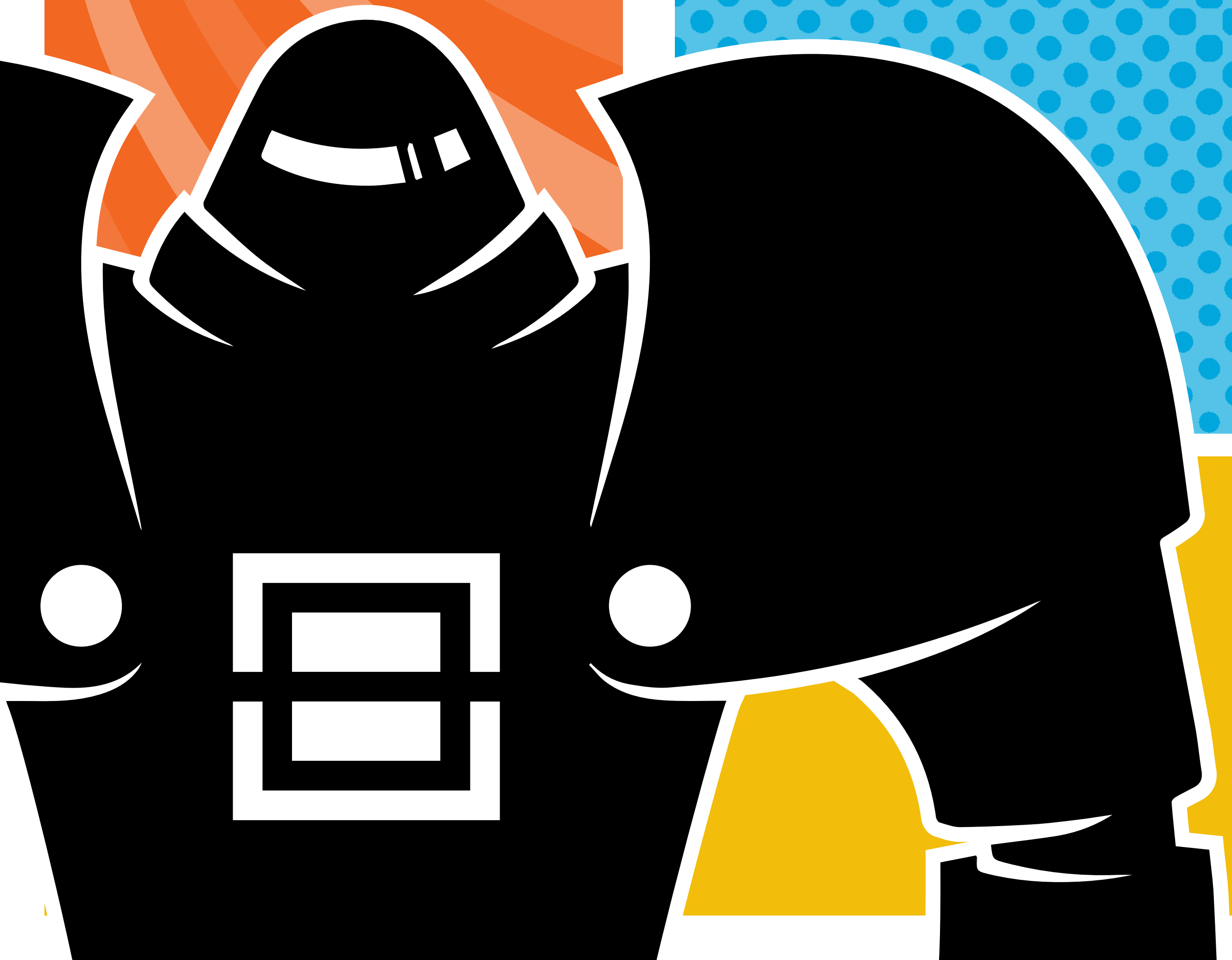
Balbix®

SETTING UP A HACKER-PROOF INFOSEC TEAM



WHAT'S A ROCKSTAR CISO'S FAVORITE SONG?

