Quorum Cyber

Member of Microsoft Intelligent Security Association

Microsoft

Security Operations

Modernising the approach to defending organisations against cyber attacks

Gold Microsoft Partner

Microsoft

Agenda

What we plan to cover

1.0 Current Trends

Insights into the cyber security threats you need to know

2.0 Cyber Security Strategy

Key Considerations when developing your risk strategy

3.0 How to modernise your Security Operations

Security Capabilities of the Microsoft Ecosystem

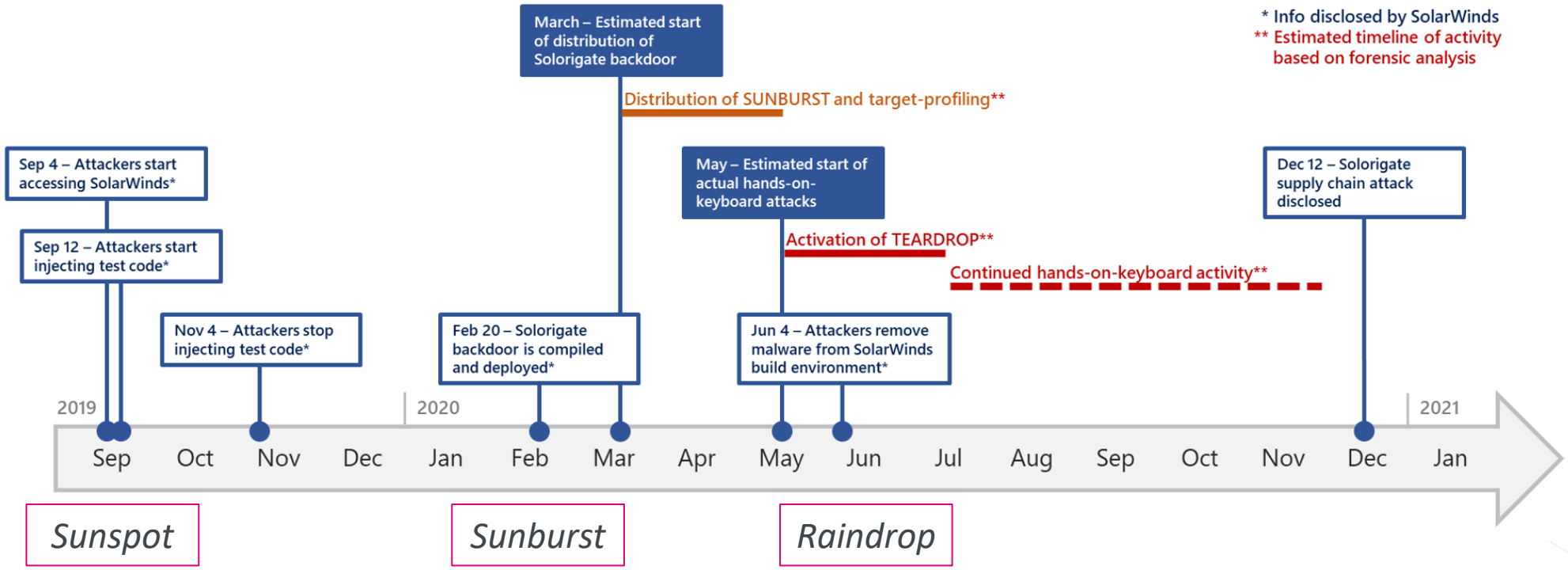
Quorum Cyber

Current Trends

Insights into the cyber security threats you need to know

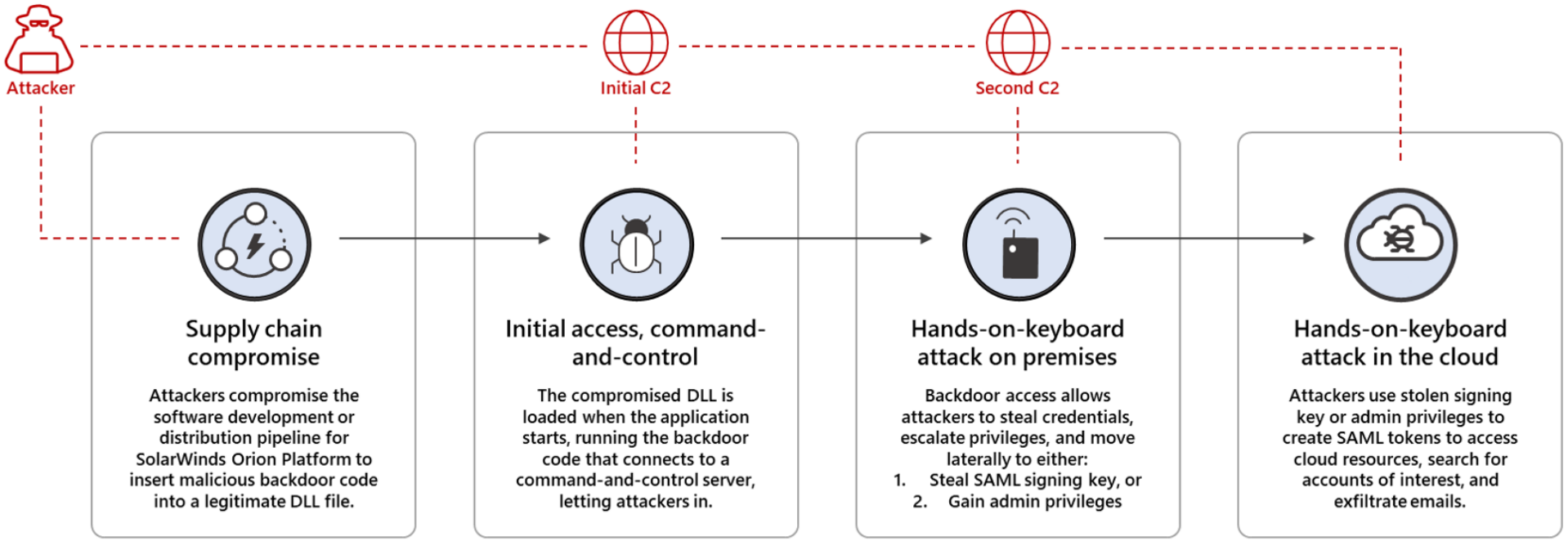
Solorigate

What we know so far



Attack Chain

High-Level View



Targets

Very Selective

- Solorigate backdoor was designed to stay dormant for at least two weeks
- From March to June, the threat actor selected victims and prepared unique Cobalt Strike implants & C2 infrastructure, before removing the malicious code from SolarWinds!
- The C2 infrastructure was hosted in *Avsvmcloud.com*

- It verifies that the process hosting the malicious DLL is named *solarwinds.businesslayerhost.exe*
- It checks that the last write-time of the malicious DLL is at least 12 to 14 days earlier
- It delays execution by random amounts of time
- It verifies that the domain name of the current device meets the following conditions:
  - The domain must not contain certain strings; the check for these strings is implemented via hashes, so at this time the domain names that are block-listed are unknown
  - The domain must not contain “solarwinds”
  - The domain must not match the regular expression *(?i)([^a-z]|^)(test)([^a-z]|$)*, or in simpler terms, it must not look like a test domain
- It checks that there are no running processes related to security-related software (e.g., *Windbg*, *Autoruns*, *Wireshark*)
- It checks that there are no drivers loaded from security-related software (e.g., *groundling32.sys*)
