Cyber Threats, Cyber resilience

CONNECTWISE

Customers have their say

43% Say they have a lack of Trust in their current IT Security Provider

We need to be Transparent

76% of businesses have experienced a financially damaging cyberattack in the past 5 years, in 2021 (62%) in 2020 (55%)

Over 67% report not having the Skills in house to properly deal with Security Issues.

29% of business decision makers cited *"Inadequate Cyber Security protections "* as a critical capability for an IT service provider

* The State of SMB Cybersecurity in 2022 (connectwise.com)

Research conducted in 2H 2022

CONNECTWISE

How Cyber Crime is Evolving

NCSC Annual Review 2022

Threats, risks & vulnerabilities

Ransomware

A form of malware used by cyber criminals to prevent or limit users from accessing their systems or data – or threatening to leak it - until a ransom is paid

Commodity attacks

High-volume, low-sophistication attacks usually involving phishing and other scams often reaching citizens and small businesses

Proliferation

Increased commercial availability of high-end disruptive and offensive cyber capabilities and tools used by state and non-state actors

Supply chain

Attacks where perpetrators access an organisation's network or systems via third-party vendors or suppliers

Vulnerabilities

Weaknesses in an IT system that can be exploited by an attacker to deliver a successful attack

The threat from state actors

Russia

used cyber capabilities to maximise operational impact in Ukraine. A seasoned cyber aggressor with a record of attacks against its neighbours and the UK, including attempts to steal Covid vaccine research in 2020

China

is becoming ever more sophisticated, increasingly targeting third-party technology, software and service supply chains

Iran

an aggressive cyber actor which, in November 2021, was called out by the NCSC, CISA, FBI and the ACSC for exploiting Microsoft Exchange and Fortinet vulnerabilities

North Korea

a less sophisticated cyber aggressor, it uses capabilities to mitigate its poor economic status through cyber crime and theft

State threat methods

The type of threats posed by these states varied widely, including:

- Disproportionate cyber-enabled espionage
- Reckless use of destructive cyber capabilities with the potential to cause harm to innocent victims
- Cyber-enabled theft of intellectual property or personal data of citizens for commercial advantage
- Undermining of legitimate democratic institutions including electoral processes

Not the Only risk to SMB

Being a target of Critical national infrastructure risk will always be there, but it isn't the only risk.

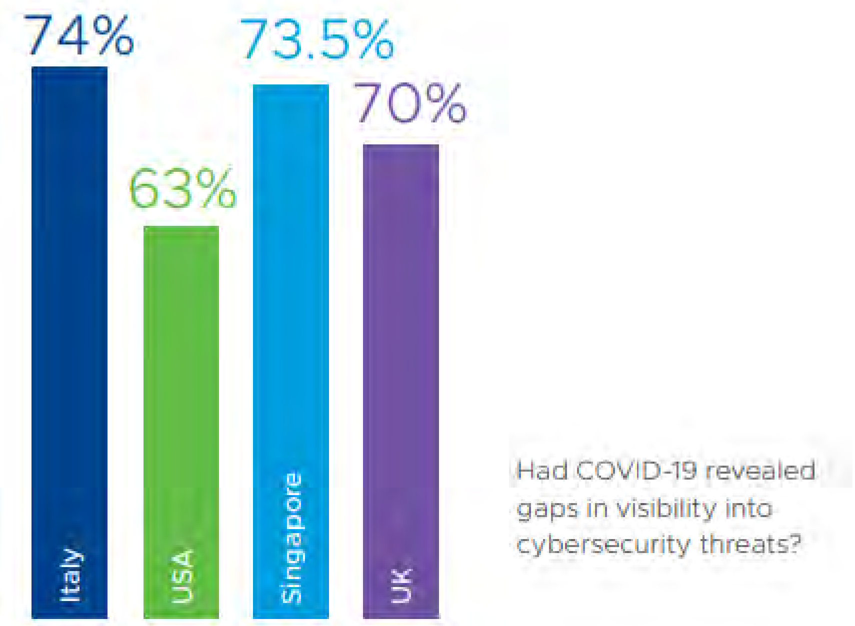
The majority of attacks on SMB are financially motivated, they use tried and tested fraud techniques combined with Technology

Ransomware and Business Email compromise are the biggest two.

How has home working added to the risk?

Home working has increased the Traditional Attack surface.

We have less control and visibility over the environment.



More than just an Enterprise issue?

Studies suggest that 70% of Ransomware attacks in 2022 are targeted at the SMB

If that is the case then Why don't we hear more?