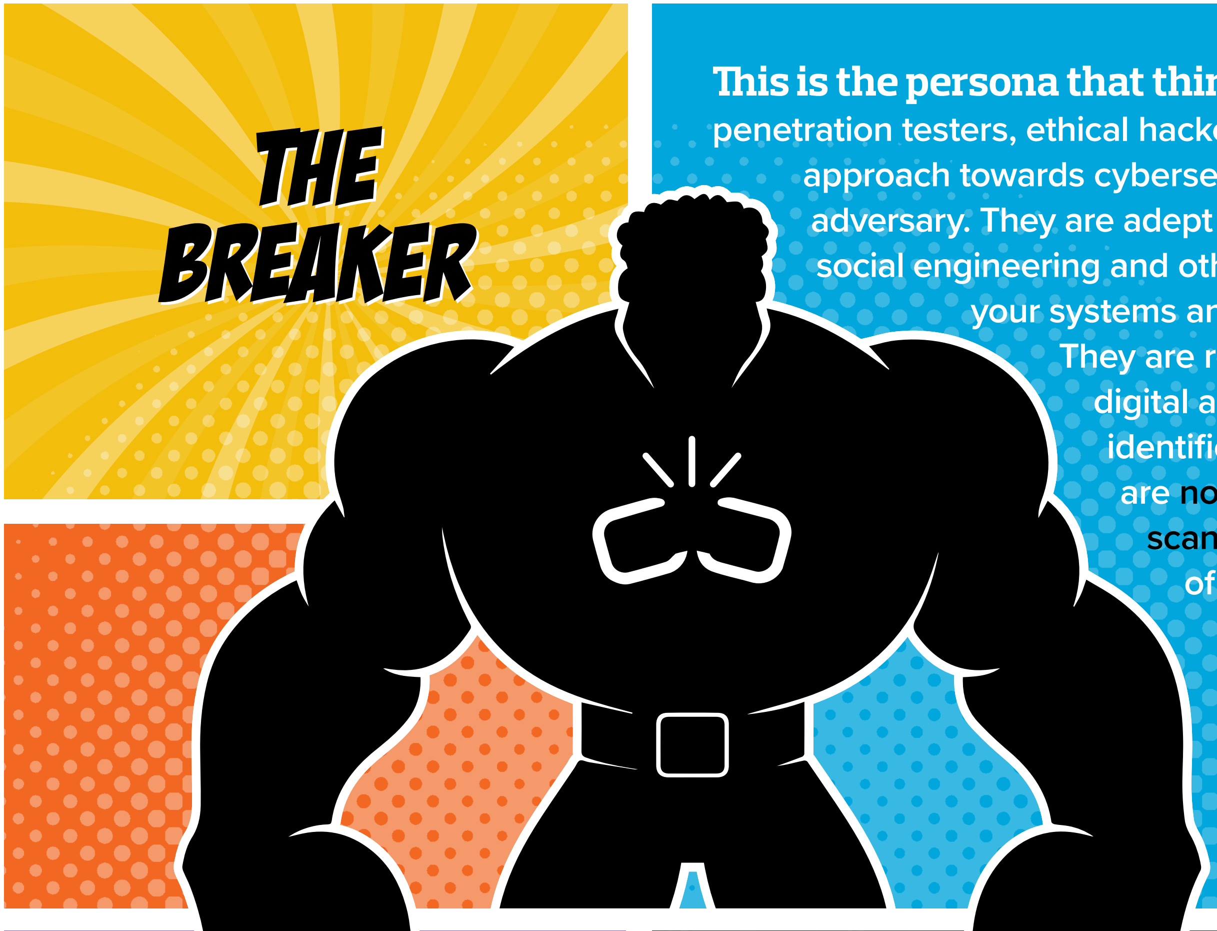
SMELLS LIKE TEAM SPIRIT!

Cheesy jokes aside, if you are or wish to be a rockstar CISO you know that you can't do it alone. You need a team that is completely aligned to your organization's overarching security goals and works like a well-oiled machine to beat the bad guys. And of course, I know that one can't really "hacker-proof" anything, but one can aspire, isn't it?

In most organizations, security teams are usually siloed around buckets of technology, an artifact of the days of traditional IT workflows. But as the threat landscape has evolved and cybersecurity has become a topic for board-level conversations, the traditional make-up of the security team has to be rethought from scratch and organized around skill-levels to be fully resilient. After all, the adversary doesn't care about your silos and is constantly looking to find a way to enter your networks, day-in and day-out.

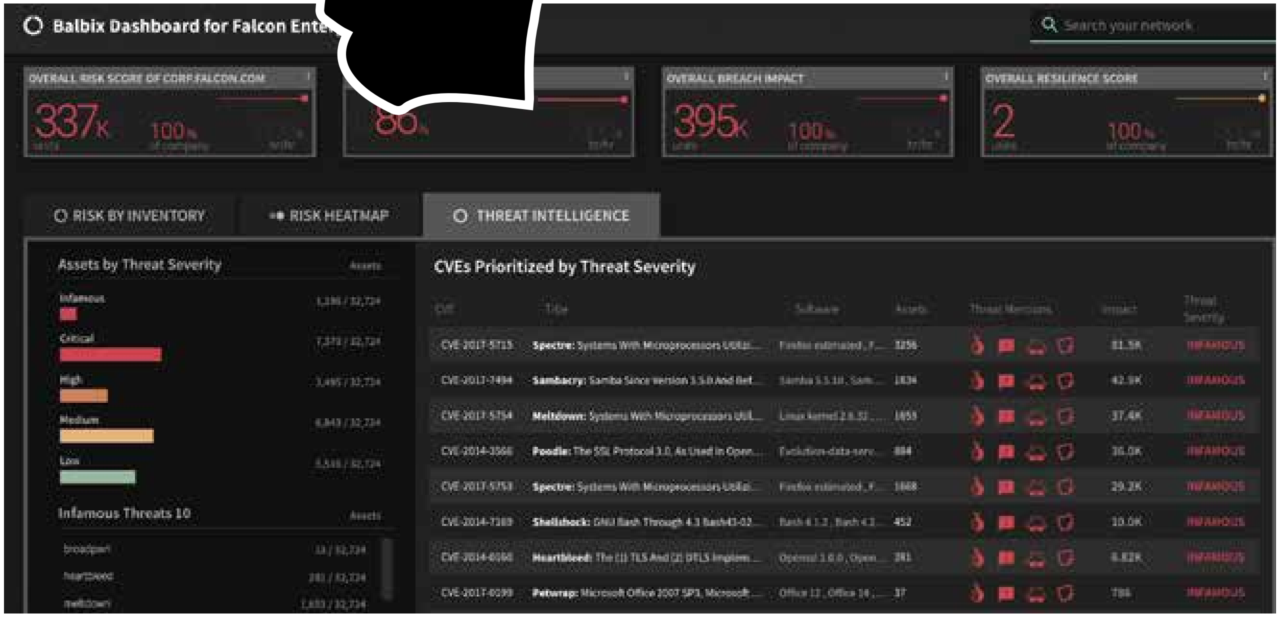
So, what does this dream–team look like? What are some essential personas that must be a part of this team?

