Microsoft

Simplifying advanced security technology

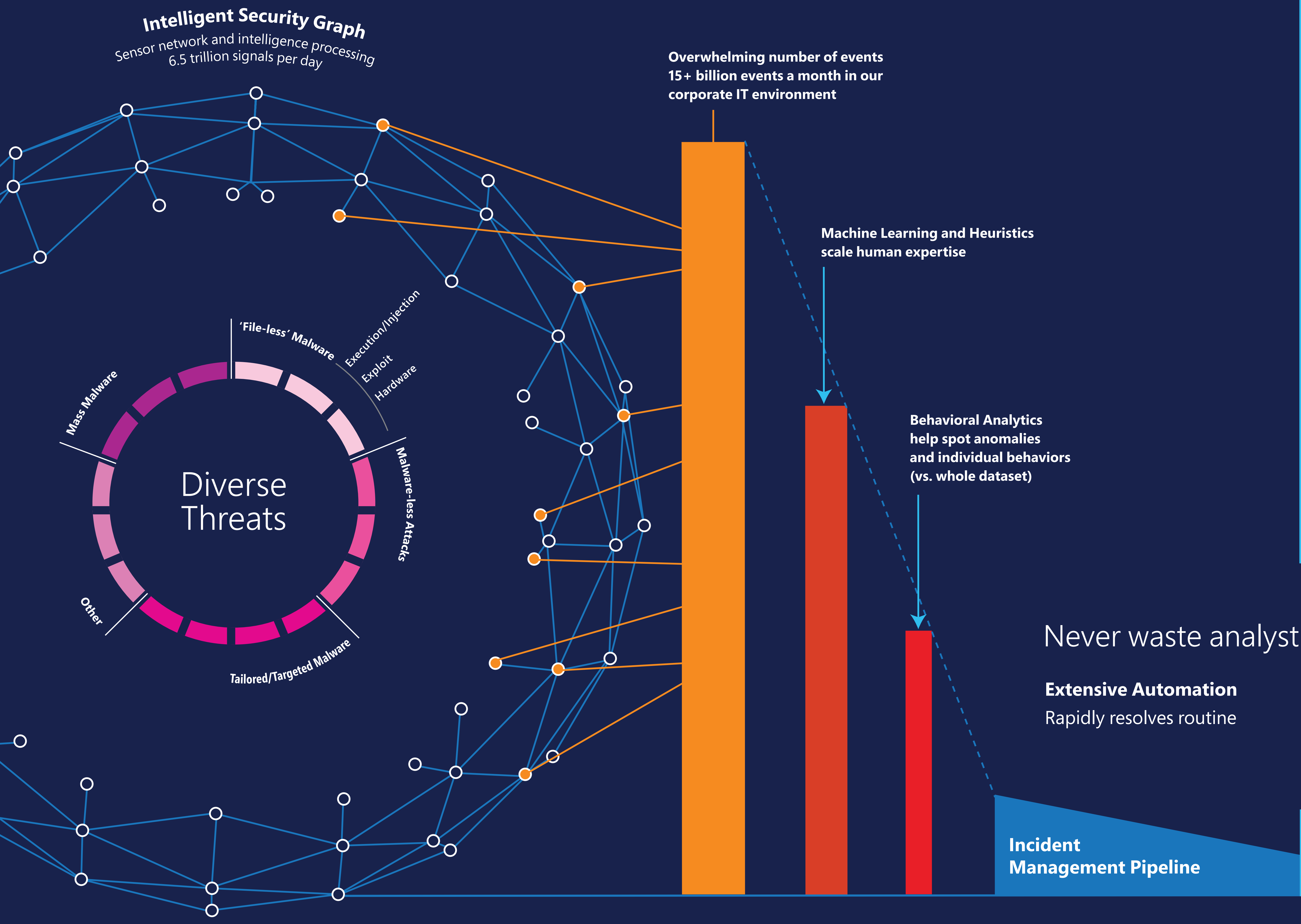
Microsoft Cybersecurity Solutions Group
aka.ms/minutesmatter

Minutes matter.

