TECH Track

Threat Hunting with Azure Sentinel

Christoph Burmeister, Jan-Henrik Damaschke

Speaker

Christoph Burmeister

Senior Consultant

MVP CDM

@chrburmeister

@hhpsug

itinsights.org

Jan-Henrik Damaschke

Senior Cloud Architect

MVP Azure, MCT

@jandamaschke

itinsights.org

Agenda

- Security primer
- What is Threat Hunting?
- Azure Security overview
- Azure Sentinel
- Alerting
- Hunting
- Integrations
- Takeaways

Security Primer

Identity is the new perimeter

Most common attacks:

- Phishing 44%
- Malware 31%
- Social Engineering 27%

-> Human based attacks > 71% of attacks

Yes, attack services are inexpensive

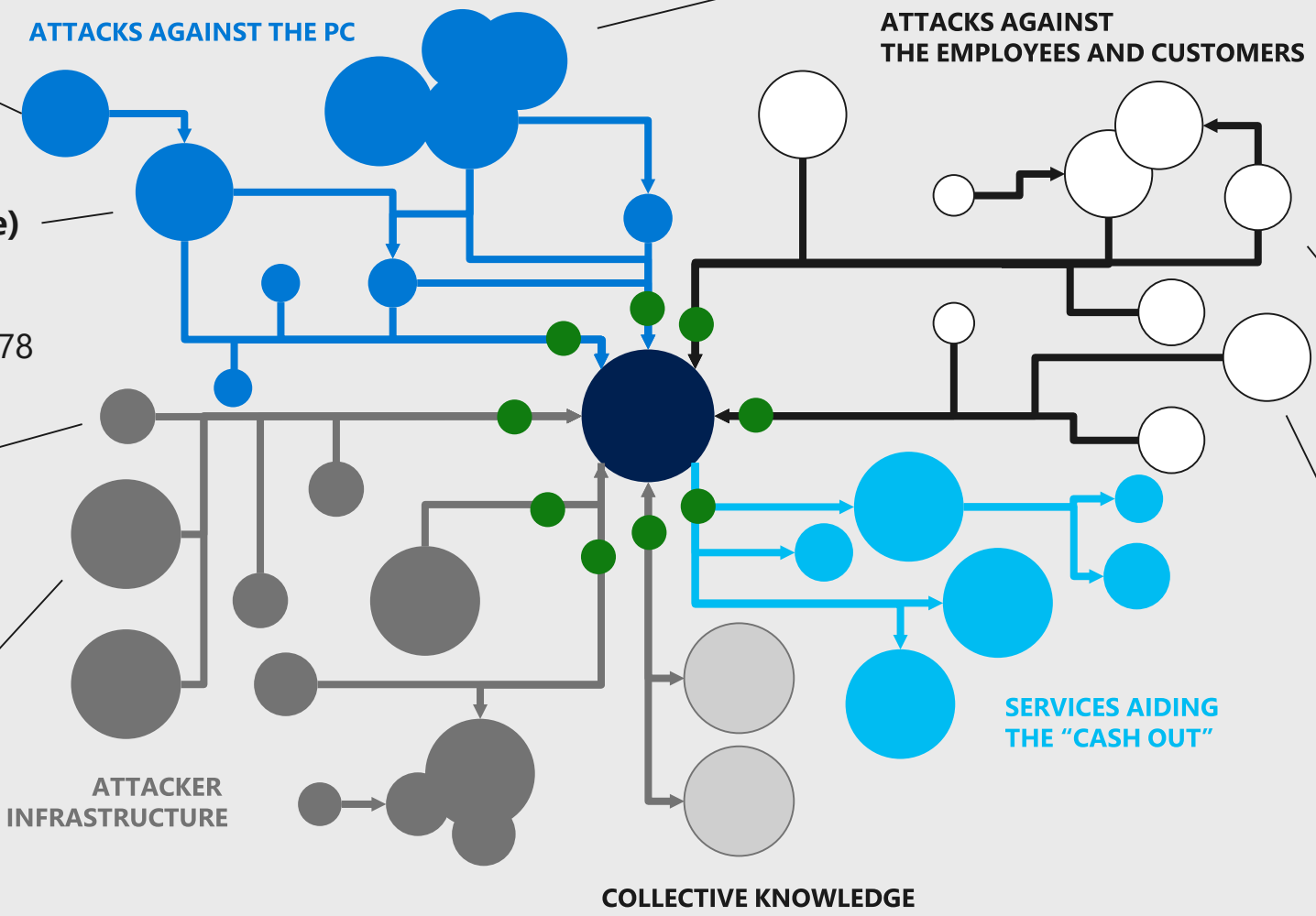
Ransomware:
$66 upfront
Or
30% of the profit (affiliate model)