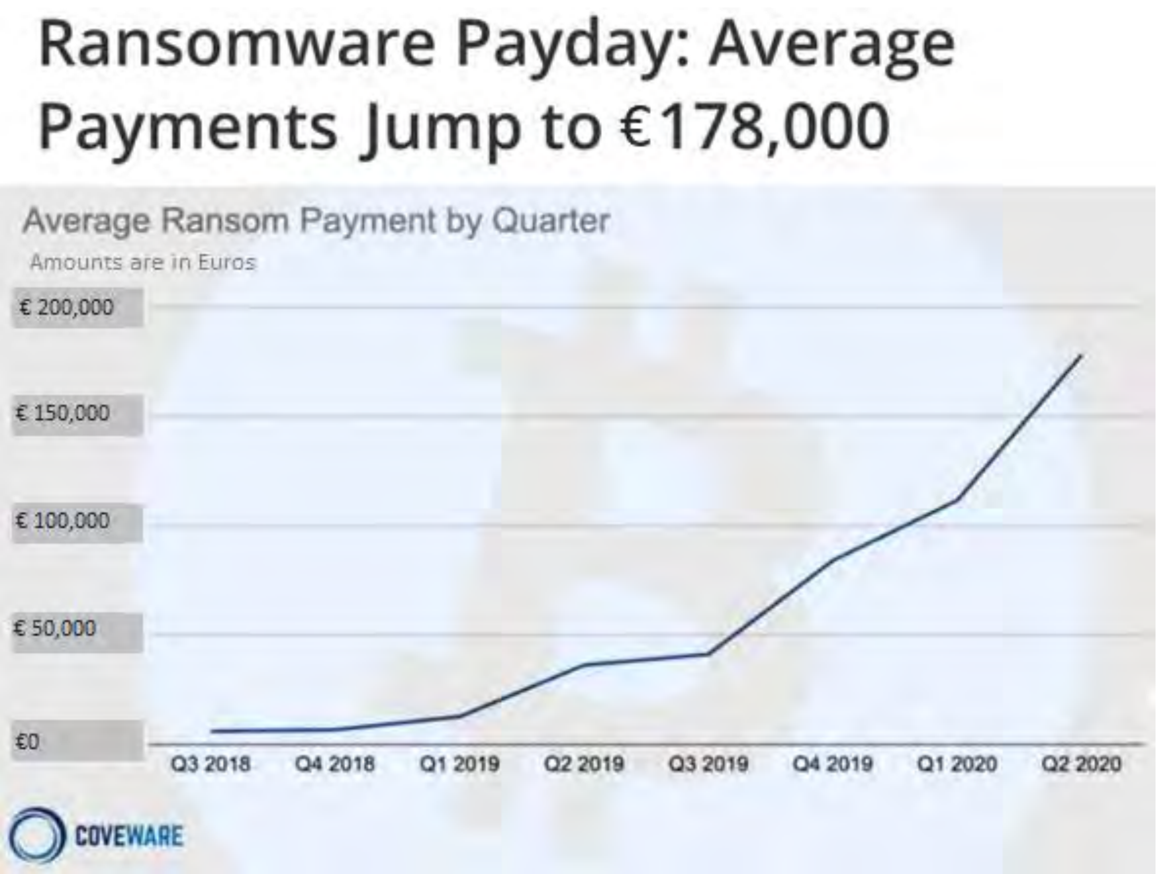
- It's not newsworthy
- It's embarrassing to admit you've been hacked
- The legal ramifications (fines, lawsuits, legal fees) can be significant, so many incidents go unreported.

44% of UK Consumers Claim they will stop spending with a business Temporarily after a Security Breach, 41% claim they will never return.

38% of US and UK companies Were found to had lost business due to security Issues in a Forrester Security report.

CONNECTWISE

The True Impact of Cyber Crime



Source: Matthew J. Schwartz, August 18, 2020

Cyber Crime is up, how much?
According to the Ponemon study *'the cost of Phishing'* phishing attacks alone have quadrupled since 2015 with US companies on average losing 14.8million or €1500 per employee)

"What we have found is that Ransoms alone account for less than **20 percent** of the cost of Ransomware attack"

The impact of a cyberattack on organizations:

1. Ransom (Up to 10% of turnover)
2. Incident response costs (Initial response and forensics)
3. Downtime damage (avg. downtime 23 days)
4. Fines due to data breaches
5. Intellectual Property theft
6. Reputational damage
7. Loss of data

Source Data : The Cost of Phishing 2021 – Report conducted by Proofpoint / Ponemon
Source Data : ING.nl Cyber Security Sector theme Update

The Role of Insurance

We transfer high risk low probability scenarios with Insurance.