In cybersecurity, the time of experts is the scarcest resource

Security Operations Centers (SOCs) must be fast and accurate

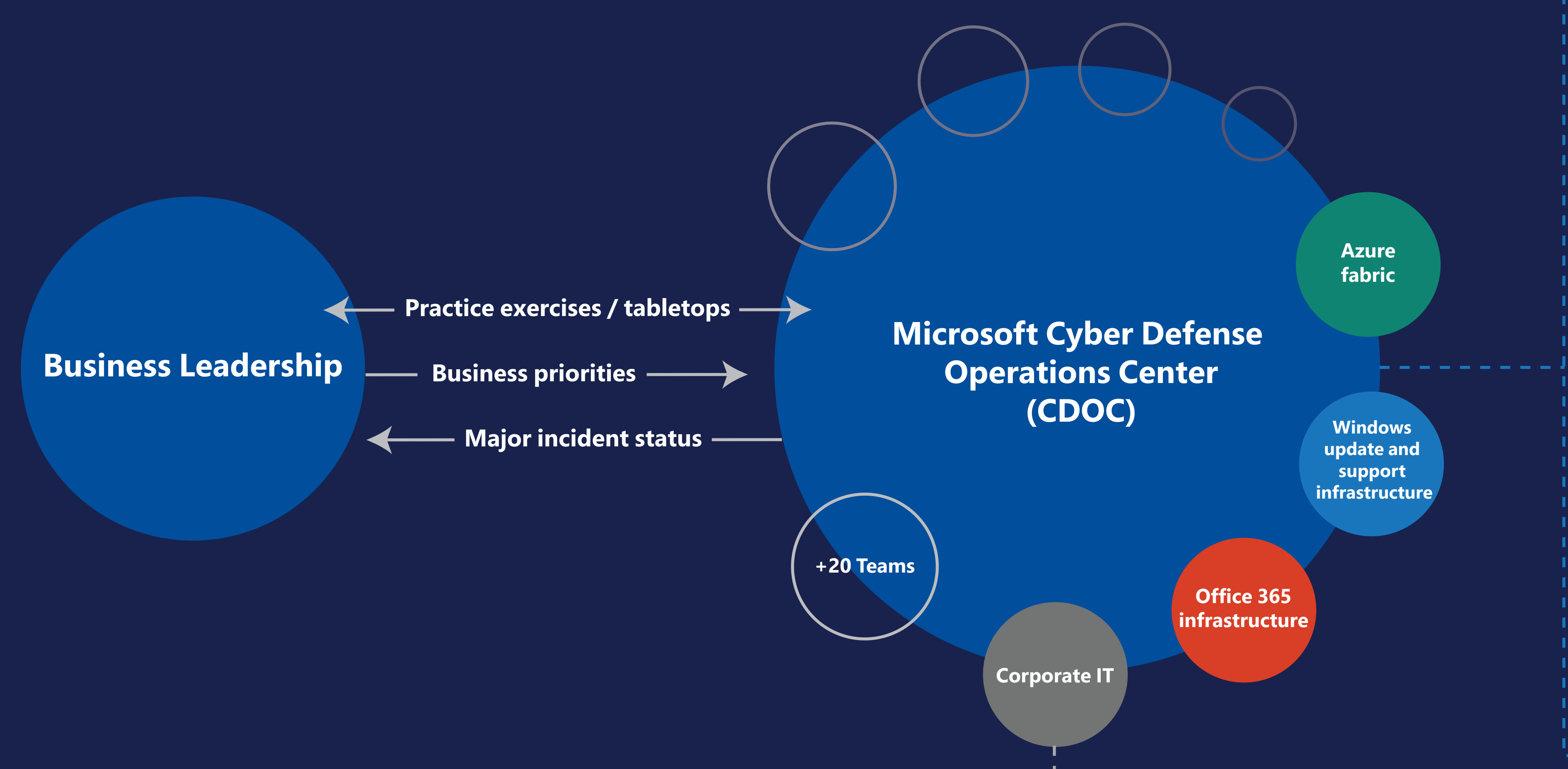
Adversaries present a danger every minute they are in your environment, but it is challenging to rapidly detect their activity among billions of events. Microsoft's approach combines human expertise, extensive telemetry, and advanced analytics.