THE BREAKER



This is the persona that thinks like a hacker. Red teams, penetration testers, ethical hackers are all folks that take an offensive approach towards cybersecurity by emulating the behavior of an adversary. They are adept at all forms of digital attack, as well as social engineering and other methods to find ways to break into your systems and test the limits of your security posture. They are responsible for securing the organization's digital assets through active hunting and identification of threats and vulnerabilities that are not detected by traditional vulnerability scanning. They possess a deep understanding of both information security and computer science and are comfortable with concepts such as networking, applications and operating system functionalities, application manipulation, exploit development, and stealthy operations.

HERE'S A VIEW OF THE ENTERPRISE A BREAKER WILL TYPICALLY LOOK AT



Balbix Dashboard for Falcon Ente

Search your network

OVERALL RISK SCORE OF CORP.FALCON.COM: 337K, 100% of company

86%

OVERALL BREACH IMPACT: 395K, 100% of company

OVERALL RESILIENCE SCORE: 2, 100% of company

RISK BY INVENTORY | RISK HEATMAP | THREAT INTELLIGENCE

Assets by Threat Severity

	Assets
Infamous	1,296 / 32,724
Critical	7,373 / 32,724
High	3,495 / 32,724
Medium	6,843 / 32,724
Low	5,546 / 32,724

