attack scenario, should be easily accessible with a fully-integrated security platform.

9 **Respond immediately.**
Well-prepared organizations that have the proper platform in place allowing complete, integrated visibility into their environment, should be able to respond to every kind of attack within seconds, even in a multiple-effected environment.

10 **Real threats or attacks must be contained.**
An Incident Response solution should be in-place to contain real threats or attacks, limiting the damage they can inflict. Removing a machine from the network, updating the credentials of a compromised user account and other forms of containment should occur automatically in response to an attack.