protiviti®

Face the Future with Confidence

EMERGING CYBER TRENDS AND THREATS

April 2019

Internal Audit, Risk, Business & Technology Consulting

TOC

BACKGROUND

Daniel Jacobson

Associate Director, Protiviti

daniel.jacobson@protiviti.com

Background

- Daniel leads our S. Florida Information, Cybersecurity & Privacy practice. Daniel has a strong background with years of experience providing both audit and regulatory compliance services as well as general consultative and project based information security engagements focusing on assessment and validation as well as strategy and program execution.
- Daniel manages IT Consulting projects including security strategy and roadmap assessments, penetration testing, vulnerability assessments, security architecture reviews, and wireless assessments. Daniel is a member of the Protiviti National Information Security Practice.

Professional Certifications

Payment Card Industry Qualified Security Assessor (PCI-QSA)

Certified Information Systems Security Professional (CISSP)

CISA, CISM, CRISC

Jonathan Trillos

Senior Manager, Protiviti
jonathan.trillos@protiviti.com

Background

- On a day-to-day basis, Jonathan manages information security projects that include vulnerability assessments, network and wireless security assessments, security architecture reviews, and mobile device security reviews.
- Jonathan serves clients in industries that include communications, banking, financial services, consumer products, retail, technology, real estate, healthcare and hospitality. And many of his engagements relate to SOX, HIPAA, and GLBA compliance requirements.

Professional Certifications

Payment Card Industry Qualified Security Assessor (PCI-QSA)

Certified Information Systems Security Professional (CISSP)

Certified Information Systems Auditor (CISA)

EMERGING CYBER TRENDS

DATA BREACH STATISTICS (1/2)