0days price range varies from $5,000 to $350,000

Loads (compromised device) average price ranges
- **PC** - $0.13 to $0.89
- **Mobile** - from $0.82 to $2.78

Denial of Service (DOS) average prices
day: $102.05
week: $327.00
month: $766.67

Proxy services (evade IP geolocation) prices vary
As low as $100 per week for 100,000 proxies.

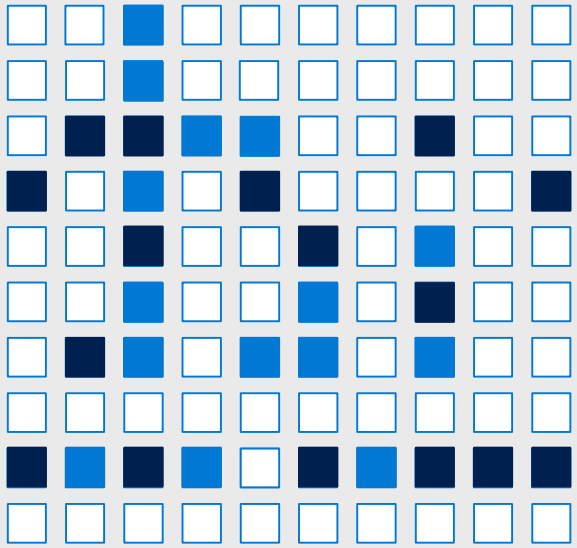


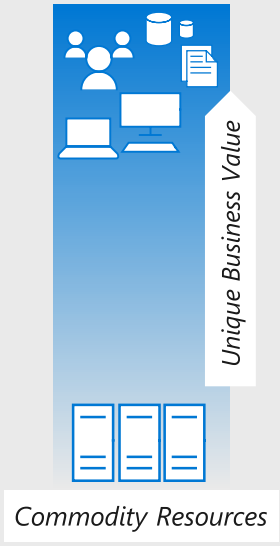
Spearphishing services range from $100 to $1,000 per successful account take over

Compromised accounts
As low as $150 for 400M.
Averages $0.97 per 1k.