Trouble is that Insurance companies have found these scenarios are no longer low probability

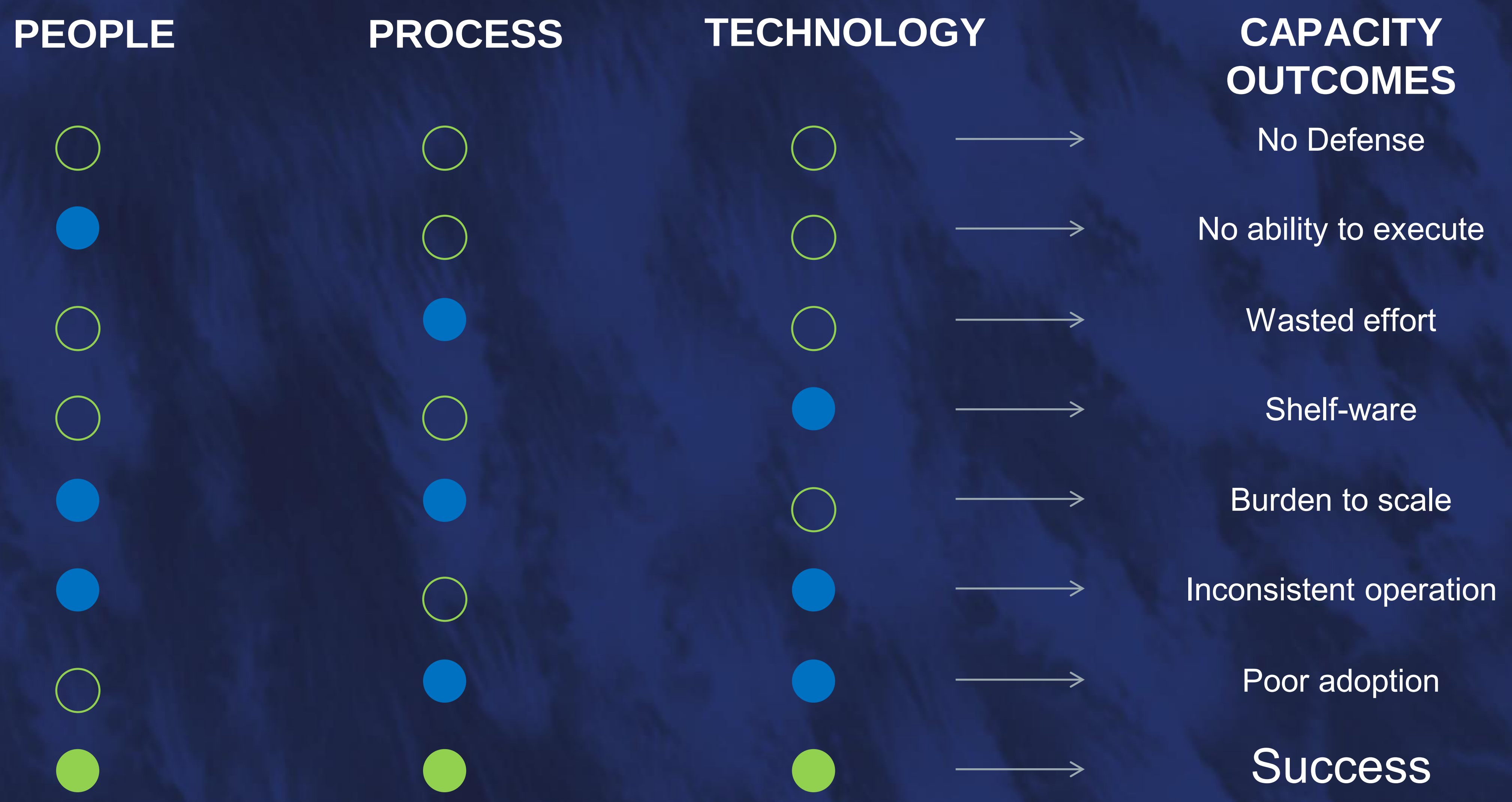
Policy's are adjusting to Risk conditional to having set services in place. Such as

- EDR
- Incident response
- Logging (Siem)
- Security Awareness Training
- Not using unsecured Tech providers

* Source: Ransomware: Ture cost to business, Cybereason

CONNECTWISE

Why does security fail?


PEOPLE
PROCESS
TECHNOLOGY
CAPACITY OUTCOMES
No Defense
No ability to execute
Wasted effort
Shelf-ware
Burden to scale
Inconsistent operation
Poor adoption
Success

What does good look like? – Security Architectures (or Frameworks)

Book Definition:

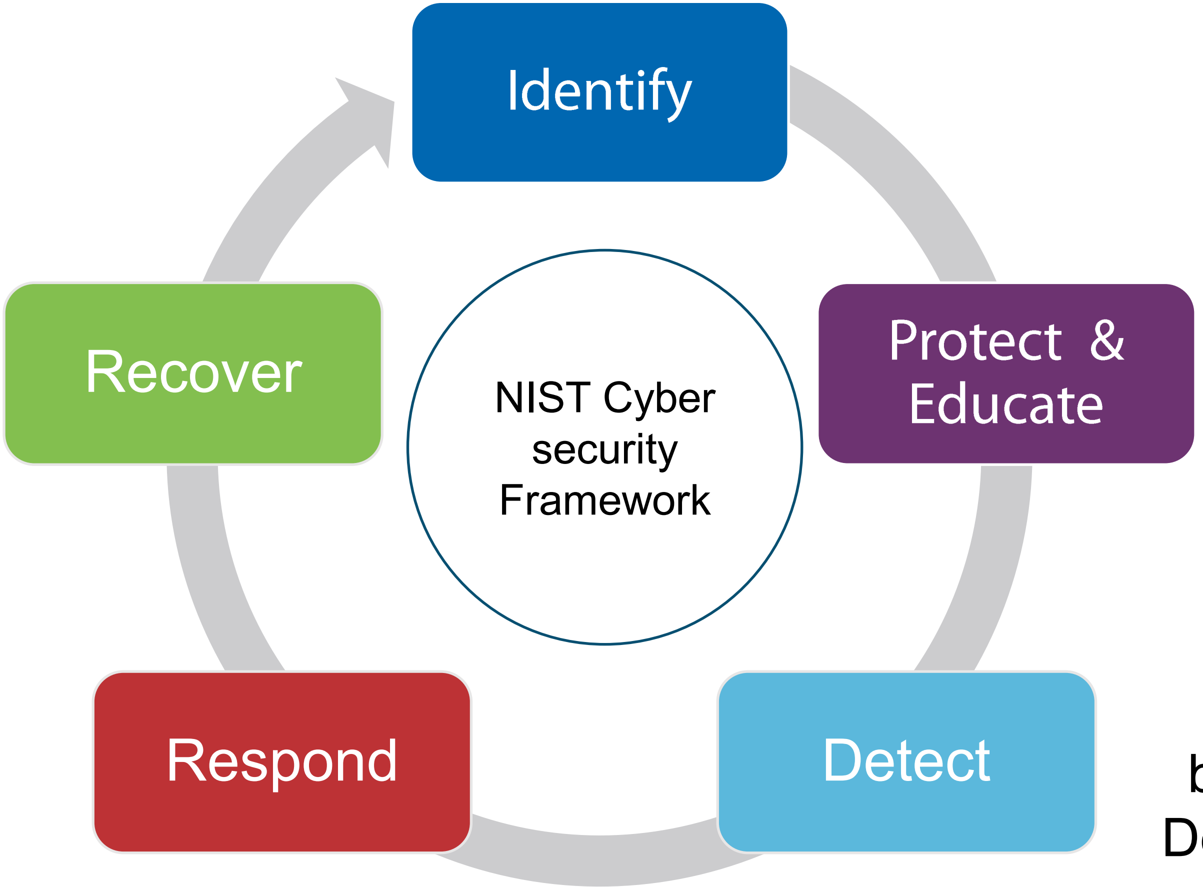
- Provide a Structured approach to Defining Business Drivers, Resource relationships and Process flows
- Ensure that contextual and conceptual elements such as business drivers and consequences are considered at the strategy development stage

Simple definition

- Security Architecture is the Rule book of what is going to help us get to the desired state
- Security Architecture or Security Frameworks help Structure the approach and align back to the business objectives, they are flexible and customizable.
- Examples of frameworks include, Nist CSF, Cobit 5, CIS controls, Iso 27001

Using a Framework in your Business

Assessment & Identify : People, Tech & Tools, Assess Risk



Process & tech to recover data
Backup Disaster recovery

EDR behavior-based AV
Protection Policies
Email Anti Phishing, Awareness training

Threat Isolation, Assessment & Containment.
Incident Response

Monitor Network traffic & behavior with **SIEM + EDR**
Detect hidden compromise & early-stage attacks

SOC : Security trained Staff, Incident Management, Emerging Threat Intel.