The Reality of Data Breaches

Data Records Lost or Stolen Since 2013

14,717,618,286

ONLY **4%** of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

6,446,613 records lost or stolen **every day**

268,609 records **every hour**

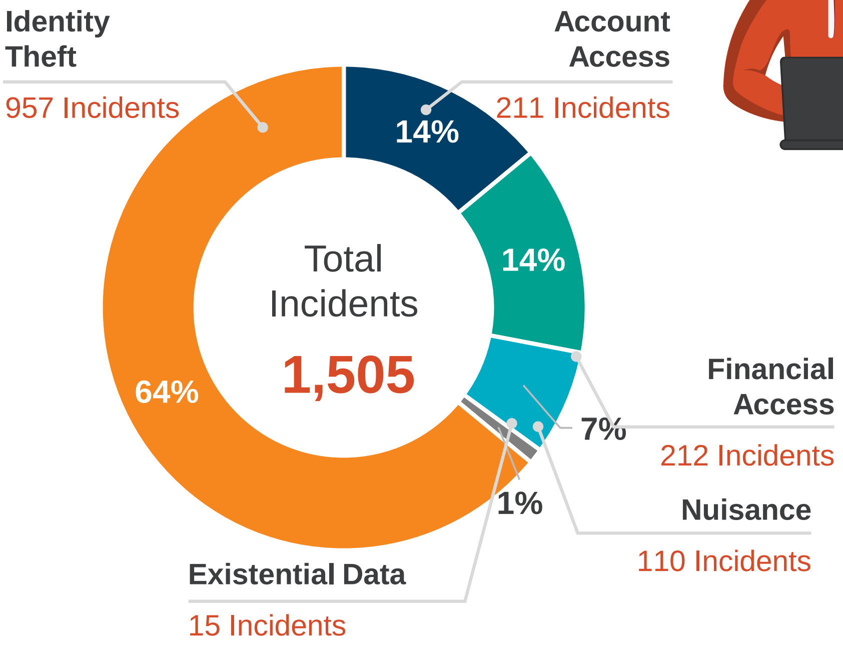
4,477 records **every minute**

75 records **every second**

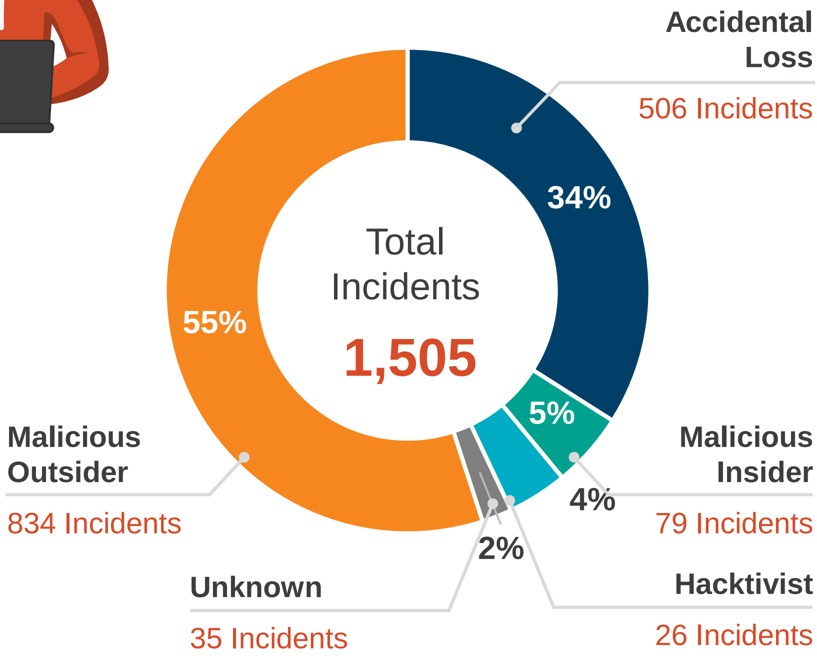
Source: Breach Index Level

DATA BREACH STATISTICS(2/2)

Number of Breach Incidents by Type



Number of Breach Incidents by Source



Source: Breach Index Level

THE CYBERSECURITY IMPERATIVE

Digital Transformation

The speed of digital transformation is heightening cyber-risks for companies as they embrace new technologies, adopt open platforms, and tap ecosystems of partners and suppliers.

Digital Backlash

Cybersecurity is further complicated by the "digital backlash". When digital transformation outpaces cybersecurity progress, companies bear a bigger chance of suffering a major cyber-attack (over $1m in losses).

General Staff

While companies see high risks from external threat actors, such as unsophisticated hackers, cyber criminals, and social engineers, the great danger, cited by 9 out of 10 firms, lies with untrained general (non-IT) staff.

Partners and Vendors

More than half of companies see data sharing with partners and vendors as their main IT vulnerability.

Investments

To cope with rising risks, companies upped their cybersecurity investment by 7% over the last year and plan a 13% boost next year.

Budget

Next year, companies will allocate 39% of their cybersecurity budget to technology, 31% to process, and 30% to people. Firms now use a variety of technologies, from MFA (90%) and blockchain (68%) to IoT (62%) and AI (44%).

Investment Trend

Companies are now investing more in cyber-risk prevention/detection than in resilience.

Cyber-attack Probability

As cybersecurity systems mature, the probability of costly cyberattacks declines. Cybersecurity beginners have a 21.1% probability of a cyberattack generating over $1m in losses vs. 16.1% for intermediates and 15.6% for leaders.

Technology Staff

As firms move up the cybersecurity maturity curve, the ratio of cybersecurity to technology staff drops.

ROI

Calculating the ROI of cybersecurity is elusive for most firms. One stumbling block is that companies often do not measure indirect costs, such as productivity loss, reputational damage which can seriously hurt bottom lines.

Source: Protiviti.com

ARTIFICIAL INTELLIGENCE IMPACT ON CYBER (1/2)

The Impact of AI and ML

- The past five years have seen a tremendous rise in the use of AI and ML technologies for enterprises. Organizations are already beginning to use AI to bolster cyber security and offer more protection against sophisticated hackers. AI helps by automating complex processes for detecting attacks and reacting to breaches.
- Data deception technology products can automatically detect, analyze and defend systems against advanced attacks by proactively detecting attackers. So, when one combines security personnel with adaptive technology that continues to change and become smarter over time, it provides a competitive edge to defenders that has till now been absent from most cyber security technologies.
- Fast detection of attacks and limiting their spread is what only AI and its algorithms as well as datasets can do. According to Steve Grobman, chief technology officer for McAfee, AI will be the cornerstone of tomorrow's cyber defense.