Infamous Threats 10

	Assets
broadpwn	33 / 32,724
heartbleed	281 / 32,724
meltdown	1,653 / 32,724

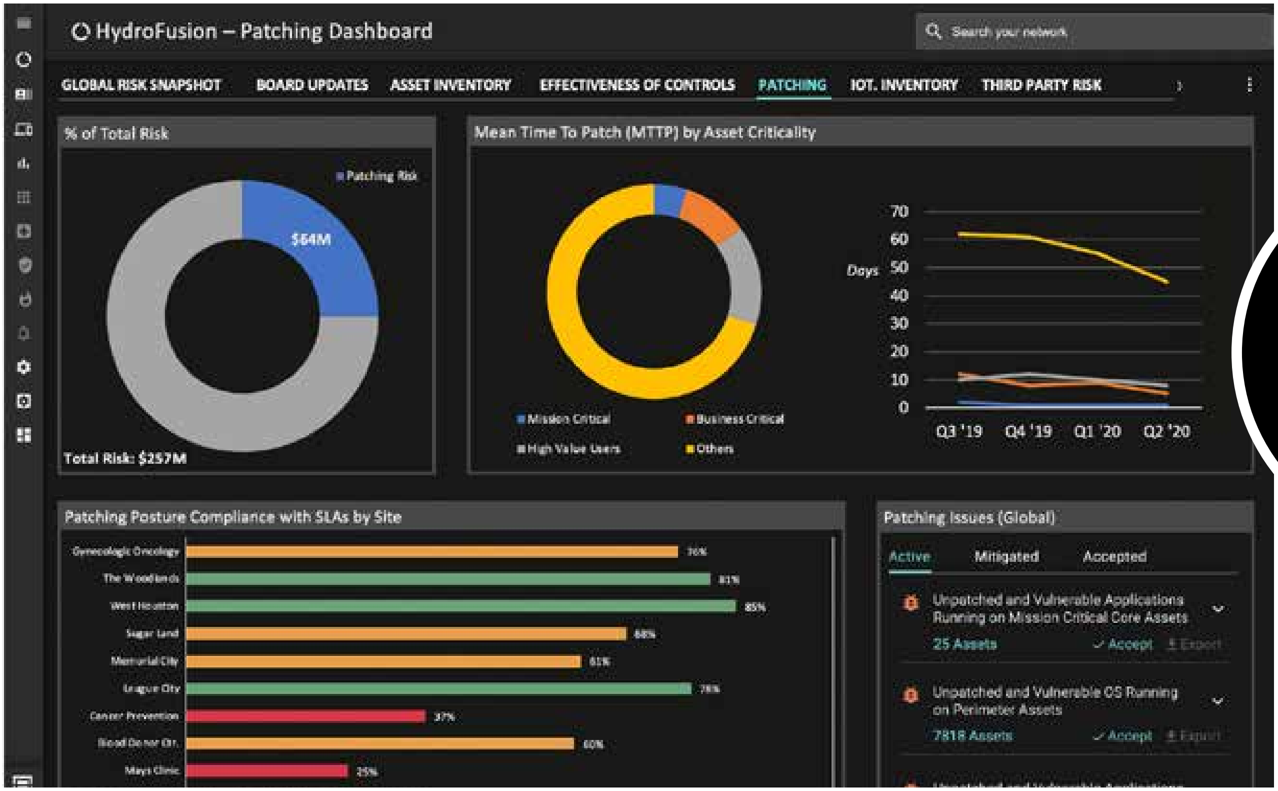
CVEs Prioritized by Threat Severity

CVE	Title	Software	Assets	Threat Mentions	Impact	Threat Severity
CVE-2017-5715	**Spectre:** Systems With Microprocessors Utiliz...	Firefox estimated , F...	3256		81.5K	INFAMOUS
CVE-2017-7494	**Sambacry:** Samba Since Version 3.5.0 And Bef...	Samba 3.5.10 , Sam...	1834		42.9K	INFAMOUS
CVE-2017-5754	**Meltdown:** Systems With Microprocessors Util...	Linux kernel 2.6.32 , ...	1653		37.4K	INFAMOUS
CVE-2014-3566	**Poodle:** The SSL Protocol 3.0, As Used In Open...	Evolution-data-serv...	884		36.0K	INFAMOUS
CVE-2017-5753	**Spectre:** Systems With Microprocessors Utiliz...	Firefox estimated , F...	1668		29.2K	INFAMOUS
CVE-2014-7169	**Shellshock:** GNU Bash Through 4.3 Bash43-02...	Bash 4.1.2 , Bash 4.2 ...	452		10.0K	INFAMOUS
CVE-2014-0160	**Heartbleed:** The (1) TLS And (2) DTLS Implem...	Openssl 1.0.0 , Open...	281		6.82K	INFAMOUS
CVE-2017-0199	**Petwrap:** Microsoft Office 2007 SP3, Microsoft...	Office 12 , Office 14 , ...	37		786	INFAMOUS

THE DEFENDER

A DEFENDER MIGHT CREATE A CUSTOM BALBIX DASHBOARD THAT LOOKS LIKE THIS

This persona makes up the majority of your cybersecurity team. Folks in vulnerability and patch management, threat intelligence, security operations, network defense, security architecture roles are all defenders. Blue teams can also be classified as defenders. They continually monitor and endeavor to harden security around and within the company's networks and data systems. The defenders provide technical expertise across the entire life cycle of vulnerability management including asset management, vulnerability scanning, threat intelligence, mitigating controls analysis, and reporting. They are also the ones to review vulnerabilities based upon footprint, threat intelligence and existing controls, in order to determine priority and risk ranking across the enterprise. In addition, they track and work with all support teams for patching and remediation report on status of patching deployments to the CISO.