Intelligent Security Graph
Sensor network and intelligence processing
6.5 trillion signals per day
Diverse Threats
'File-less' Malware
Execution/Injection
Exploit
Hardware
Malware-less Attacks
Tailored/Targeted Malware
Other
Mass Malware
Overwhelming number of events
15+ billion events a month in our corporate IT environment
Machine Learning and Heuristics scale human expertise
Behavioral Analytics help spot anomalies and individual behaviors (vs. whole dataset)
Incident Management Pipeline

Protect. Detect. Respond.

Fusion center model of Cyber Defense Operations Center (CDOC)

Microsoft utilizes a fusion center model to bring together our Security Operations Center (SOC) teams in shared facilities. While not needed for all organizations, this approach helps us maintain deep specialization while sharing situational awareness and subject matter expertise across teams.


Business Leadership
Practice exercises / tabletops
Business priorities
Major incident status
Microsoft Cyber Defense Operations Center (CDOC)
Azure fabric
Windows update and support infrastructure
Office 365 infrastructure
Corporate IT
+20 Teams

Red vs. Blue

We operate several full-time Red teams that mimic behavior of determined adversaries to test our security against realistic attack methods (in addition to penetration tests).

Purple Teaming

To increase fidelity of both Red and Blue team learning, we regularly conduct activities where Red and Blue teams operate against each other in the same room.

Never waste analyst time:

Extensive Automation
Rapidly resolves routine

Alert quality is critical
Corporate IT SOC requires 90%+ true positive for alerts requiring analyst response

Track Responsiveness and Resolution Time

Time to acknowledge

Time to remediate

Corporate IT defense

Learnings and recommended practices from Digital Security and Risk Engineering (DSRE) SOC

The enterprise IT SOC mission always comes first when selecting tools. Microsoft security capabilities have replaced many third-party tools by:

- Reducing investigation time for common incidents from hours to minutes
- Increasing analyst productivity by reducing false positives and integrating solutions
- Meeting scalability needs of environments using the cloud services model
- Manage cloud and on-premises assets as a single hybrid enterprise
- Focus on signal diversity for intelligence to provide critical insights across endpoint, identity, email, network, and more

Key observations

Attackers think in graphs (interconnecting access paths), so defenders need to see their environment this way too

Cloud-scale tools handle most enterprise IT SOC needs (though specialized tools can supplement as needed)

SOC tooling

SIEM + SOAR as a Service
Azure Sentinel

ENDPOINT – Windows Defender ATP Endpoint Detection & Response (EDR)

IDENTITY – Azure ATP + Azure AD Identity Protection

SaaS – Office 365 Advanced Threat Protection (ATP) + Cloud App Security

AZURE ASSETS – Azure Security Center

NETWORK – 3rd party Logs and Tools

SERVERS – 3rd party and Microsoft Logs and Tools

OTHERS – 3rd party and Microsoft Logs and Tools

Custom &
3rd Party tools
(as needed)

Built on Azure Monitor, Logic Apps, and Microsoft's UEBA/ML Technology

Tiers

TIER 3
Proactive Hunting and Advanced Forensics
Any/All tools, data, intelligence sources

TIER 2
Advanced Analysis and Remediation
Primary Tools: Microsoft Threat Protection

Special Cases
High Value Assets
Campaign Monitoring

TIER 1
High Speed Remediation
Primary Tools: Microsoft Threat Protection

Default Alert Path
Alerts from MTP tools (~65%)
User Reporting (~10%)
Log/Event/Other (~25%)