- It checks that the status of certain services belonging to security-related software meets certain conditions (e.g., *windefend*, *sense*, *cavp*)
- It checks that the host “api.solarwinds.com” resolves to an expected IP address

Facilities under attack

When cyber moves into the physical world

- Last week (Feb 2021) a threat actor gained unauthorised remote access (TeamViewer) to a computer for a Florida city's water treatment plant
- The threat actor leveraged the access to increase the amount of sodium hydroxide by 100 times the normal level
- Multiple other controls prevented the water from going into the water supply
- Attribution is key (was it a Nation State? Was it someone who got lucky on Shodan?)

This happened before!

- April and June 2020 – two cyber attacks hit Israel water management system
- The advice was to change passwords "with emphasis on operational systems and chlorine control devices in particular,"
- Attribution: assumed to be Iran
- Two weeks later (May 2020) a cyber attack cripples the Iran port of Shahid Rajaei

Two more cyber-attacks hit Israel's water system | ZDNet

What's most interesting about the Florida water system hack? That we heard about it at all. — Krebs on Security

Key takeaways

Based on the news, based on what we've seen

Supply Chain is the new fools gold

Expect lots of silver bullets and "experts" making investment recommendations > instead focus on Privileged Accounts

Remote access is a very real risk

We've seen a dramatic increase – over 50% of the incidents we've participated in abuse valid remote access

You are most vulnerable during adoption and transition to Cloud

Hybrid deployments are doubling your threat surface, an on-prem compromise can lead to a cloud compromise

Quorum Cyber

Cyber Security Strategy

Key Considerations when developing your risk strategy

The Fear Factor

The force continues to be strong

- Evil hackers are coming to get you
- You are probably already hacked
- This is too difficult for you to fix
- You will never understand this… so just trust our marketing!