29%

want to use AI-based cybersecurity technology to accelerate incident detection.

27%

want to use AI-based cybersecurity technology to accelerate incident response.

24%

want to use AI-based cybersecurity technology to help their organization better identify and communicate risk to the business.

22%

want to use AI-based cybersecurity technology to gain a better understanding of cybersecurity situational awareness.

Source: OpenSourceForU, The Guardian, CSO Online

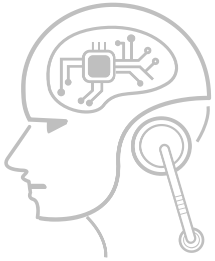
ESG research provided the above statistics.

- Dmitri Alperovitch, the co-founder of information security firm CrowdStrike, said:
- "There are going to be improvements on both sides; this is an ongoing arms race. AI is going to be extremely beneficial, and already is, to the field of cybersecurity. It's also going to be beneficial to criminals. It remains to be seen which side is going to benefit from it more.
- "My prediction is it's going to be more beneficial to the defensive side, because where AI shines is in massive data collection, which applies more to the defense than offence."

ARTIFICIAL INTELLIGENCE IMPACT ON CYBER (2/2)

The Flip Side of Artificial Intelligence

- One of the most serious threats organizations face in 2018 and beyond is malware with the capability to learn and grow through its own successes.
- Nextgen AI-generated malware will be aware and capable of adapting itself.
- Instead of simply following a set of pre-programmed instructions, it will select targets of opportunity, assess their weaknesses, develop a plan of attack and cover its tracks.
- Hostile AI will be extremely dedicated to exploration, finding weaknesses at every possible crease in the network perimeter. Without any need for operator intervention, it will be able to fully map targets, design and deploy exploits, and even collect (and spend) ransoms.



Future AI Based Cyberattacks Landscape

The hivenet is frightening because each unit of the hivenet, **a swarmbot**, will itself be powered by AI. Swarmbots will be able to make autonomous decisions without relying on a botnet herder and join together into larger autonomous thinking networks. The potential for hivenet damage is substantially greater than anything world has faced from already-potent botnets.

Polymorphic malware with pre-coded algorithms designed to subvert countermeasures and screens is already a reality. This approach simply generates millions of slight variations on the same theme.

Machine learning has proven effective in sandbox environments at exploring potential vulnerabilities and devising defenses.

At a recent cybersecurity conference, **62 industry professionals**, out of the 100 questioned, said they thought the first **AI-enhanced cyberattack could come in the next 12 months.**

Wired magazine is warning that hackers are on the brink of **launching a wave of AI powered** cyberattacks and also that AI powered cyberattacks against humans will be almost impossible to stop.

Google has created a non-traditional security group called "**AI Fight Club**" for deterrence and to train systems to more effectively combat harmful AI.

Source: Medium, The Conversation, Fortinet, Ipswitch

EMERGING CYBER THREATS

INTERNET OF THINGS (IOT) ATTACKS

IoT and Chip Processors are Emerging Battlegrounds

- Since the unwelcomed and unexpected appearance of Mirai and related DDoS attacks in September 2016, the IoT space has been highly active.
- IoT-connected devices, such as smart refrigerators, webcams, TiVos and Smart TVs are more vulnerable to attacks, and have already been exploited for use in botnets, but Ipswitch predicts that they will be targeted more often in ransomware attacks, and in 2019, there will be larger-scale attacks against infrastructure and IoT security.
- In January 2018, a processor vulnerability, known as Meltdown, was published by Google's Project Zero security team. Variants of this issue are known to affect many modern processors. A successful exploit of this vulnerability could allow an attacker to access sensitive information (e.g., passwords, emails) inside protected memory regions on modern processors.

IoT Cyberattacks

The most high-profile evolution of **Mirai is IoT Reaper**. This variant doesn't leverage weak password policies like Mirai, but rather exploits **nine vulnerabilities in various IoT devices**.

As an example, IoT Reaper, a type of Trojan, integrated **LUA** execution environments for more complex attacks.

From a manufacturing perspective IoT has also impact **on operations technology (OT).**

According to Cisco 2018 Cybersecurity Report, **31%** of security professionals said their organizations have already experienced cyber-attacks on OT infrastructure.