AUTOMATION
Automated Investigation & Remediation

Well known attacks
Microsoft Threat Protection (MTP) Alerts

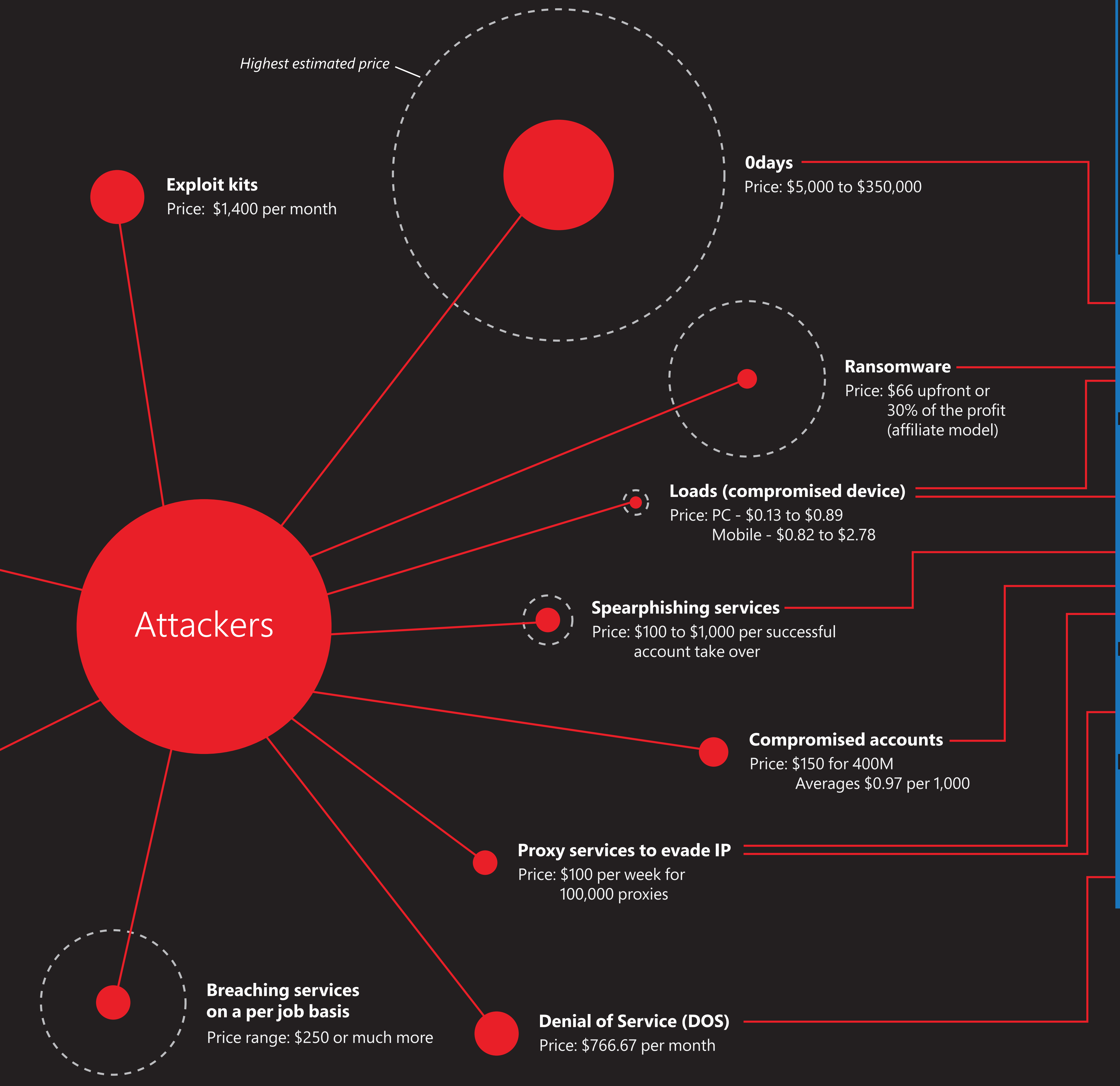
Microsoft

Microsoft Cybersecurity Solutions Group
aka.ms/motivationmatters

Motivation matters.