Shiny Toy Syndrome

One myth to rule them all

- Do you even multi cloud, bro?
- *All your XDR is belong to us*
- ”good” security = £££
- Next-Gen Hyper-Converged AI powered Machine Learning Blockchain secured robots will save the world

Key insights

Conversations we have regularly

Time to evolve the “Defence In Depth” paradigm to include “Defence In Breadth”

Focus on visibility across dimensions including identities, endpoints, networks, cloud, and data.

Focus on vendors with good coverage to reduce overhead and increase integration.

Zero Trust and Assume Breach are key components.

The Simon Sinek approach – Start with “why”

Think of “threats” that can materialise the risks you care about (not in a vacuum)

Prioritise threats that lead to really bad days for the business, not for IT

Action focused design

How are we going to respond to the “output” of each control (feed data to an action centre)

Effective, Efficient and Elegant

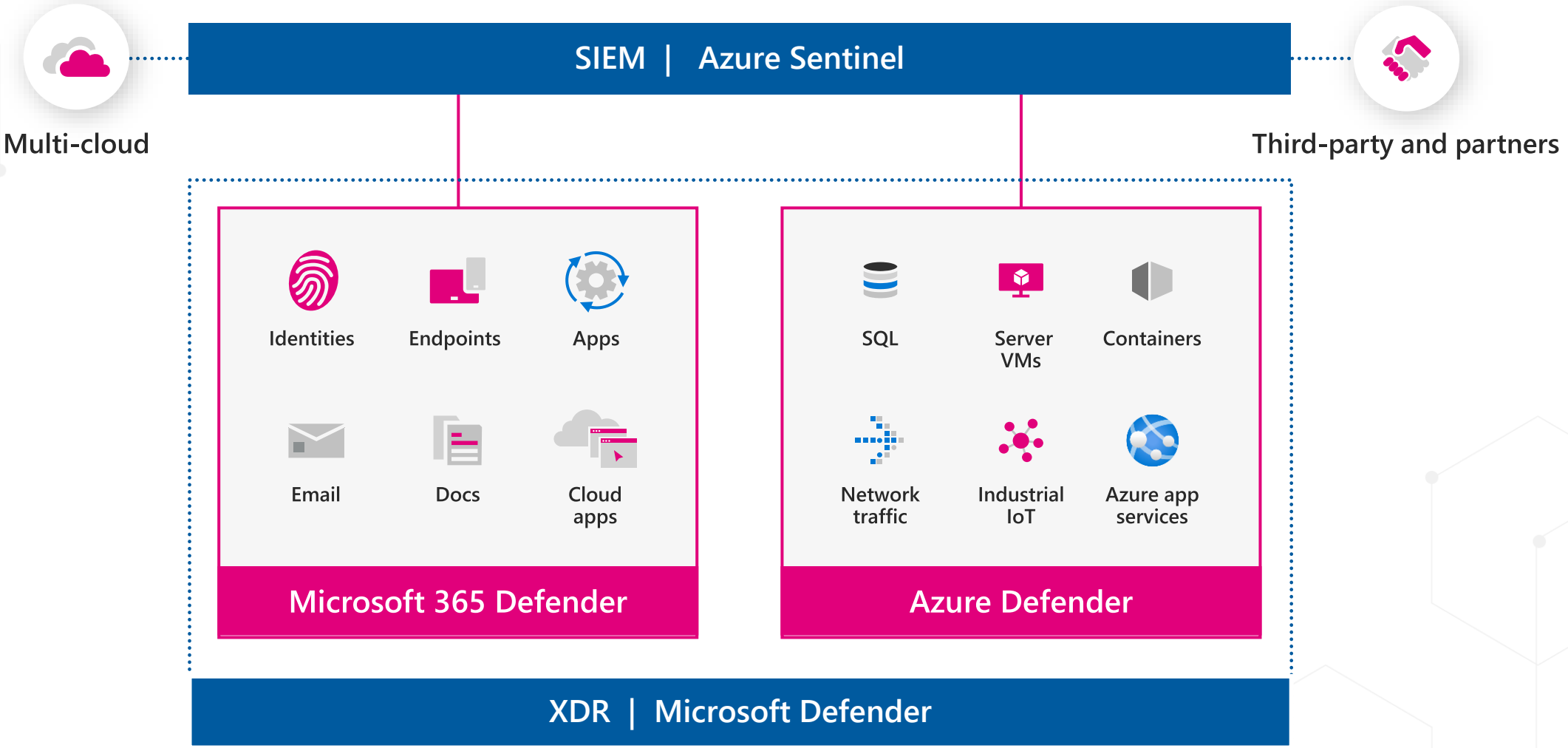
[Using Zero Trust principles to protect against sophisticated attacks like Solorigate - Microsoft Security]