Rapid proliferation of Internet of Things devices in advance of IoT-oriented security standards and configuration practices, expect these devices to be increasingly used as weapons for **DDoS** and other attacks.

According to SonicWall, **Home-based IoT attacks** will lead headlines as they begin to threaten average citizens' privacy, information and identities.

The top three botnet kits are responsible for infecting over **1 million** devices per month according to CSO.

Source: SonicWall, Ipswitch, Sandiego.edu, Cisco

ATM ATTACKS

ATM “Jackpotting”

- Hackers have been draining ATMs of cash across Europe after compromising the networks of banks and planting malicious software on the **machines, the security company Group-IB says. The Cobalt group is believed to have stolen more than $25 million from banks**, Group-IB says.
- If the ATM is running off the malware-infected hard drive, it can be remotely controlled to dispense cash on demand.
- While these physical ATM attacks have been happening in Europe and Asia since 2012, **they are new to the U.S. as of 2018.**

Malware-only ATM Attacks

- In addition to the black-box “jackpotting” schemes, which require internal, physical access to internals to the ATM itself, there have also been network-based ATM attacks in other parts of the world since 2016.
- In general, the attackers were able to gain access to a bank’s internal network through the usual probing mechanisms (spear phishing, social engineering, etc.), and then navigate the bank’s internal networks to deploy malware out to the ATMs.
- The cyber-criminals could then remotely control the infected ATM to dispense cash on demand. This style of ATM attack has not hit the U.S. yet, but it is an emerging threat financial services’ senior management needs to be aware of.

Solution

- To prevent network-based attacks on ATMs, however, network segmentation would be part of a good strategy.
- It is important to ensure that only legitimate traffic can pass through to critical resources anywhere in the environment. In this case, organizations want to separate their ATM network from the rest of the corporate IT network, which reduces the risk to that portion of the environment.

Source: Security Roundtable, Bank of Security

OTHER CYBERSECURITY EMERGING THREATS (1/2)

Type	Description
Advanced Phishing	• It is becoming harder to distinguish the authentic communication from the malicious. Phishing has been purported as one of the greatest risks to system integrity. • An example is **spear phishing**, which uses carefully targeted digital messages to trick people into installing malware or sharing sensitive data. • **Machine-learning** models can now match humans at the art of crafting convincing fake messages, and they can churn out far more of them without tiring. Hackers will take advantage of this to drive more phishing attacks.
Social Engineering	• Sophisticated criminals use deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. • Through 2022, at least **95%** of cloud security failures will be the fault of the organization, according to Gartner. • As more sophisticated tactics such as **social engineering** are engineered to compromise sensitive data, organizations should expand their cybersecurity team to address evolving digital risks.
Malicious Encrypted Web Traffic	• **50%** of global web traffic was encrypted as of October 2017. Encryption is meant to enhance security. But it also provides malicious actors with a powerful tool to conceal command-and-control activity. Those actors then have more time to inflict damage. • Without the ability to inspect encrypted traffic, the average organization would have missed over **900 file-based attacks per year** hidden by SSL/TLS encryption. • Encryption also reduces visibility. More enterprises are therefore turning to machine learning and artificial intelligence. With these capabilities, they can spot unusual patterns in large volumes of encrypted web traffic.
Cryptocurrency Mining	• With the rise of bitcoin, the threat won't just be the mining but the theft of computer processing power. • In the first three months of 2018, Comodo said it "detected **28.9 million cryptominer incidents** out of a total of 300 million malware incidents, amounting to a 10 percent share." • According to The Next Web that cited findings from the annual report of cybersecurity vendor Group-IB late on Friday, North Korean hacker group (Lazarus) was behind 14 hacking attacks on cryptocurrency exchanges since January 2017 – stealing **$571 million**.