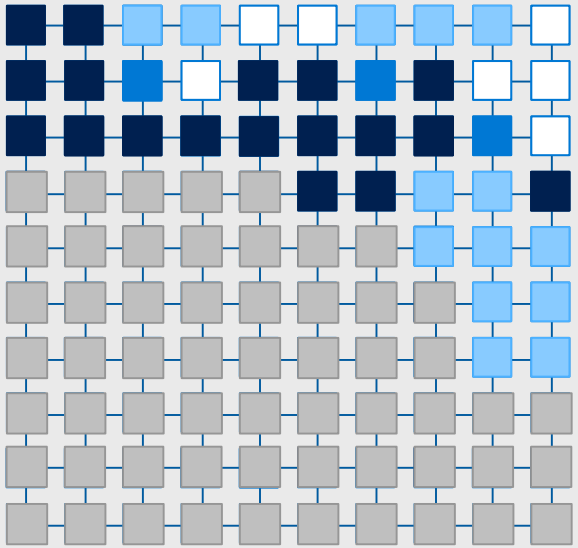
Security Advantages of Cloud Era

TRADITIONAL APPROACH





CLOUD-ENABLED SECURITY



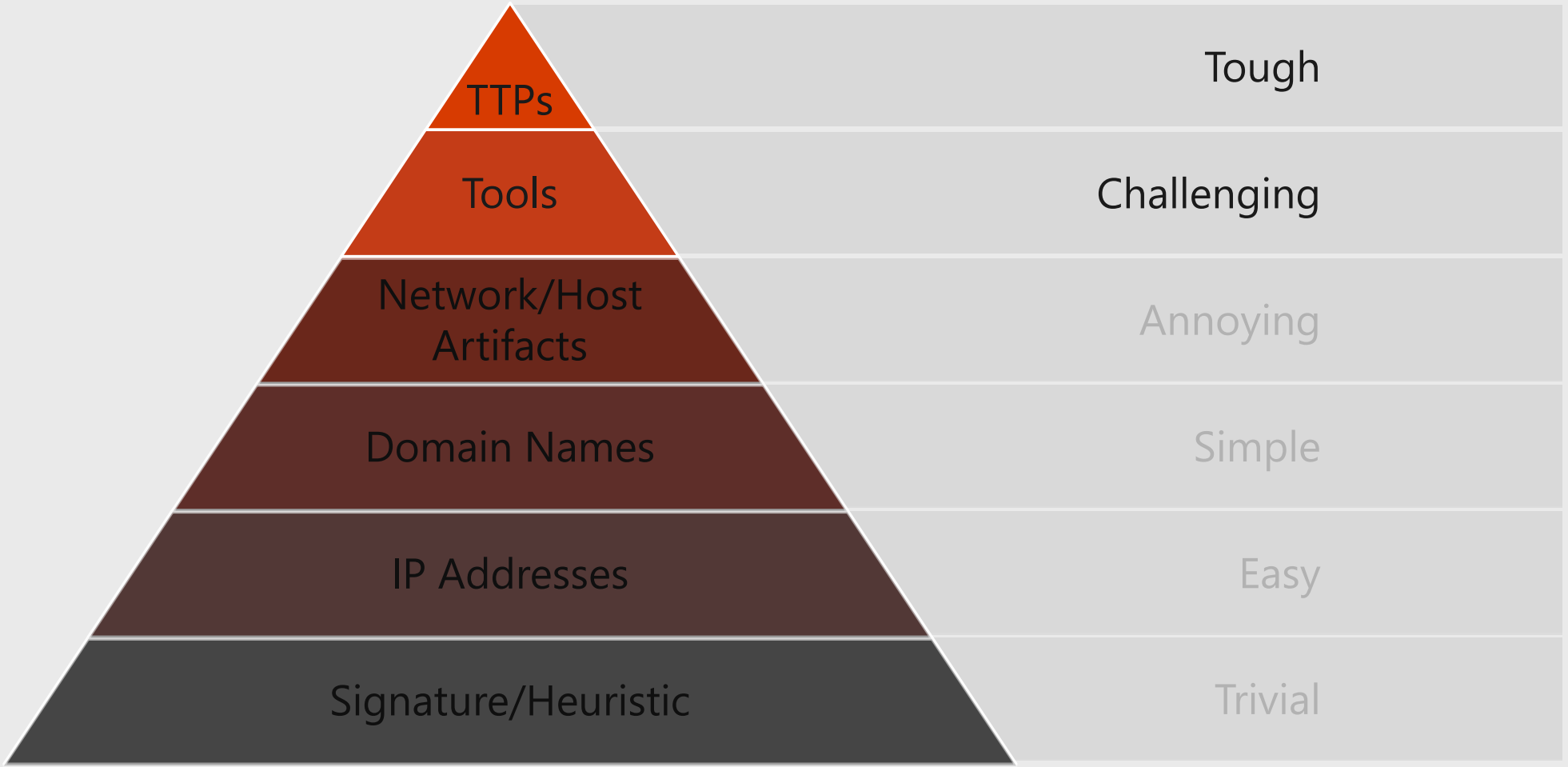
Security is a challenging and under-resourced function

- Satisfied responsibility
- Partially met responsibility
- Unmet responsibility
- Cloud Provider responsibility (Trust but verify)

Cloud Technology enables security to:

- Shift commodity responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- Use Cloud intelligence improve detection/response/time

Pyramid of Pain



What is Threat Hunting?