Quorum Cyber

How to modernise your Security Operations

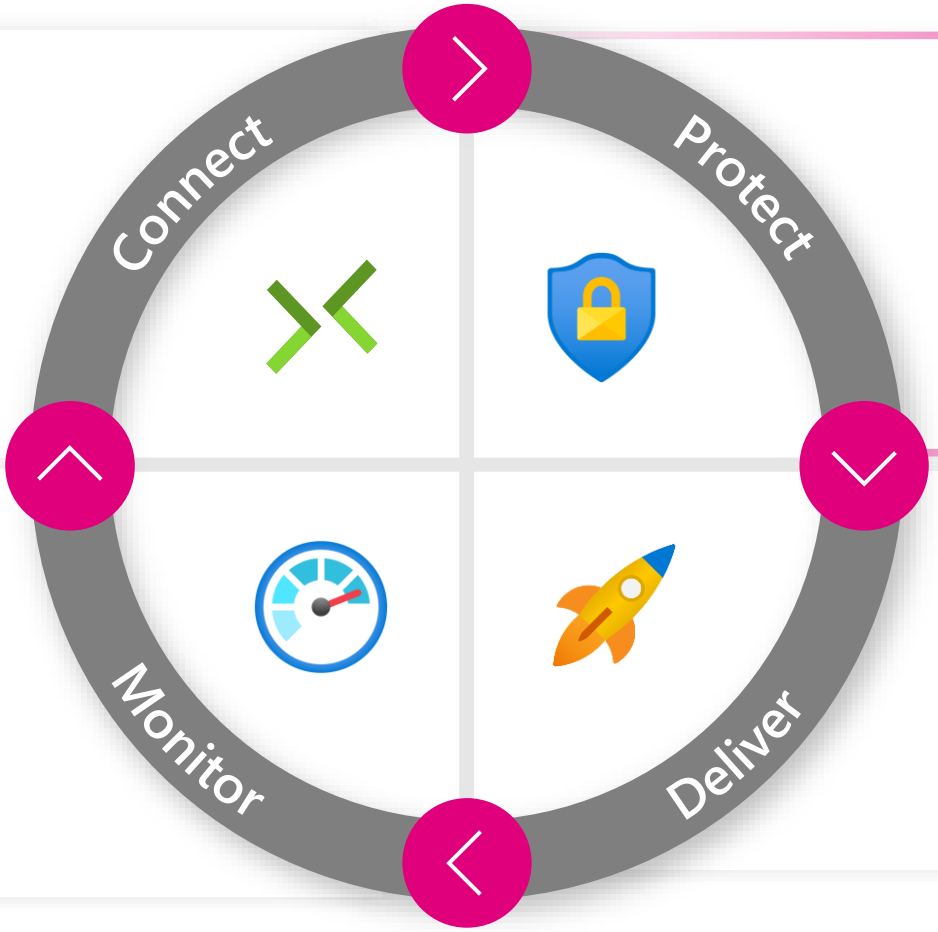
Unleashing the power of the Microsoft Ecosystem

A unified SecOps Ecosystems



Extending the field of view

Virtual Network
Virtual WAN
ExpressRoute
VPN
DNS



DDoS Protection
Azure WAF
Azure Firewall
Azure Firewall Manager
Network Security Groups
Service Endpoints/Private Link

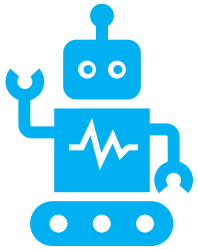
Network Watcher
ExpressRoute Monitor
Azure Monitor
Virtual Network TAP

CDN
Front Door
Traffic Manager
Application Gateway
Load Balancer

The fundamentals to SecOps

SecOps

Unified Technology Ecosystem



Focused on integration and automation as force multipliers

Empowering people to be creative and efficient

Quorum Cyber

Demo Time!

Azure Sentinel

Quorum Cyber

We help good people win