Current Security

PREVENT

Firewall

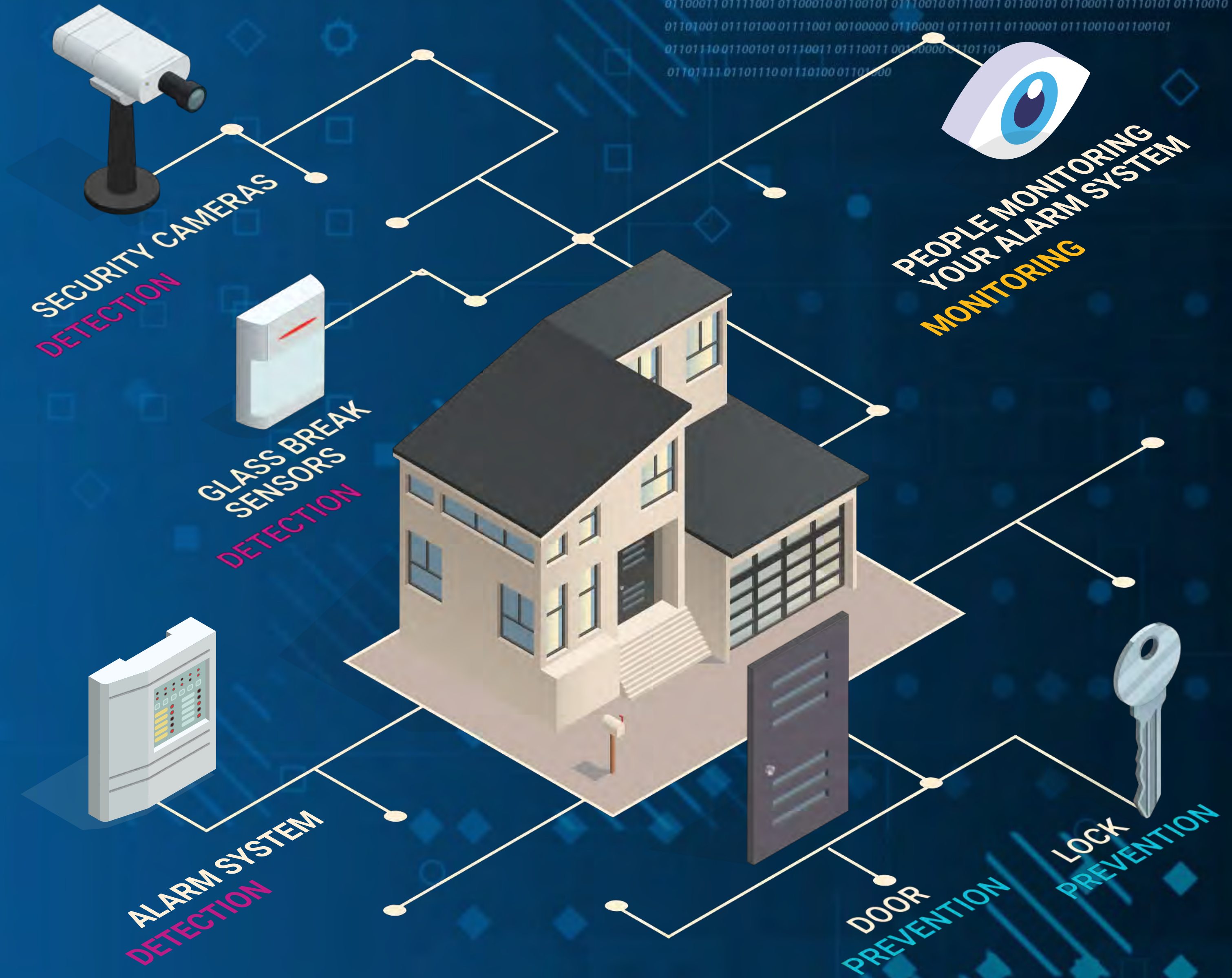
Anti-virus

DETECT

MONITOR

Home Security

PREVENT	Front Door Lock
DETECT	Glass Break Sensors CCTV Cameras Alarm System
MONITOR	Humans keeping watch



Future Security

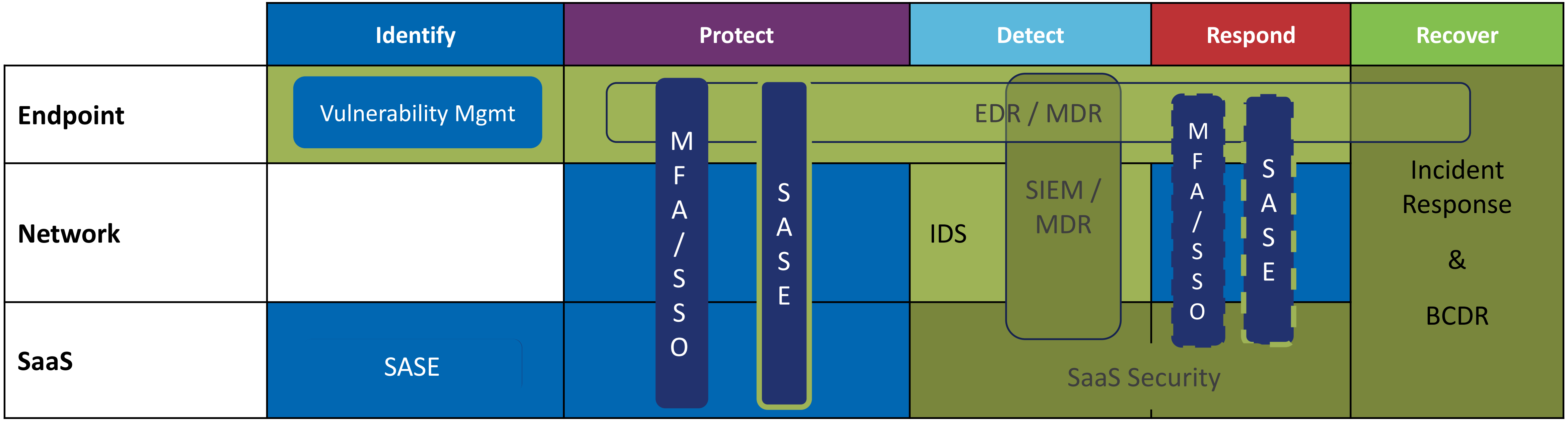
PREVENT	Firewall Anti-virus
DETECT	Detection & Response Platform (SIEM & EDR) Network Sensors Log aggregation (on prem/remote/cloud)
MONITOR	Security Operations Center Threat Hunting Security Research