- Blue Team Tactic
- Basically proactive incident response
- Technical, network and system related
- Detect threats that are not detected by classic security tools
- Continuous planned process
- Analytics of IOCs

-> Data is key for threat hunting!

Cybersecurity Reference Architecture

April 2019 – https://aka.ms/MCRA | Video Recording | Strategies

Security Operations Center (SOC)

Microsoft Threat Experts | Incident Response, Recovery, & CyberOps Services

Azure Sentinel – Cloud Native SIEM and SOAR (Preview)

Vuln Mgmt | MSSP | Cloud App Security | Azure Security Center | Microsoft Defender | Office 365 | Azure

Advanced Threat Protection (ATP)

Graph Security API – 3rd Party Integration

Alert & Log Integration

This is interactive!

1. Present Slide
2. Hover for Description
3. Click for more information

Roadmaps and Guidance

1. Securing Privileged Access
2. Office 365 Security
3. Rapid Cyberattacks (Wannacrypt/Petya)

Software as a Service

Office 365

- Secure Score
- Customer Lockbox

Dynamics 365

Clients

Unmanaged & Mobile Devices

Intune MDM/MAM

Managed Clients

System Center Configuration Manager

Microsoft Defender ATP

Secure Score | Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection

Extranet

NGFW | Edge DLP | SSL Proxy | IPS/IDS

Azure Firewall | Security Appliances

Express Route

Intranet Servers

Windows Server 2019 Security

Window 10 + Just Enough Admin, Hyper-V Containers, Nano server, and more...

Shielded VMs | Azure Stack | VMs

Privileged Access Workstations (PAWs)

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Application & Network Security Groups
- Backup & Site Recovery
- Disk & Storage Encryption
- Confidential Computing
- DDoS attack Mitigation+Monitor

Information Protection

Conditional Access – Identity Perimeter Management

Cloud App Security

Azure Information Protection (AIP)

- Discover
- Classify
- Protect
- Monitor

Hold Your Own Key (HYOK)

AIP Scanner

Classification Labels

Office 365

- Data Loss Protection
- Data Governance
- eDiscovery

Azure SQL Threat Detection

SQL Encryption & Data Masking

Azure SQL Info Protection

Microsoft Defender ATP

Identity & Access

Azure Active Directory

- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Azure AD B2B
- Azure AD B2C
- Hello for Business
- MIM PAM

Azure ATP

Active Directory

ESAE Admin Forest

Windows 10 Enterprise Security

Network protection | Credential protection | Exploit protection | Reputation analysis | Full Disk Encryption | Attack surface reduction

App control | Isolation | Antivirus | Behavior monitoring

S Mode

IoT and Operational Technology

Windows 10 IoT | Azure IoT Security | Azure Sphere | IoT Security Maturity Model | IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL)