Source: Technology Review, Gartner, Gartner: PR, Cisco, SonicWall, CSO, News18

OTHER CYBERSECURITY EMERGING THREATS (2/2)

Type	Description
Evolution of Malware	• Organizations now face everything from network-based ransomware worms to devastating wiper malware. At the same time, adversaries are getting more adept at creating malware that can evade traditional sandboxing. • **WannaCry** and **Trickbot** use worm functionality to spread malware. More malware families will use this technique in 2018 because network compromise from worms spread faster than many other methods. • While no single exploit rose to the level of Angler or Neutrino in 2016, there were **plenty of malware writers leveraging one another's code** and mixing them to form new malware, thus putting a strain on signature-only security controls. • If hackers can figure out how to use worms without being too noisy (a traditional downfall of this approach), this tactic can amass a large number of victims very quickly.
Supply Chain Attacks	• The US government has repeated warnings of state-sponsored cyber-attacks made possible by infiltrating the **software supply chain**. The report from the National Counterintelligence and Security Center (NCSC) reveals insight into foreign economic and industrial espionage against the US. • Background: US calls out China, Russia and Iran as "three of the most capable and active cyber actors tied to economic espionage and the potential theft of US trade secrets and proprietary information." • While new technologies such as AI and IoT will introduce new vulnerabilities into networks "for which the cybersecurity community remains largely unprepared," it's the software supply chain that represents one of the **biggest emerging threats, the NCSC claimed**.
Bot (DDoS)	• The threat of Bots is ever present. Bots are efficient little blighters designed to scan a system and find specific information such as credit card information, weak points in new software patches or previously unknown access points that can then be exploited. • According to Akamai, hospitality industry experiences many more credentials & PII abuse attacks than other sectors. • Akamai analyzed nearly **112 billion** bot requests and **3.9 billion** malicious login attempts that targeted sites in hospitality industry.

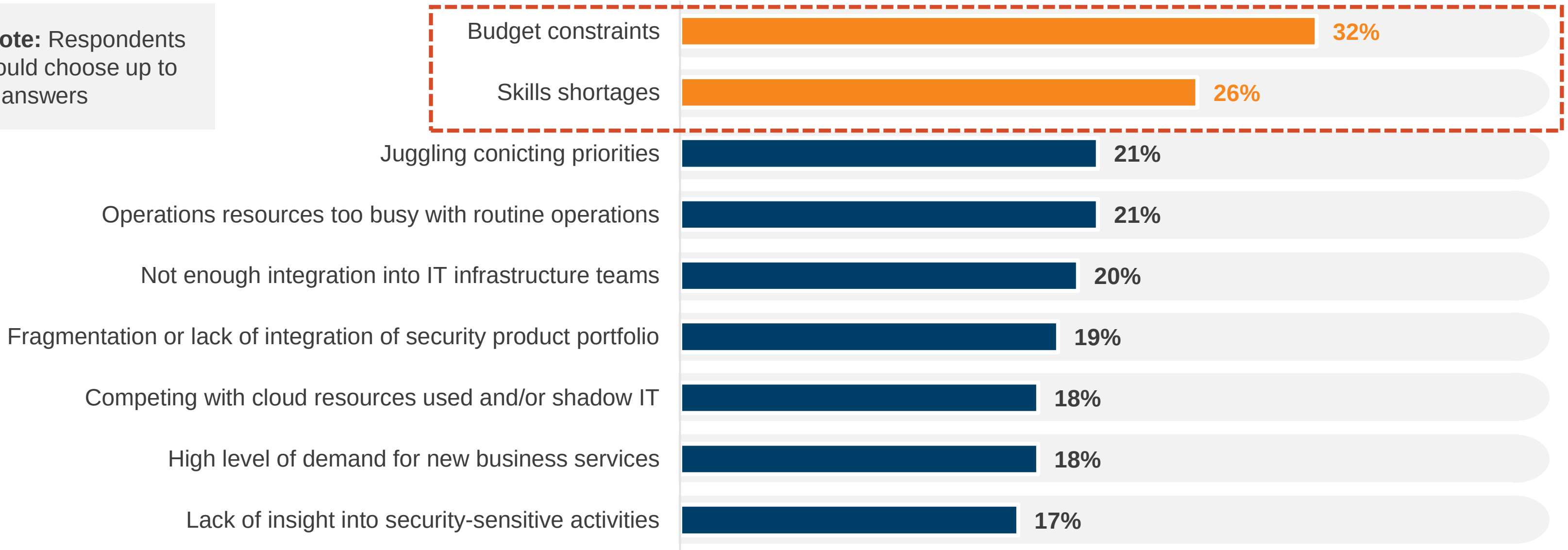
Source: Cisco, SC Magazine, SonicWall, Infosecurity, Purplegriffon.com, Akamai