…and aligning that to a Cyber Defense Matrix

NIST

CONNECTWISE

This can go down into further Layers



CRU & SOC – Changing the Threat Landscape

Out of 133 threat detection signatures and 92 event notifications, we've generated over 3M alerts + 15k escalations

173

MITRE Threats Sightings Reported

96%

Percentage of Alerts Handled By SOC

3M+

Alerts Triaged By CW SOC

4,586

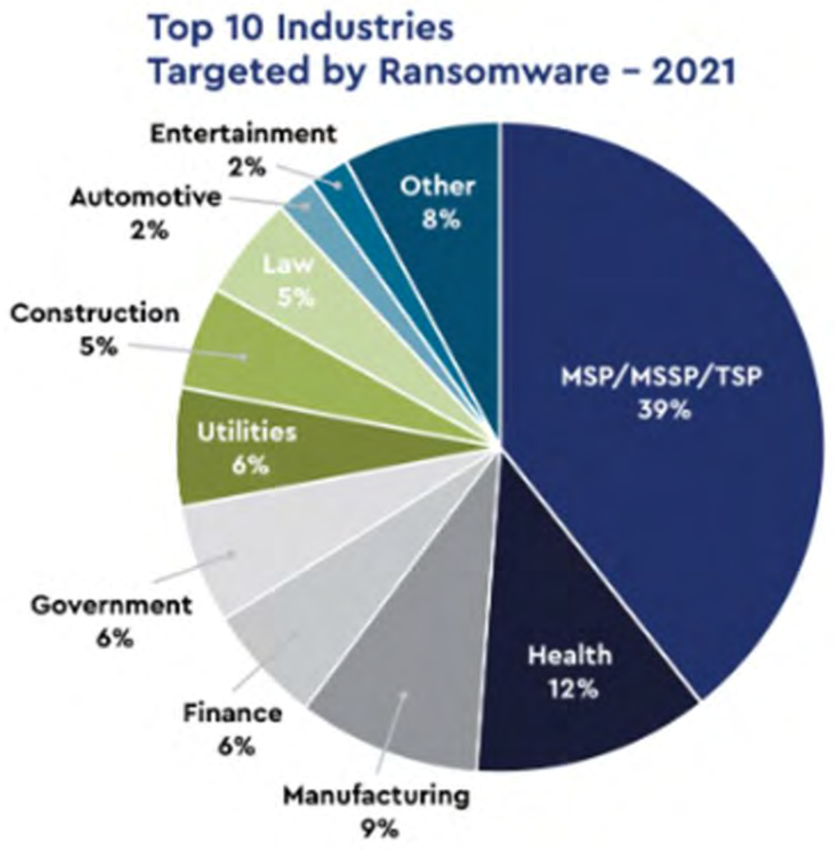
Indicators Added to CRU Threat Feed

**All data based on reports from 2021*

Notable Findings

Throughout 2021, the CRU collected data for 500 cybersecurity incidents from ConnectWise MSP partners and their clients.

- Of those 500 incidents, **40% were related to ransomware**, 25% were directly related to Exchange vulnerabilities, and 10% were coin miners with some overlap.
- Most incidents occurred in Q1 and Q3. There was a **significant increase in ransomware incidents targeting MSPs in the second half of 2021**, with 72% of all ransomware incidents directly targeting MSPs occurring in the second half of 2021.
- We recorded the mass ransomware attacks that happened during the July 2 Kaseya incident as a single incident. This attack targeted at least 40 MSPs and over 1500 of those MSPs' clients, putting MSPs in the spotlight for threat actors, researchers, and government officials alike.