Unpatched and Vulnerable Applications Running on Mission Critical Core Assets

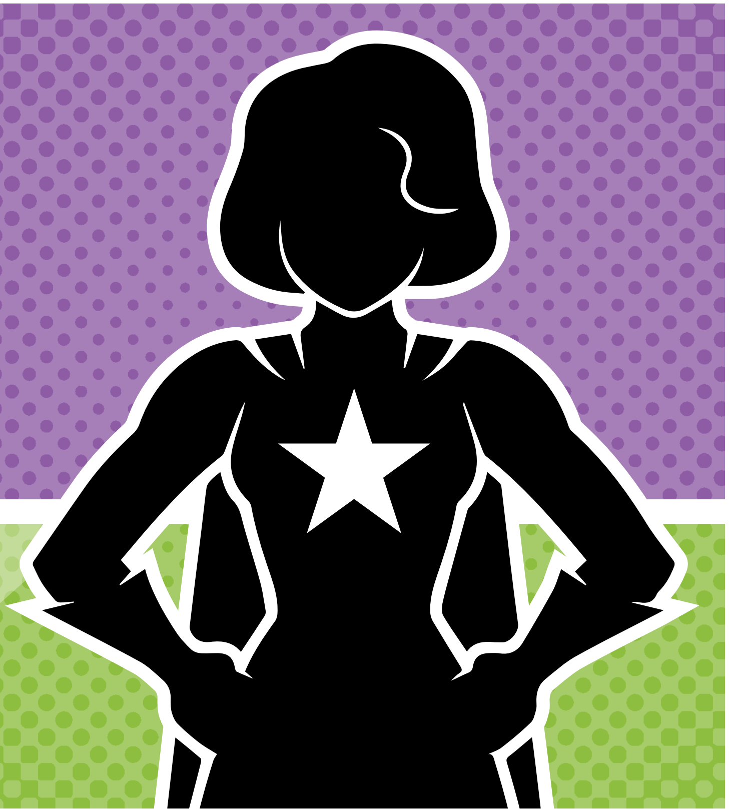
25 Assets ✓ Accept Export

Unpatched and Vulnerable OS Running on Perimeter Assets

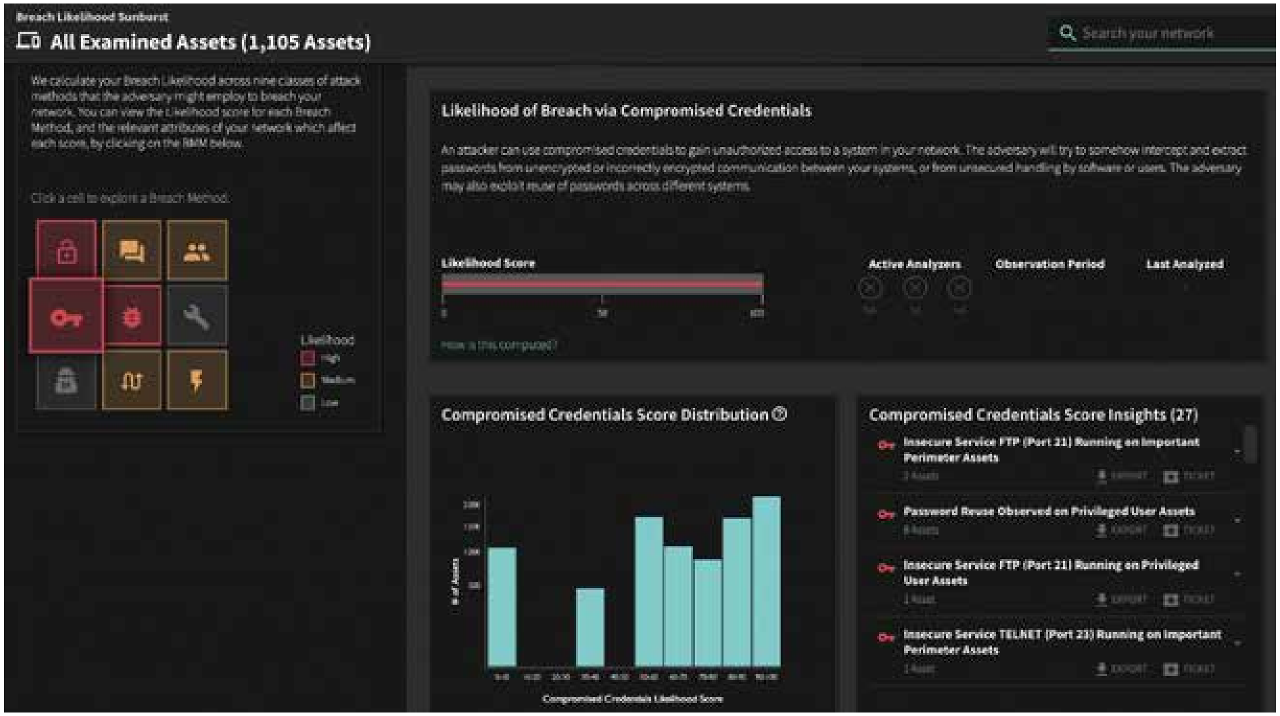
7818 Assets ✓ Accept Export

THE ENFORCER

This is the team member who is the policy and compliance expert. The person who is skeptical about who needs access to what and what rules can be relaxed. The Enforcer is also the person who says “no” to the employees (or admins) that have risky behavior —the tendency to click on phishing links and reuse passwords across accounts putting themselves at risk for credential stuffing. The enforcer takes the responsibility of ensuring that the organization is following all compliance best practices very seriously.



A SUITABLE VIEW OF THE ENTERPRISE FOR THE ENFORCER PERSONA WOULD LOOK LIKE THIS



Breach Likelihood Sunburst

All Examined Assets (1,105 Assets)

We calculate your Breach Likelihood across nine classes of attack methods that the adversary might employ to breach your network. You can view the Likelihood score for each Breach Method, and the relevant attributes of your network which affect each score, by clicking on the RMM below.

Click a cell to explore a Breach Method.