CYBER DEFENSE APPROACH

CHALLENGES AND OBSTACLES (1/2)

Obstacles to Improving Cybersecurity

Note: Respondents could choose up to 3 answers



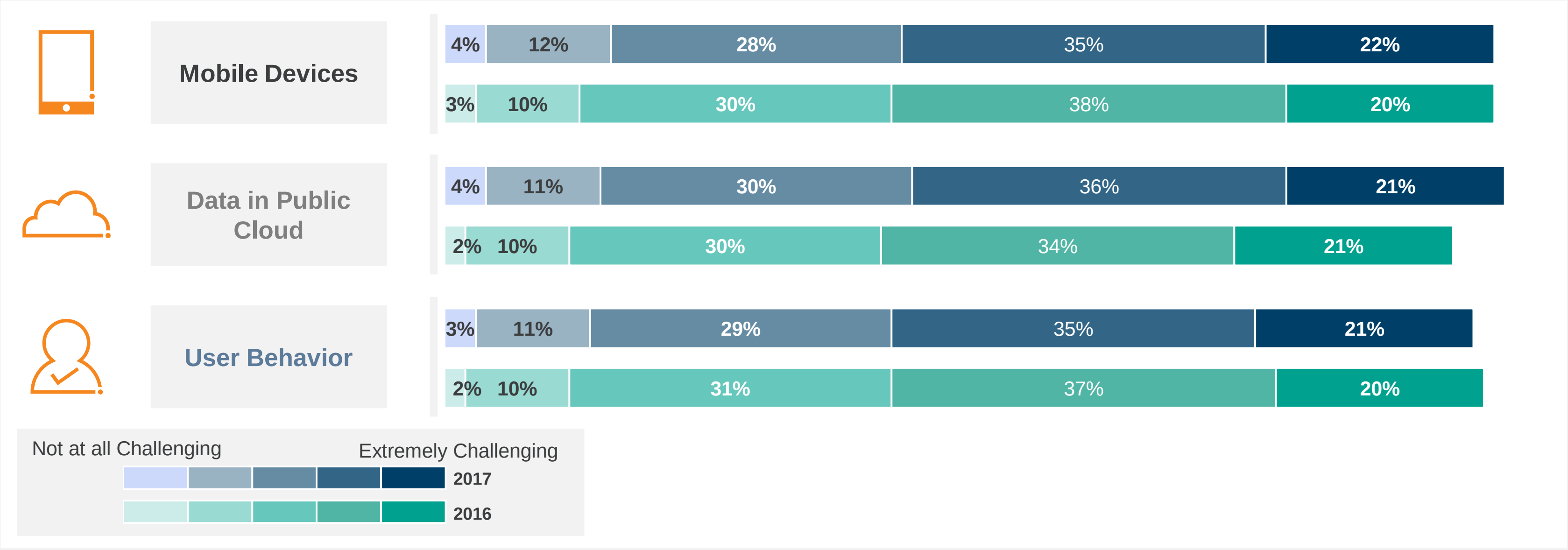
According to IDC, Security professionals cite budget, and personnel as their key constraints when managing security. The lack of trained personnel is also named as a challenge to adopting advanced security processes and technology. In 2017, 26% cited the lack of talent as an obstacle, compared with 25 percent in 2016 and 22 percent in 2015. In 2017, the median number of security professionals at organizations was 40, a significant increase from 2016's median number of 33.

Sources: VMWare

CHALLENGES AND OBSTACLES (1/2)

Challenging Areas to Defend

In their efforts to protect their organizations, security teams face many roadblocks. Organizations must defend several areas and functions, which adds to security challenges. The most challenging areas and functions to defend are mobile devices, data in the public cloud, and user behavior.



Sources: VMWare

CYBER DEFENSE CRITICAL QUESTIONS

Prevention

Are we able to prevent breaches?