Trust Center | **Intelligent Security Graph**

Microsoft

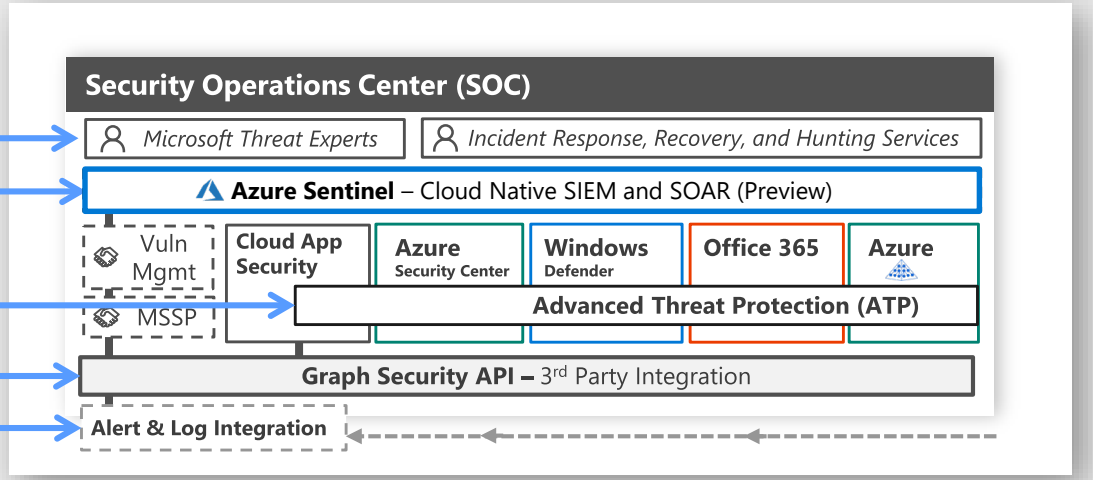
Security Operations Center (SOC)

CHALLENGES

- Legacy model results in **wasted security expertise**
  - **Analyst Overload** - too many false positives
  - **Poor Investigation Workflow**
  - **Manual integration** for tools and threat intelligence
  - Constantly evaluating products
- **Limited experience and toolsets** for securing hybrid architecture and Platform as a Service
- **Critical Risks -** Privilege management and security hygiene critical for cloud workloads

MICROSOFT PLATFORM

- ✓ **Incident Response and Recovery, hunting for adversaries**
- ✓ Cloud-native SIEM+SOAR
- ✓ **Integrated investigation experience**
- ✓ **Integrate existing SOC tools**
- ✓ Intelligent Security Graph



Azure Sentinel

- Cloud native Security Information and Event Management – SIEM
- Security Orchestration Automation Response - SOAR
- Currently in public preview
- Based on Log Analytics data
- ML based integration
- External service integrations

Features

- Dashboarding (Workbooks)
- Analytics
- Incidents
- Automation
- Behavior Analytics
- Investigation
  - Investigation graph
- Hunting
  - Hunting queries
  - Correlations

Azure Sentinel vs. Azure Security Center

Topic	Sentinel	ASC
Targets	Hybrid focused (SIEM, SOAR)	Cloud focused (CSPM, CWPP)
Alerting	Alerting integrated	No alerting capabilities
Dashboarding	Dashboarding integrated	No dashboarding capabilities
Threat Hunting	Threat hunting based on LA queries	No threat hunting capabilities
Recommendations	No built-in recommendations	Azure based recommendations
Compliance	No built-in compliance features	Policy and regulatory based compliance
Advance Defenses	No defense features built-in (SIEM)	Adaptive application control, JIT, etc.
Automation	Playbooks (Logic Apps) based automation	No integrated automation
Integration	Yes	Few and they will be deprecated
Pricing	Priced with Log Analytics Namespace	Priced per instance (always all subscription instances)