Likelihood
🟥 High
🟧 Medium
⬛ Low

Likelihood of Breach via Compromised Credentials

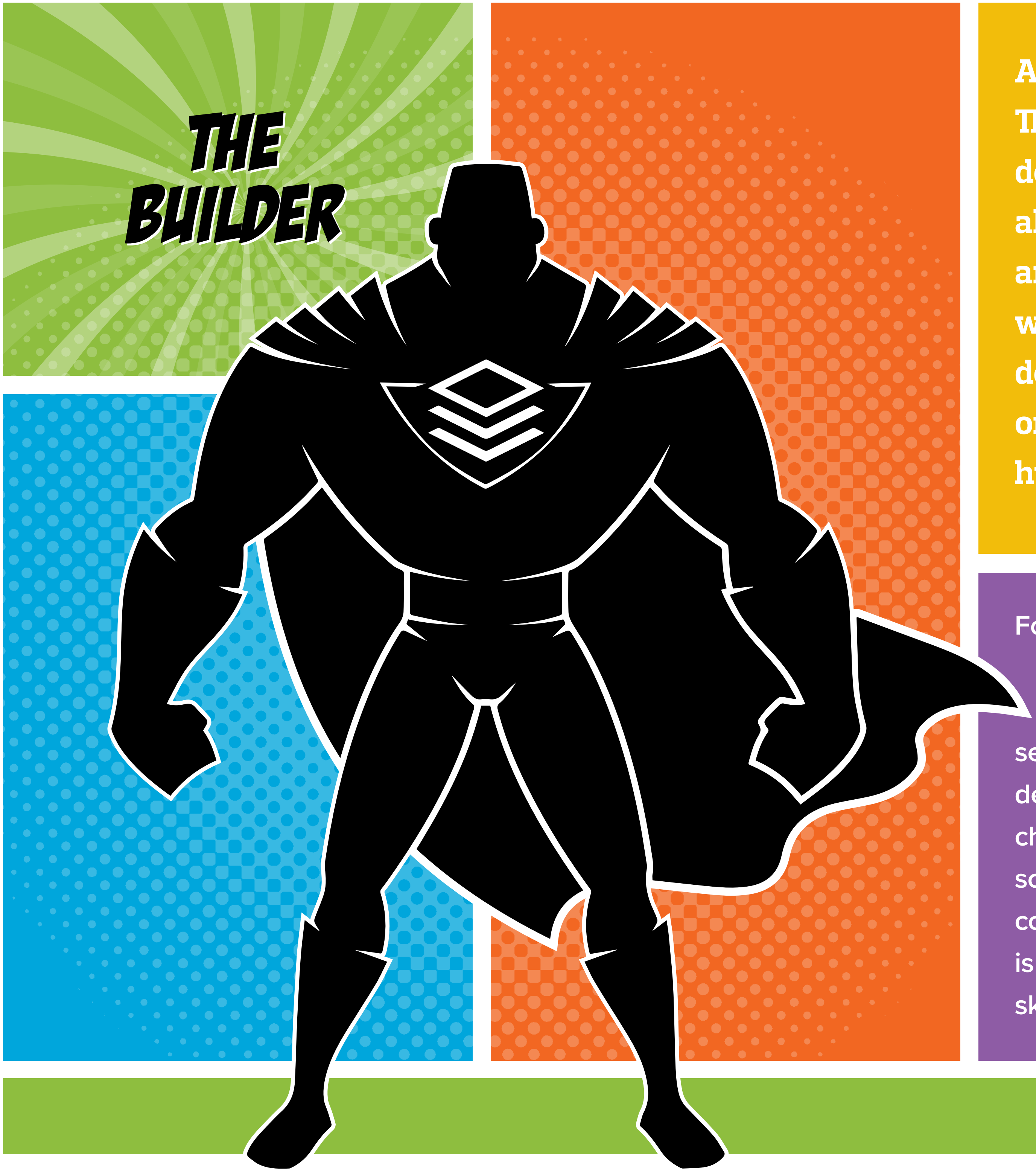
An attacker can use compromised credentials to gain unauthorized access to a system in your network. The adversary will try to somehow intercept and extract passwords from unencrypted or incorrectly encrypted communication between your systems, or from unsecured handling by software or users. The adversary may also exploit reuse of passwords across different systems.

Compromised Credentials Score Distribution

Compromised Credentials Score Insights (27)

- Insecure Service FTP (Port 21) Running on Important Perimeter Assets
  2 Assets
- Password Reuse Observed on Privileged User Assets
  8 Assets
- Insecure Service FTP (Port 21) Running on Privileged User Assets
  1 Asset
- Insecure Service TELNET (Port 23) Running on Important Perimeter Assets
  1 Asset