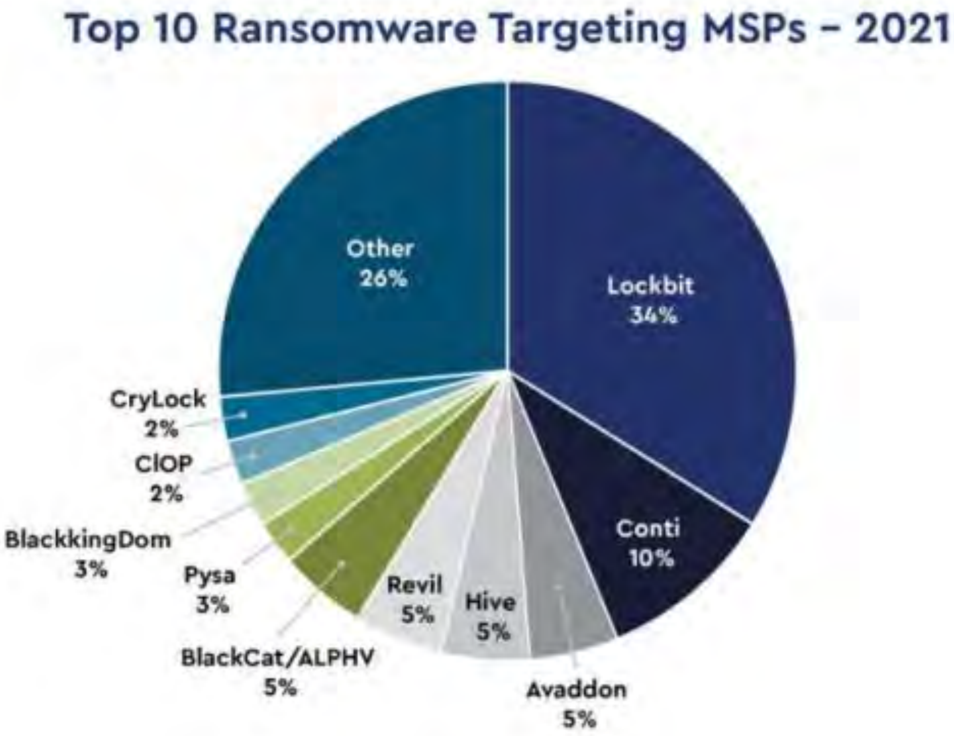


CONNECTWISE

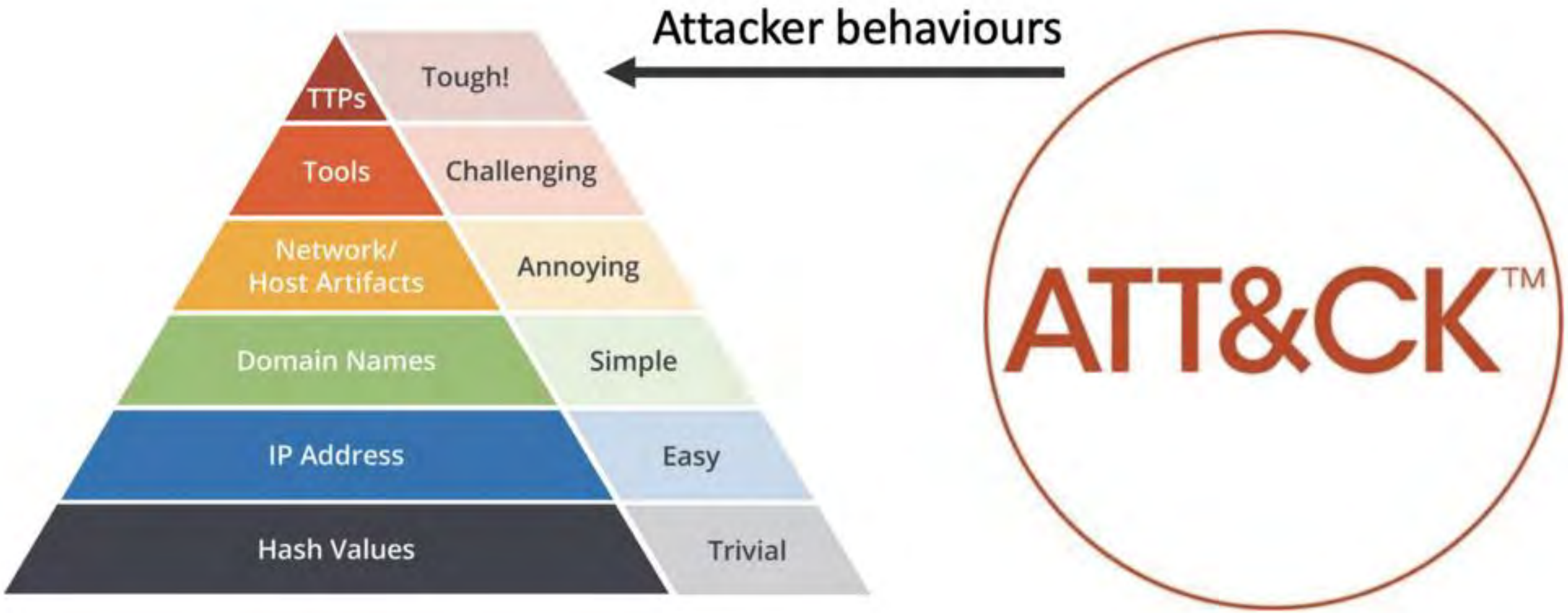
Notable Findings

2021 Top Threat Actor Profiles

Several ransomware groups now see MSPs are prime targets. The CRU gathered information on the top five ransomware groups that are targeting MSPs and their clients. They mapped each group's tactics, techniques, and procedures (TTPs) to the MITRE ATT&CK® framework, a data-driven knowledge base currently used by threat actors. It is a handy tool that provides a common language to describe how threat actors operate. MITRE has also defined common mitigation techniques that defenders can use and mapped these mitigations to each ATT&CK technique and sub-technique. The maps appear in the full report.