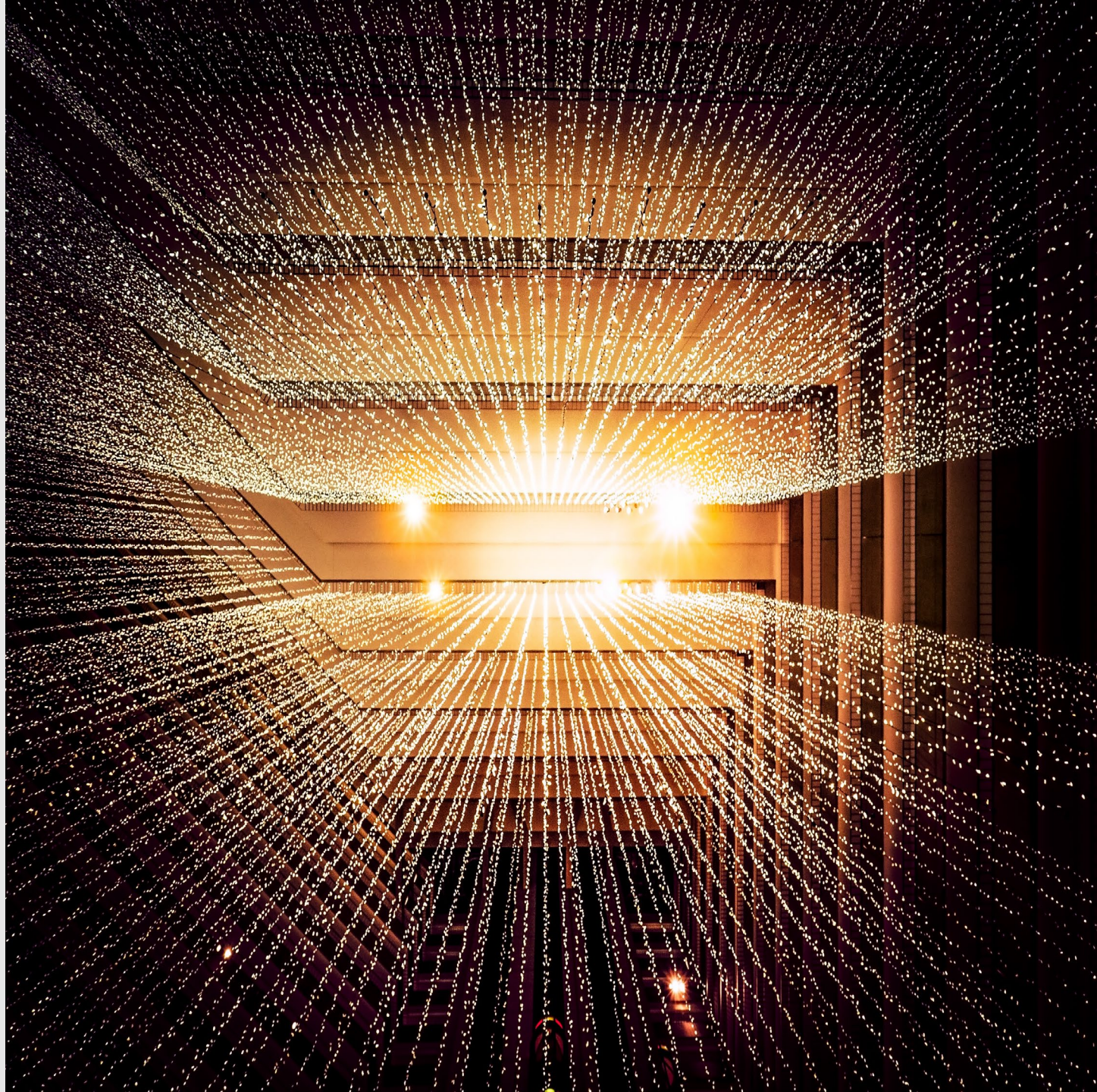
DEMO
Dashboards/Workbooks

Alerting

- Sentinel Analytics based alerts
- Azure Sentinel Incident Management
- Logic Apps incident automation
- Investigation graph

DEMO

Brute-force attack



Hunting

- Kusto based hunting queries
- Classified by MITRE ATT&CK

Sources for Hunting:

- Azure Sentinel Repo (https://github.com/Azure/Azure-Sentinel)
- Sigma rules (https://github.com/Neo23x0/sigma)
- https://attack.mitre.org/
- https://docs.microsoft.com/en-us/azure/kusto/query/

Common Attacks

PLAN

ENTER

TRAVERSE

EXECUTE MISSION

A. Enter and Navigate

Any employee opens attack email
→ **Access to most/all corporate data**

Any

2a

Workstation compromised, threat actor gathers credentials

3a

Threat Actors use stolen credentials to *move laterally*

1

Threat Actor targets employee(s) via phishing campaign

4

Threat Actors exfiltrate PII and other sensitive business data

B. Device Compromise

Targeted employee opens attack email
→ **Access to same data as employee**

2b

Employee B opens infected email (Mobile or PC). Attacker disables antivirus

3bc

Compromised credentials/ device used to access cloud service / enterprise environment