THE BUILDER

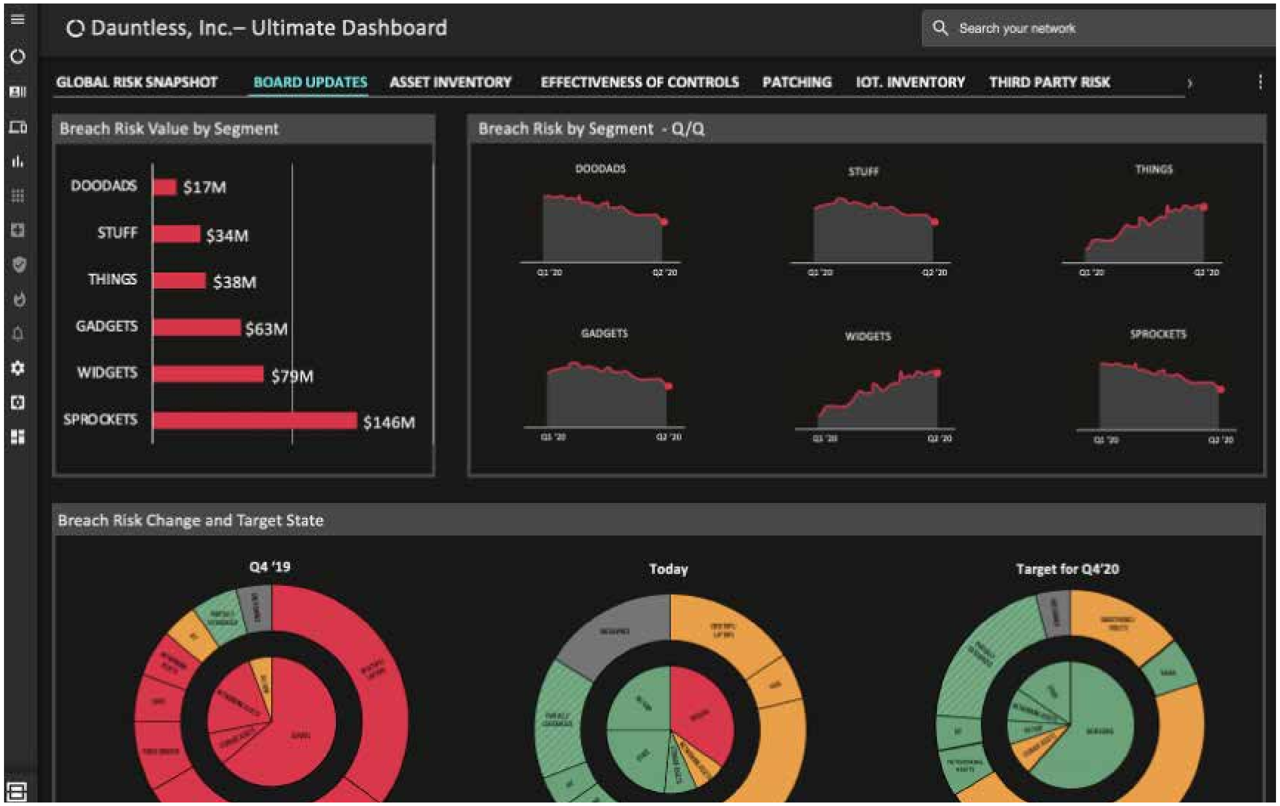


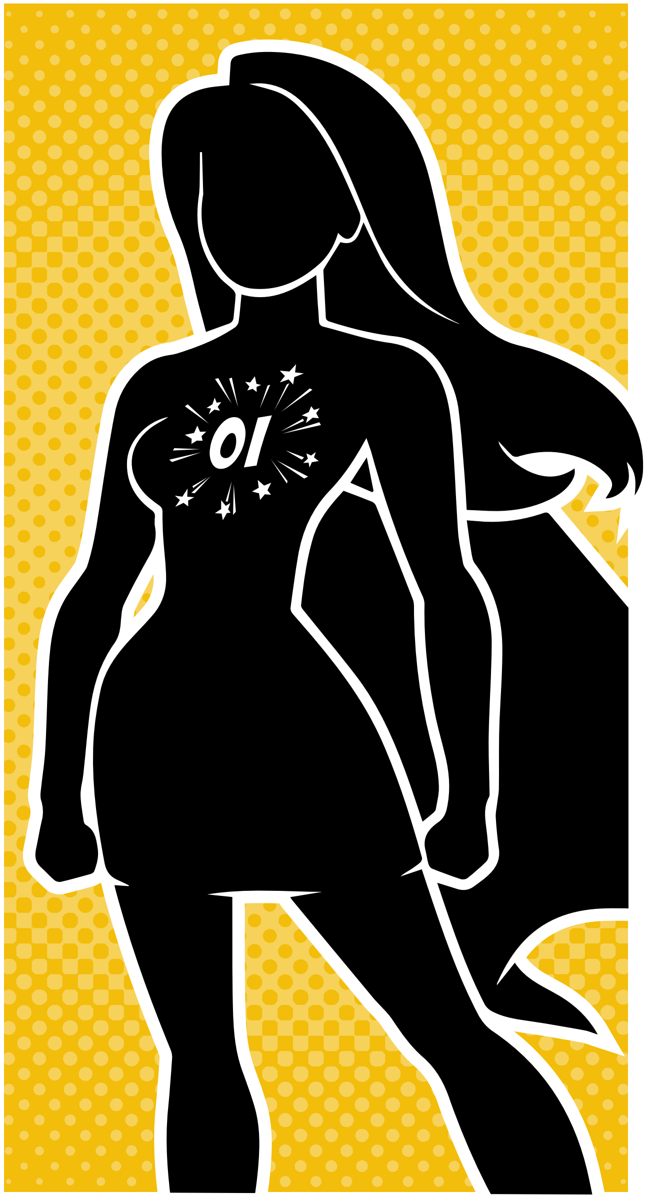
As the name suggests, The Builder (or software developer) brings key abilities to the team and having someone with secure software development skills on your team is a huge advantage.

For example, you need coding skills to enable API based integrations of the various security products you have deployed. Also, security challenges are frequently solved by integrating third-party components and SDKs, so this is one area where developer skills can come in handy.

THE NUMBER CRUNCHER

The Number Cruncher (or CFO) as a part of the security team may come as a surprise to you. But security really is everyone's responsibility and building relationships across the enterprise has never been more pertinent. Cybersecurity is a critical financial risk to an organization and the cost of cybersecurity is not only related to purchasing tools and hiring resources to avert cyberattacks, but also the potential cost of a breach.