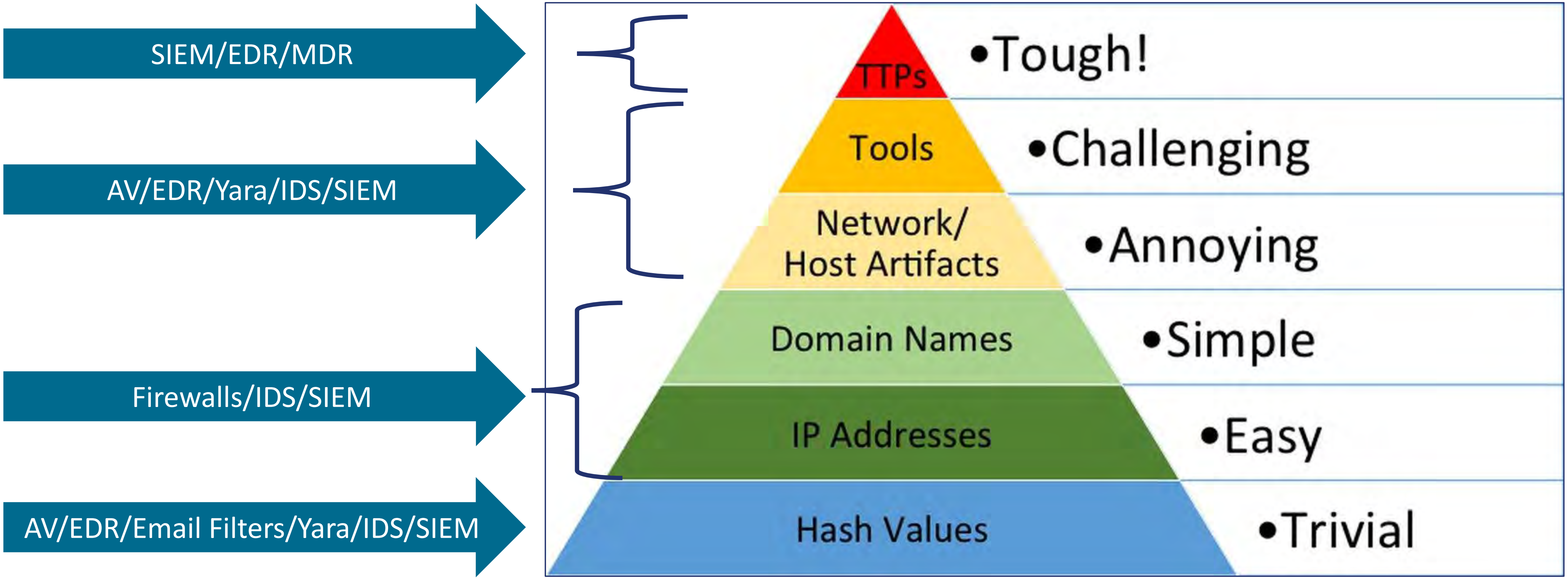


We can fight them with MITRE ATT&CK Framework



Pyramid of Pain

Pyramid of Pain (Detection Tools)



MITRE ATT&CK Framework (TTPs)

Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques
Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services
Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing
External Remote Services	Deploy Container	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer
Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Phishing (3)	Inter-Process Communication (3)	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (6)
Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media
Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create Account (3)	Escape to Host	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools
Trusted Relationship	Serverless Execution	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (7)	Container and Resource Discovery	Taint Shared Content
Valid Accounts (4)	Shared Modules	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)
	Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery	
	System Services (2)	Hijack		Exploitation for Defense Evasion		File and Directory Discovery	
	User Execution (3)			File and Directory Permissions Modification (2)		Group Policy Discovery	
	Windows			Hide Artifacts (10)		Network Service	
				Hijack Execution			

2021 Top Threat Actor Profiles

- TTPs shared by all 5 groups:
  - Initial Access (TA0001)
    - Phishing (T1566)
  - Execution (TA0002)
    - Command and Scripting Interpreter (T1059)
    - Windows Management Instrumentation (T1047)
  - Defense Evasion (TA0005)
    - Obfuscated Files or Information (T1027)
  - Impact (TA0040)
    - Data Encrypted for Impact (T1486)
    - Inhibit System Recovery (T1490)
    - Service Stop (T1489)

Things you can do Today? - Cyber Assessment

Do you understand your cyber risk, and the Assets you need to look after?

Security Frameworks such as NIST, Iso27001, and Cyber essentials aim to provide Guidance and Navigation around Cyber Risk assessment.

Work in partnership with your Technology provider to determine specific risks to your company.

CONNECTWISE