Understanding attacker motivations is key to disrupting attacks and defending your assets

Dark Market Products are notably inexpensive with a few exceptions (like zero days).



Exploit kits
Price: $1,400 per month

0days
Price: $5,000 to $350,000

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

Loads (compromised device)
Price: PC - $0.13 to $0.89
Mobile - $0.82 to $2.78

Spearphishing services
Price: $100 to $1,000 per successful account take over

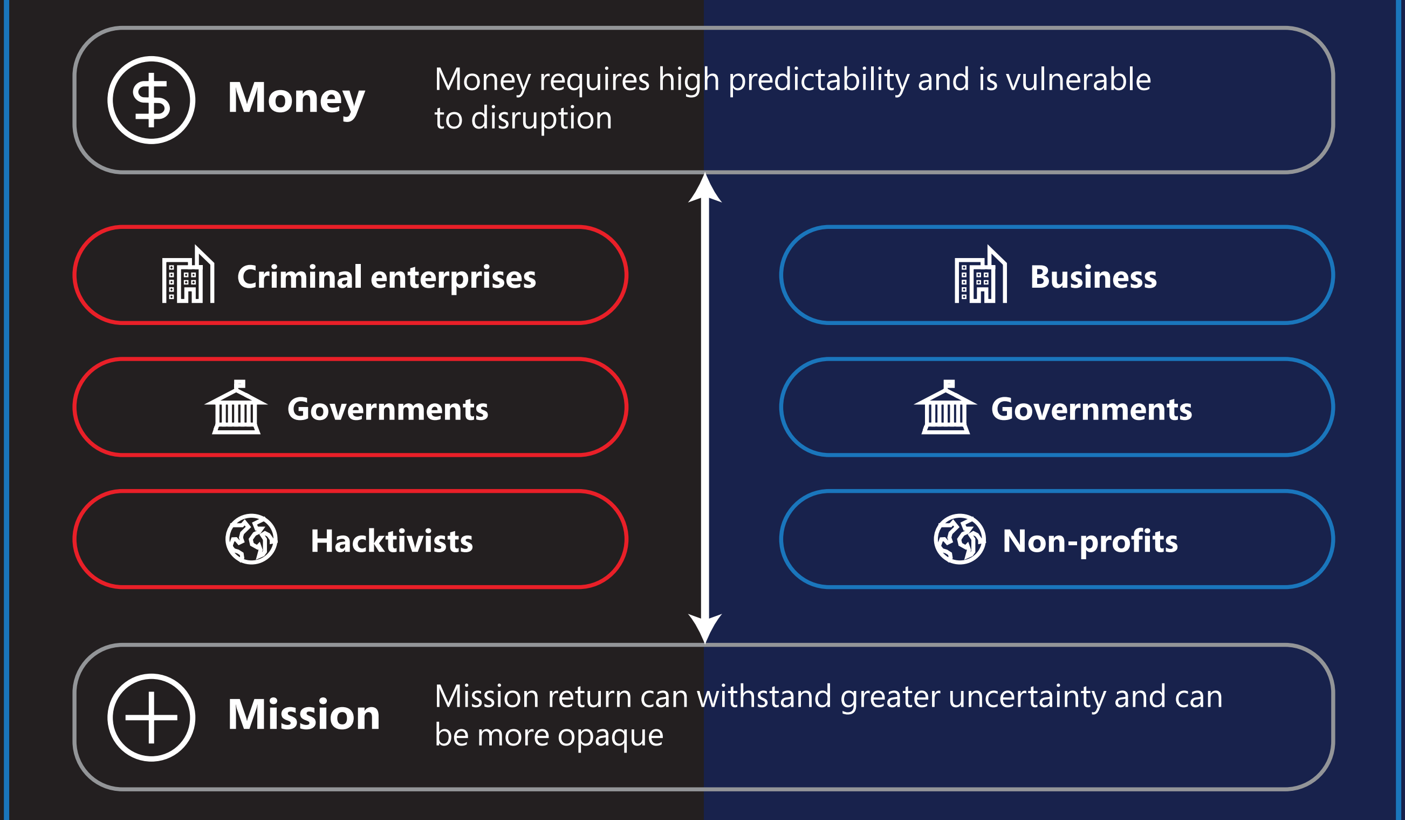
Compromised accounts
Price: $150 for 400M
Averages $0.97 per 1,000