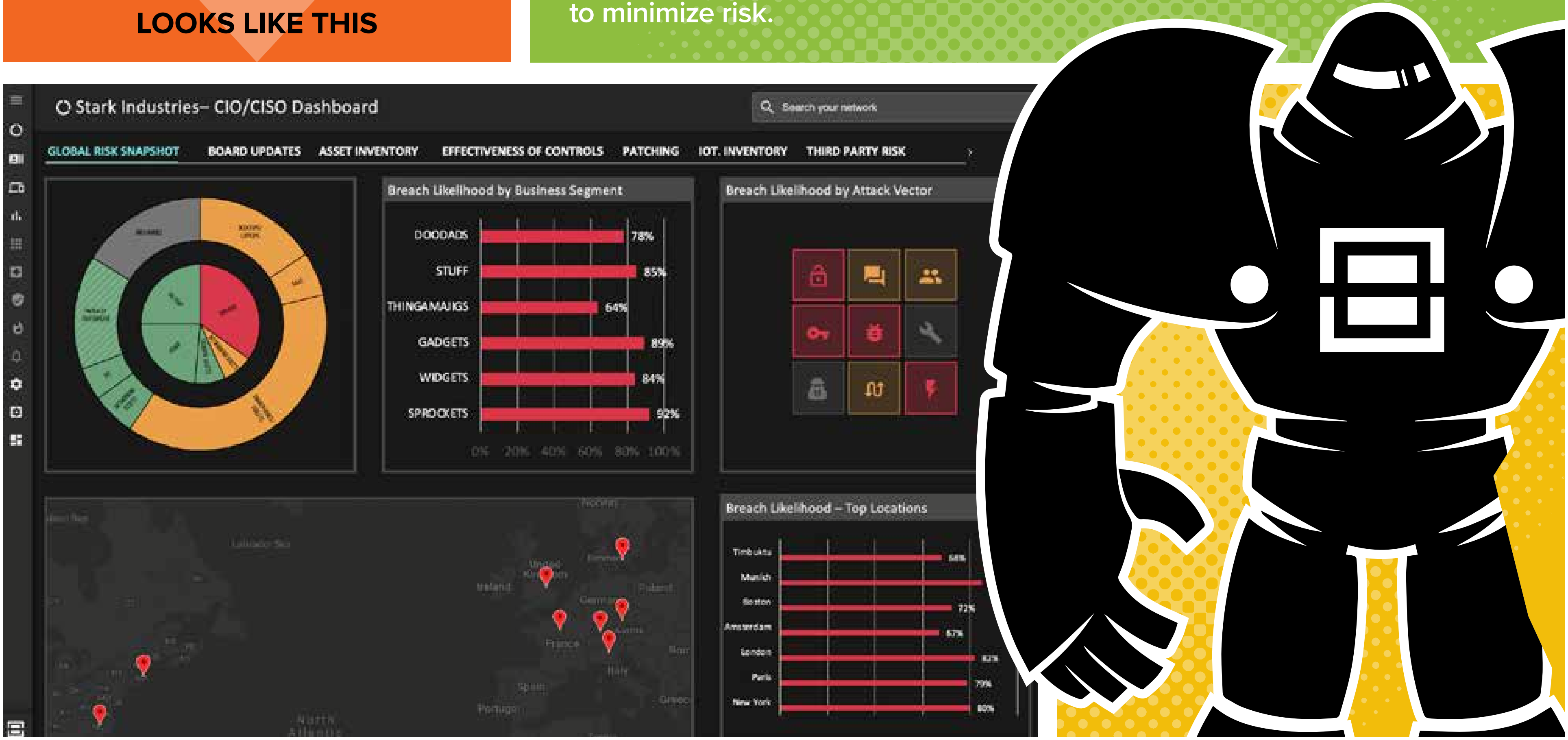
THE NUMBER CRUNCHER NEEDS TO HAVE VISIBILITY INTO THE FINANCIAL ASPECT OF CYBER RISK THAT THE ORGANIZATION TAKES ON, SO THEIR BALBIX DASHBOARD VIEW MIGHT LOOK LIKE THIS

THE INTELLIGENCE

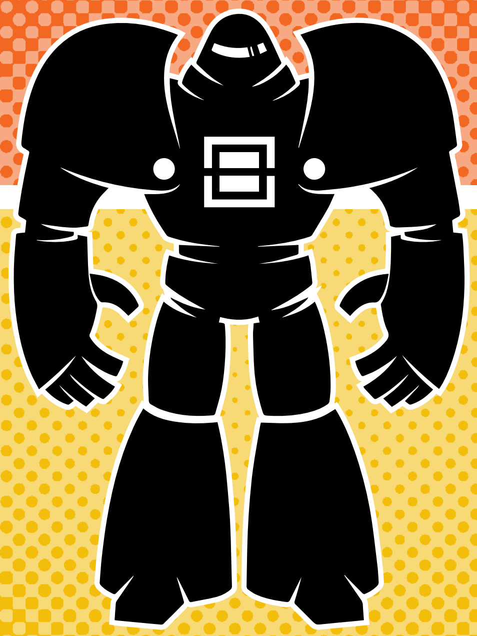
THE BALBIX DASHBOARD MOST USED BY CISOS & CIOS TO GET A HIGH LEVEL VIEW OF WHERE RISK LIES IN THEIR ORGANIZATION LOOKS LIKE THIS

Balbix—an extension of your security team. With the number of cybersecurity threats growing every day and increased digitization of assets and processes that could be vulnerable to those threats, it is mathematically impossible for humans to monitor for threats and sift through hundreds of thousands of vulnerabilities to determine which to prioritize and how to address your cyber-risk. You need AI for that.

The Balbix platform is powered by AI, a smart system of automated breach risk assessment, which discovers and continuously analyzes your complete attack surface with little or no human effort, learns the context of your business, identifies and categorizes your assets, and monitors them for security vulnerabilities in real time. Balbix then prescribes the necessary tactical and strategic mitigations to minimize risk.



Let us show you how Balbix can be an extension of your security team and enable other members to do their jobs even more effectively and efficiently.



Balbix®

SCHEDULE A 30-MINUTE PRESENTATION

Balbix is the world's first cybersecurity platform to leverage specialized AI to provide real-time visibility into an organization's breach risk. The Balbix system predicts where and how breaches are likely to happen, prescribes prioritized mitigating actions, and enables workflows to address the underlying security issues. By using Balbix, CISOs and CIOs can transform their security posture, reducing cyber risk by 95% or more, while making security teams 10 times more efficient. Balbix counts many global 1000 companies among its rapidly growing customer base and was named a "Cool Vendor" by Gartner in 2018.