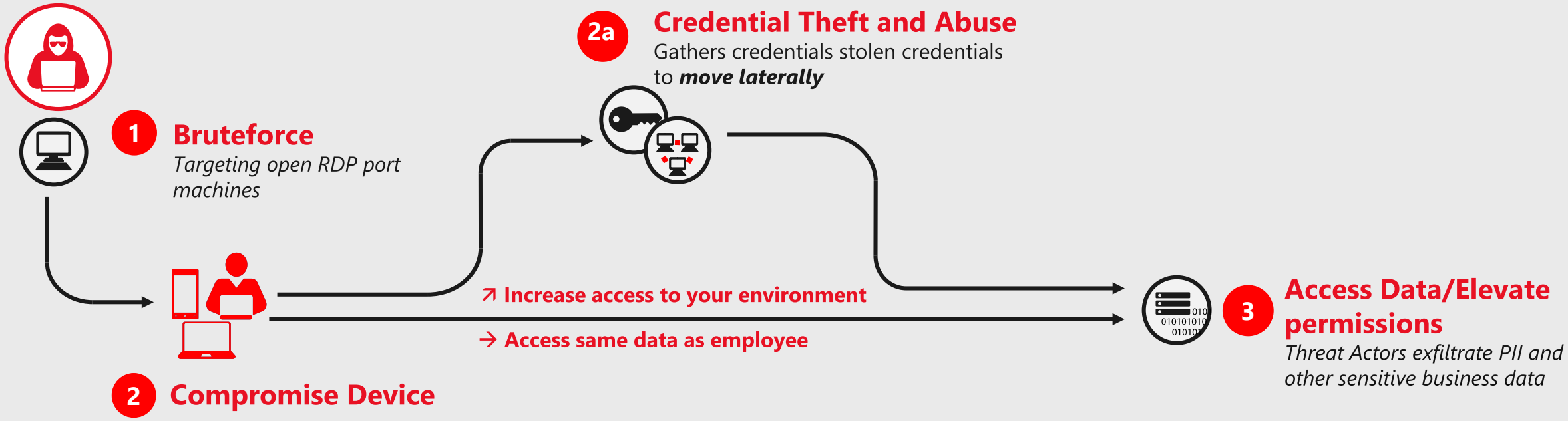
C. Remote Credential Harvesting

Targeted employee(s) enter credentials in website
→ **Access to same data as employee(s)**

2c

Credentials harvested when employee logs into fake website

Demo attack chain



Used tools on C2 server:

- Ubuntu based
- Covenant (.NET based command and control framework)
- Offensive PowerShell scripts
- Metasploit

DEMO

PowerShell execution

DEMO

Privilege escalation

DEMO
Persistence

Current Integrations

AWS

Azure AD

Azure AD Identity Protection

Azure Activity

Azure ATP

Azure Information Protection

Azure Security Center

Barracuda

Check Point

Cisco ASA

Common Event Format (CEF)

CyberArk (Preview)

DNS (Preview)

F5

Fortinet

MCAS

MDATP (Preview)