Proxy services to evade IP
Price: $100 per week for 100,000 proxies

Breaching services on a per job basis
Price range: $250 or much more

Denial of Service (DOS)
Price: $766.67 per month

Disruption strategies differ



Money Money requires high predictability and is vulnerable to disruption

Mission Mission return can withstand greater uncertainty and can be more opaque

Recommended strategies

Prioritize hygiene over ‘zero day’ defenses
Zero day vulnerabilities are expensive and impractical for many attacks. Focus first on critical security hygiene like rapidly applying security updates/patches (which have much lower cost to attackers). Microsoft built prioritization guidance with NIST + CIS + DHS NCCIC:
aka.ms/cyberhygiene

Shift from network to Zero Trust strategies
While network controls are required for some attacks, adversaries have proven capable at evading them. You should begin aggressively modernizing your strategy with a modern identity-based perimeter composed of:

- Endpoint and identity security capabilities as the front line
- Data centric security that prioritizes highest value assets
- Application / SaaS protections
- Centralized access control (such as Microsoft's Conditional Access)

aka.ms/zerotrustsecurity

Limit efforts to restrict traffic by geography
Blocking IP addresses by geography (e.g. hostile countries) can be easily and cheaply evaded, so focus your security efforts elsewhere.

Denial of Service protection for critical services
Distributed Denial of Service (DDoS) attacks are a cheap commodity and are sometimes used as a distraction from a “real” targeted attack. You should ensure that your critical services have DDoS protection from Azure platform or a capable 3rd party.
aka.ms/ddosprotection

Microsoft Digital Crimes Unit (DCU)

DCU is leading the fight against cybercrime to protect our customers and promote trust in Microsoft. We fight cybercrime globally through the innovative application of technology, forensics, civil actions, criminal referrals, and public/private partnerships while committed to protecting the security and privacy of our customers.

Leading the fight against cybercrime

DCU focuses on disrupting cybercrime through civil actions and referrals to law enforcement so that criminals are held accountable and our customers are protected. Information uncovered during our investigations is also used in technical countermeasures and Microsoft product improvements. Our focus areas are:

Cloud Crime and Malware – Applying unique legal and technical solutions to investigate and disrupt malware facilitated cybercrime and nation-state sponsored activity targeting our customers and cloud services.

Global Strategic Enforcement – Driving enforcement actions against global online criminal networks who specialize in business email compromise, credential misuse, online fraud, and intellectual property theft with a focus on protecting customer security.

Tech Support Fraud – Leveraging data analytics and machine learning to tackle one of the most significant global cybercrimes through investigations and enforcement, technological disruptions and education.

Online Child Exploitation – Building on our legacy of PhotoDNA to prevent and deter the distribution of online child sexual abuse material to better protect customers and stop revictimization of some of the most vulnerable.

You face an ecosystem, not just individual attackers

⇄ Dark Markets are the criminal forums where a wide range of attack tools, services, and data are traded. This is an industrialized economy with specialization of skills, products, services, and profit models. The attackers you face are very likely to utilize these markets as they prepare their attack campaigns.