Detection

Are we able to detect breaches?

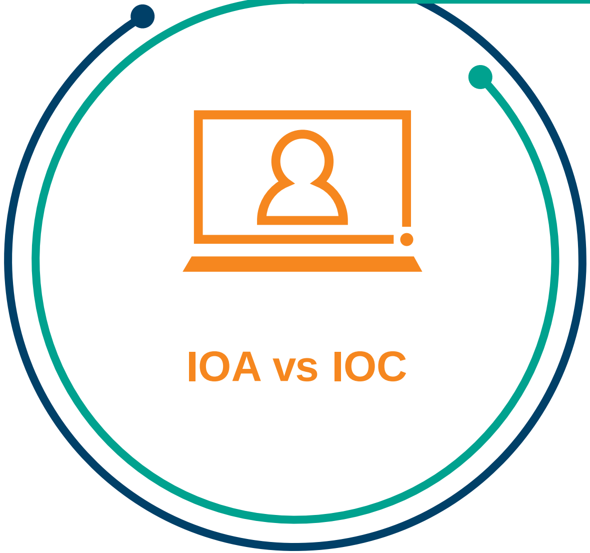
Awareness

Are we already breached?

UNDER ATTACK OR ALREADY COMPROMISED?

Indicators of Attack (IOA)

- Internal reconnaissance & enumeration
- Attempts to access credentials in memory
- Password spraying against large user population



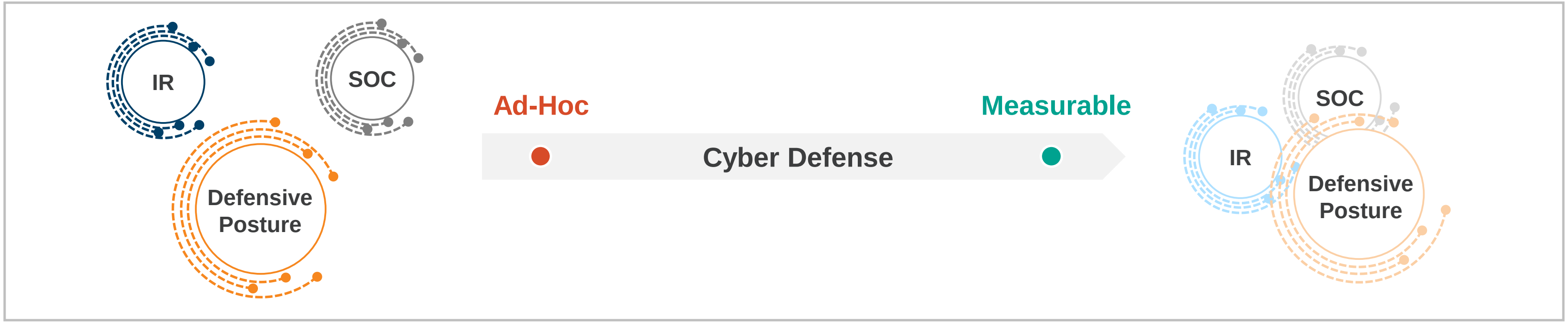
IOA vs IOC

Indicators of Compromise (IOC)

- Malicious file detected on disk
- Exploitation of a vulnerability using known malicious payload
- Communication to a known malicious IP address

- **Align detection controls to behaviors** in addition to signatures
- **IOAs often occur before IOCs** after the initial breach has occurred
- Focus your effort on catching the attacker **before further compromise occurs**

CYBER DEFENSE BASICS



Governance

- Enforce a security by design approach to stay ahead of future threats for new infrastructure
- Establish ongoing alignment and transparency between the SOC and IR programs with overall defensive posture
- Align defense according to security building blocks (CIS Critical 20, Defense in Depth)

Strategy

- Build manageable and reportable metrics (realistic goals and traceability)
- Support the natural growth of cyber defenses through attack frameworks (MITRE, Kill Chain, DiD)
- Incorporate current and effective threat based tactics and techniques to reduce business risks

Validation

- Use threat simulations to continually improve defensive posture (preventative and detective)
- Make a threat hunt valuable to the organization

Face the Future with Confidence

protiviti®