WAF

Office 365

Palo Alto Networks

Security Events

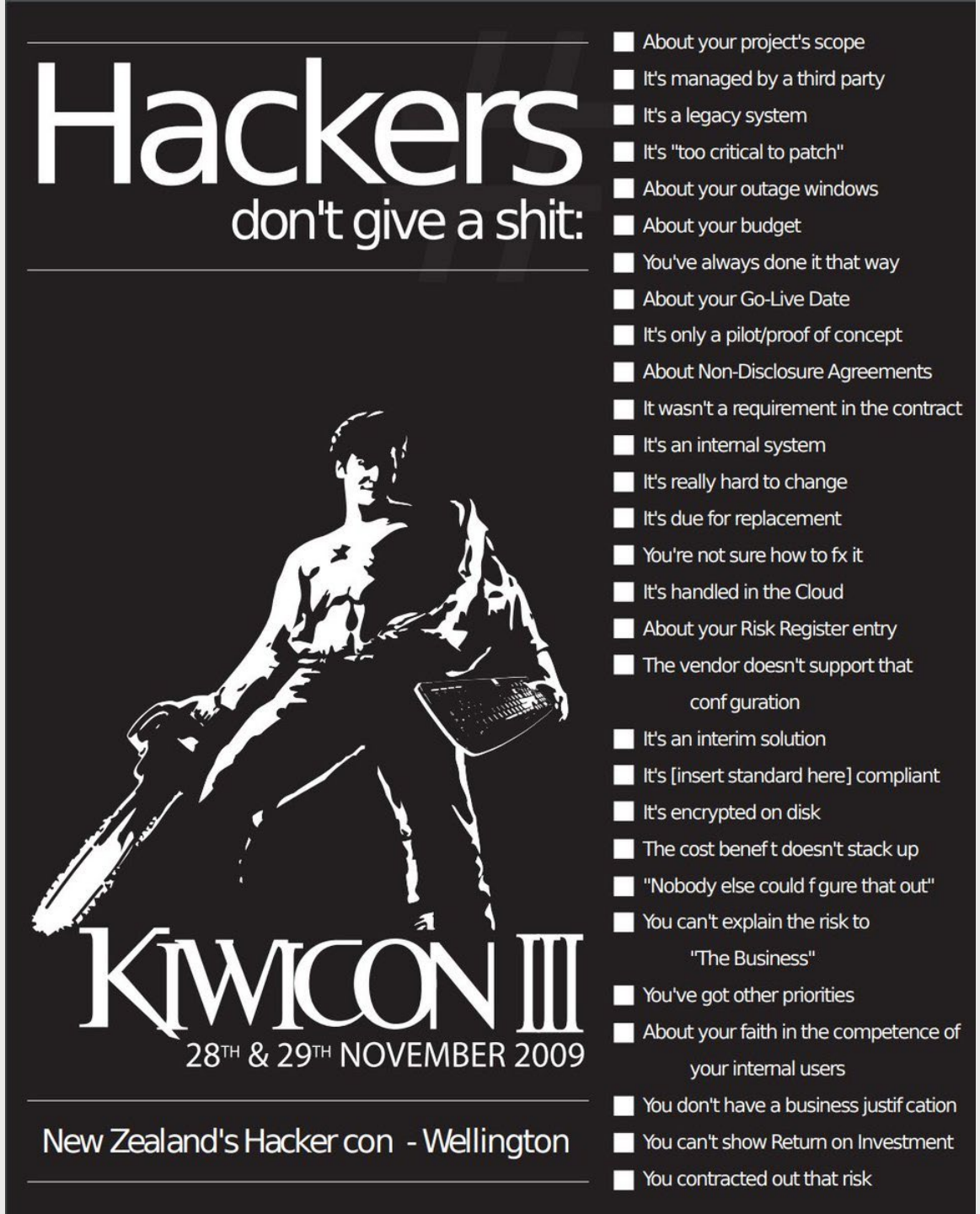
Symantec ICDx

Syslog

Threat Intelligence Platforms

Windows Firewall

Takeaways


Hackers
don't give a shit:
KIWICON III
28TH & 29TH NOVEMBER 2009
New Zealand's Hacker con - Wellington
About your project's scope
It's managed by a third party
It's a legacy system
It's "too critical to patch"
About your outage windows
About your budget
You've always done it that way
About your Go-Live Date
It's only a pilot/proof of concept
About Non-Disclosure Agreements
It wasn't a requirement in the contract
It's an internal system
It's really hard to change
It's due for replacement
You're not sure how to fx it
It's handled in the Cloud
About your Risk Register entry
The vendor doesn't support that conf guration
It's an interim solution
It's [insert standard here] compliant
It's encrypted on disk
The cost benef t doesn't stack up
"Nobody else could f gure that out"
You can't explain the risk to "The Business"
You've got other priorities
About your faith in the competence of your internal users
You don't have a business justif cation
You can't show Return on Investment
You contracted out that risk

Questions